S. Hrg. 113–426

# THREATS TO THE HOMELAND

## HEARING

BEFORE THE

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

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

NOVEMBER 14, 2013

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 PRINTING OFFICE

86–635 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing 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
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota

TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire

RICHARD J. KESSLER, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
HARLAN C. GEER, *Senior Professional Staff Member*
MICHELLE C. TAYLOR, *Federal Bureau of Investigations Detailee*
KEITH B. ASHDOWN, *Minority Staff Director*
CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*
DANIEL P. LIPS, *Minority Director of Homeland Security*
MARK K. HARRIS, *U.S. Coast Guard Detailee*
LAURA W. KILBRIDE, *Chief Clerk*
LAUREN M. CORCORAN, *Hearing Clerk*

# CONTENTS



## WITNESSES

### WEDNESDAY, NOVEMBER 14, 2013



### ALPHABETICAL LIST OF WITNESSES



## APPENDIX

# THREATS TO THE HOMELAND

**WEDNESDAY, NOVEMBER 14, 2013**

COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant to notice, at 10:04 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, presiding.

Present: Senators Carper, Levin, Coburn, Johnson, and Ayotte.

## OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. This hearing will come to order.

Good morning, everyone. Welcome to our witnesses, Dr. Coburn. I welcome all of you, and we will be joined by some of our colleagues here as the morning progresses, but we are happy you are all here bright and early.

Today's hearing will consider threats to the U.S. homeland from terrorists, from cyber attackers, from homegrown extremists, and from lone wolf offenders. The objective of this hearing is for this Committee to gain a better understanding of how these threats have evolved over the last year and if our national security agencies are keeping up with these ever-changing threats. I would add another purpose for these hearings is to find out what we need to be doing on the legislative side to better enable you to keep up with these ever-changing threats.

As we know, 12 years ago, our country's sense of security was upended when Al-Qaeda launched the most significant attack on U.S. soil since Pearl Harbor. In the years since that tragic day, we have made significant progress in combatting the terrorist threat to our homeland. On behalf of this entire Committee, I want to express our thanks from the American people for the very good work that has been done and continues to be done to try to make sure that we stay safe in a very dangerous world.

Our aviation system is more secure. Our borders are stronger. Our government agencies share more terrorist intelligence than ever before. Our first responders are better prepared to deal with disasters and terrorist attacks. Americans are safer because of these efforts.

And while we have made great strides, our system for preventing terrorist attacks is not perfect, and as Dr. Coburn knows, one of my guiding principles is, if it is not perfect, make it better. This is not a time to rest on our laurels. This is not the time to take a victory lap. It is a time to thank those that are working hard to

make us safe, keep us safe, and let us continue to work hard and work smarter.

In this spirit, this Committee will continue its work to improve America's defenses against terrorism and other threats. Part of this process means understanding that the threat is also evolving. If we are to make America safer from these threats and secure our homeland, we must do a better job of anticipating those evolving threats.

We do a good job at fighting the last war, but to secure the homeland, we must be better at anticipating the next war. We know that the threats from Al-Qaeda have changed over the past decade and we are now dealing with a number of splinter groups, including Al-Qaeda in the Arabian Peninsula, which was responsible for the Christmas Day attack in 2009 and which continues its efforts to attack us to this day.

And we know that American citizens, as well as Canadian and European nationals, have taken up arms in Syria, Yemen, and Somalia. The threat that these individuals could return home to carry out attacks is real and troubling. Even as our borders and ports of entry (POE) have become more secure, there are still those within our borders who have become radicalized by online Al-Qaeda propaganda and seek to carry out their own attacks against the United States.

And there are other threats to our domestic security unrelated to Al-Qaeda which we must be prepared to address. As the September attack on the Washington Navy Yard and the shooting at the Los Angeles airport just 2 weeks ago demonstrate, there are a variety of threats to Federal personnel and Federal facilities that we must be prepared to defend against.

However, nowhere is the need to prepare for the next attack more pressing than in the cybersecurity realm. In the words of your predecessor, Director Comey, Bob Mueller, cyber threats may "equal or surpass the threat of terrorism in the foreseeable future." With a few keystrokes, hackers can shut down our electric grid. They can release dangerous chemicals into our air that we breathe. They can disrupt our financial markets. And now, more than ever, we must come together to pass cybersecurity legislation that strengthens our defenses against these cyber threats and others. The threat is too great, the potential consequences too severe to do nothing. Today's hearing will explore these threats as well as others.

Today, we will hear testimony from the leaders of the Department of Homeland Security (DHS), from the National Counterterrorism Center (NCTC), and from the Federal Bureau of Investigation (FBI) about the greatest dangers to the homeland and the steps that their colleagues are taking to further secure our country.

The findings from today's hearing will help continue our process of recalibrating our homeland defenses to address our current threats as well as prepare for tomorrow's threats. It will also help to ensure that we have a government in place that can connect the dots before terror comes to our shores.

We look forward to hearing from each of our witnesses, and the Members of our Committee do, as well, as we seek to defeat those threats and keep our countrymen and women safe from those who wish to do us harm.

Now, let me turn to Dr. Coburn for any remarks he wishes to make.

Senator COBURN. Thank you, Senator Carper.

Chairman CARPER. Good morning.

Senator COBURN. Good morning.

Chairman CARPER. Good morning Mr. Johnson, and good morning, Dr. Coburn.

**OPENING STATEMENT OF SENATOR COBURN**

Senator COBURN. First of all, let me welcome you to the Committee. I have expressed this to Senator Carper. I think we are best when we have open hearings, but this Committee also needs to have a closed hearing because the Members will not be able to be made aware of the things they need to be made aware of without a closed hearing. So, I would look forward to that at some point in the future.

Secretary Beers, I want to thank you for the great work you are doing, filling in at Homeland Security, and the cooperative nature you have demonstrated. You have been great to work with and I want to tell you I appreciate that and thank you for it.

Director Comey, it is a privilege to have you serving in your position today. I supported your position, having worked with you both on the Intelligence Committee and here. I appreciate what you are doing.

And, Matt, you have been tremendous. People will never know all the work that NCTC does because they cannot, but it is tremendous and I applaud you being here.

Other than that, I will reserve most of my comments for question and answer after we have heard the comments from our panelists. But I do appreciate your service. This is an important issue and it is important that we are having a discussion in public about what the real threats are. There is a discussion on how we address those. There is a difference of opinion in how we do it.

The one final note I would make is we need to have some reforms so this Committee has the authority and the responsibility to do those things, like the Federal Information Security Management Act (FISMA) reform and some of the other reforms in terms of cyber. But it is going to be hard to move on cyber until we create competency, and that is one of the areas that we have to make sure we have right before we give more authority.

So, with that, I would yield back and look forward to our witnesses' testimony.

Chairman CARPER. Thank you, Tom.

Let me take just a moment to introduce our panel of distinguished witnesses.

Our first witness is Rand Beers. I was joking in the anteroom that I knew Rand when he was six-foot-four and had shoulder-length blond hair, but I really did not know him then, and I do not know that he ever had hair that long. But, we are delighted, and I just want to say, to back up to what Dr. Coburn has said, you have taken on a tough job. First, you had your day job at Homeland Security, and then you were asked to be Deputy Secretary, and now you are asked to be the Acting Deputy Secretary and now

the Acting Secretary. That is a whole lot for any one man or woman to carry, so thank you for doing it in good spirit.

Rand has been serving as the Acting Secretary of Homeland Security since early September, when Janet Napolitano left us to head up the department at the University of California system on the West Coast. Rand most recently served as the Acting Deputy Secretary. Before that, he held the position of Under Secretary of National Protection Programs Directorate at the Department (NPPD).

Prior to coming to the Department of Homeland Security, Secretary Beers served on the National Security staff under not one, not two, not three, but four Presidents. He began his professional career as a Marine Corps officer in Vietnam. I think if we go back 5 days, there was a birthday for the Marine Corps, so happy belated birthday and thank you for your service in Southeast Asia and welcome home. But, thank you for joining us today.

Our next witness is James Comey, Director of the Federal Bureau of Investigation. He has a tough act to follow, as he knows. We talked about it not long ago in my office. Thank you for your willingness to do this and we are excited about your leadership and the way you hit the ground running.

Jim is the seventh Director of the FBI since September, I believe. He brings a wealth of law enforcement experience to the FBI, having served as the U.S. Attorney for the Southern District of New York and as Deputy Attorney General (AG) at the Department of Justice (DOJ). After leaving the Department of Justice in 2005, Mr. Comey served as the General Counsel at Lockheed Martin and then held the same position at the investment management firm of Bridgewater Associates.

Thank you for your presence today and your testimony. Thank you very much for your years of service to our country.

Our final witness is Matt Olsen, Director of the National Counterterrorism Center. Matt, good morning. Mr. Olsen has served as the Director of the National Counterterrorism Center for just over 2 years. In this position, Director Olsen oversees the analysis and the integration of all terrorism intelligence in the U.S. Government, reporting directly to the Director of National Intelligence (DNI). Additionally, he oversees the strategic operational planning for counterterrorism activities, a role that requires him to report directly to the President.

Prior to joining the National Counterterrorism Center, Mr. Olsen was the General Counsel for the National Security Agency and the Deputy Assistant Attorney General in the Department of Justice's National Security Division.

Again, Matt, thank you for joining us today. We welcome your testimony.

I am going to turn it over to you, and Mr. Secretary, if you would like to lead us off, and after you have finished your testimonies, we will get into a good conversation. But, you are recognized. Please proceed. Thank you all, again, for joining us.

**TESTIMONY OF THE HON. RAND BEERS,[1] ACTING SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY**

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

I would also like to thank my co-panelists, Directors Comey and Olsen, for their partnership and strong collaboration as we together meet the shared responsibility of keeping the American people safe.

Before I begin my testimony, I would like to urge you all and the Senate to confirm Jeh Johnson as my replacement and confirmed nominee. I have known him for a long time and I think he cares deeply about our mission and I think he has considerable skill, intellect, and experience, and dedication to deal with these evolving threats. And, Senator Coburn, I appreciate your remarks to him yesterday. In short, I think he will make an excellent Secretary.

I would also like to take a moment, as you did, Senator Carper, to recognize Transportation Security Officer (TSO) Gerardo Hernandez, who was killed at the Los Angeles airport on the first of November. He was an exceptional officer and his loss will be felt within the Transportation Security Administration (TSA) and the Department. I had the honor and somber experience of going to his memorial service yesterday. It was a very moving event, and this——

Chairman CARPER. Let me just interrupt, Secretary. Is there another memorial service, maybe next Monday or something——

Mr. BEERS. We are having one here at TSA, yes, that is correct, sir.

Chairman CARPER. That is one o'clock on Monday, I think?

Mr. BEERS. I will get the time precisely to you, but yes, we are going to have another one——

Chairman CARPER. Thanks so much.

Mr. BEERS [continuing]. Another one here.

That senseless act, as you said, sir, reminds us every day of the dangers that the men and women who work on the front lines of our Department, and other parts of the U.S. Government, have very real sacrifices that they often have to make on our behalf. We continue to work closely with the Bureau and with State and local law enforcement to fully investigate this crime and ensure that justice is done, as the Attorney General said yesterday.

DHS works very closely with all of our partners across the country to build critical capabilities at every level, whether it is sharing information, protecting critical infrastructure, or protecting our cyberspace. We work with the private sector on improving preparedness and resilience and addressing the evolving threats, such as I just mentioned. Because of this work, our Nation, I believe, is stronger and better equipped to handle these threats and we are more nimble in our ability to respond and recover. Nevertheless, we continue to face a dynamic threat environment that includes threats from abroad as well as those that originate within our borders.

At DHS, our chief operating principle has been to work with partners to detect and deter these threats as early as possible, to

[1] The prepared statement of Mr. Beers appears in the Appendix on page 43.

build the capabilities to respond if and when required, and enhance our ability to recover after the fact. We have sought to get information, tools, and resources out of Washington, D.C., and into the partners that we work with on the front line.

At the Federal level, with intelligence and law enforcement partners like the Bureau and NCTC, we have made significant strides, I believe, in information sharing and joint analysis. Through State and major urban area Fusion Centers, we have improved sharing of both classified and unclassified information and built grassroots analytic capabilities at the State and local levels.

With the FBI, we have now standardized how we train front line law enforcement to recognize behaviors and indicators that have historically been associated with terrorism and report suspicious activities as part of the National Suspicious Activities Reporting (SAR) Initiative (NSI). We have greatly expanded our training and our outreach on encountering violent extremism and active shooter threats, providing extensive tools, workshops, and analysis on potential indicators of terrorism and providing partners with resources and training to effectively respond to active shooter threats.

We have also strengthened our ability to address improvised explosive devices (IEDs) through training and awareness and grants and information sharing. These investments directly contributed to the comprehensive and well executed response at the Boston Marathon attack and prevented more lives from being lost on that tragic day.

We have also expanded our "If you see something, say something" campaign to more than 250 cities and States and transportation systems, universities, and private sector entities nationwide to encourage the public to play an active role in reporting suspicious activity.

With respect to our aviation sector, we have built upon the successes of our risk-based intelligence-driven approach, which includes prescreening of passengers, deployment of new technologies, training of airport security and law enforcement personnel to better detect those behaviors potentially associated with terrorism and strengthening our air cargo security.

Today, we are much better able to protect the aviation sector because we vet those who are traveling—who seek to travel or immigrate to the United States against a broad array of law enforcement and intelligence information. We are working with our components to identify ways further to enhance these vetting operations to harness the power of data management while providing better safeguards and access control. And we also continue to leverage information and technology to expedite trusted travelers through a successful program such as Global Entry and TSA Pre-Check. To date, more than 16 million travelers have already experienced Pre-Check.

Of course, as you said, one of our major threats, one of our gravest threats that we continue to face is the threat to our cyber networks and infrastructure. Our Nation confronts a dangerous combination of known and unknown cyber vulnerabilities and adversaries with strong and rapidly expanding capabilities. Our focus at DHS remains securing unclassified Federal system government

networks, working with critical infrastructure owners and operators, combating cyber crime, building a national capacity to promote responsible cyber behavior, and cultivating the next generation of front line cybersecurity professionals, all the while protecting privacy, civil rights, and civil liberties.

To this end, we have deployed technology to detect and block cyber intrusions and we are developing continuous diagnostic capabilities while providing guidance to Federal agencies on how to protect themselves. We have also worked closely with infrastructure owners and operators to strengthen their facilities through an onsite risk assessment, mitigation, and incident response by sharing risk and threat information through U.S. Computer Emergency Readiness Team (US–CERT) and other means.

Since 2009, we have also prevented $10 billion in potential losses through our cyber crime investigations with domestic and international partners and arrested more than 5,000 individuals for participating in cyber crime activities. We have also partnered with the Departments of Justice and Defense (DOD) to ensure the whole of government approach when responding to cyber incidents and threats.

While these accomplishments are significant, and President Obama has further strengthened them through executive action, we still need Congress to pass a suite of comprehensive cybersecurity legislation to be best able to meet this growing threat.

Thank you very much for this opportunity.

Chairman CARPER. Thank you. Thank you for that testimony.

Before I turn it over to Director Comey, during the question and answers (Q&A), we are going to come back to cybersecurity——

Mr. BEERS. Good.

Chairman CARPER. And get just an update as to where the Administration is, where are we with respect to implementing the President's Executive Order (EO), the framework, and then what you need from us and why you need it. So, just be ready for that. That will be my first question. Director Comey.

**TESTIMONY OF THE HON. JAMES B. COMEY, JR.,[1] DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE**

Mr. COMEY. Thank you, Chairman Carper, Ranking Member Coburn, and Members of the Committee, for inviting me here today, and most of all for your support of the men and women of the FBI.

As I think about threats to the homeland, I worry most about terrorism and cyber attacks. First, terrorism. I think about our terrorism threat today as a metasticizing threat in two different ways. First, I worry most at home about the individuals we call homegrown violent extremists (HVEs). They are people who are inspired by Al-Qaeda but who direct themselves and equip themselves to engage in their own version of jihad on behalf of terrorist interests. They are certainly encouraged by Al-Qaeda around the world. We have seen Al-Qaeda propaganda already embracing the tragedy at

[1] The prepared statement of Mr. Comey appears in the Appendix on page 59.

the Boston Marathon. And I worry very much that they are inspired also by high-profile attacks around the world on so-called soft targets.

The second aspect in which I worry about the homeland terrorism threat is in Al-Qaeda itself. Although we as a Nation have made great progress against core Al-Qaeda in Pakistan, the threat posed by Al-Qaeda, in a way, has become Hydra-headed, and by that I mean Al-Qaeda affiliates have blossomed and flourished in places around the world, especially in the Middle East and North Africa, and especially there in territories that are ungoverned or poorly governed. Al-Qaeda and its affiliates, as you mentioned, especially Al-Qaeda in the Arabian Peninsula, pose the top terrorist threat to this Nation. They are constantly working to develop operatives and techniques to get past our defenses and wreak havoc in the homeland.

To combat these threats, the FBI relies upon our more than 100 Joint Terrorism Task Forces (JTTF) around the country which bring together State, local, and Federal enforcers to assess the threat and to disrupt the threat before it becomes a reality. And we also work closely through our 60 legal attache offices—more than 60—around the world with the Intelligence Community (IC) and foreign partners to try to press out beyond our borders to identify threats and disrupt them.

With respect to cyber, whether by foreign governments or criminals or activists or terrorists, attacks on our computers and the systems that connect them have become one of the most serious threats to our Nation. As you said, Mr. Chairman, Bob Mueller, my predecessor, testified and also told me privately that he believed that this threat would, during my tenure term, come to eclipse even the threat from foreign terrorism to our homeland. And just based on my 2 months on the job, I believe that he is accurate in that prediction, and the reason is simple.

We have connected, all of us, all of our lives, personal, professional, and national, to the Internet, and that is where the bad guys will go because that is where our lives are and our money, our secrets, and our intellectual property. And they can go there at the speed of light. A trip around the world takes milliseconds on the Internet. And there are no safe neighborhoods. All of us are next-door neighbors on the Internet in the blink of an eye.

In response, the FBI has been working very hard under my predecessor and continues to buildup our capacity to identify and respond to cyber threats, focusing on intrusions, both—our work is done in the homeland and overseas. Here at home, the National Cyber Investigative Joint Task Force (NCIJTF) is a grouping of 19 agencies—intelligence, military, and law enforcement—that have come together to try and assess the threat, deconflict our work, and work in a smart and quick way. A critical partner in that is seated to my right, the Department of Homeland Security, with whom we are working better than ever, and the National Security Agency (NSA). We have different responsibilities and different lanes in the road, but it is essential that we work together, and the good news for the American people is that we are doing that incredibly well.

While national-level coordination is important, the local level is also important to us and so we have stood up Cyber Task Forces

(CTFs) in each of our 56 field offices to focus on cyber intrusions. And just as the JTTFs do, it is to bring together Federal, State, and local enforcers to focus on this threat and to blunt it.

And, as I said, overseas, we are working through 60-some legal attachés to do the same with our foreign partners. We have FBI agents now embedded with police departments around the world, including in Romania, Estonia, Ukraine, and the Netherlands, to identify emerging threats, because these threats know no boundaries and move at the speed of light, and to try to also identify the key bad actors.

But, I should add, as hard as we are working to work better together, it is essential that the private sector work effectively with the government. The private sector is, in almost every circumstance, the victim of cyber crime and cyber intrusions and we need their help to stop them.

And let me finish by just saying a couple of words about how I think you and your colleagues in Congress can help us combat these threats and carry out our mission. When I became FBI Director, I did not know exactly what challenges I would face. I knew it would be a hard job. I have discovered that the challenge that I face most near field is the budget challenge imposed on the FBI by sequestration. I am staring at a situation where I need to reduce almost 10 percent of our budget this year. We are eliminating 3,500 positions and face the prospect of furlough.

We have, as you know, Mr. Chairman, an enormous portfolio of responsibilities for the American people and the challenge of sequestration makes it enormously difficult for us to accomplish that mission. The FBI will always soldier on. We have always tried to do more and more with less. I worry very much, though, we are approaching a situation where we are going to be doing less with less.

With that, I thank you very much for inviting me here today and I look forward to discussing these important issues with you.

Chairman CARPER. Thank you. You said the prospect of eliminating 3,500 positions in this fiscal year?

Mr. COMEY. Yes. We have already done that. Through attrition, we are not hiring, and it was Bob Mueller's plan, which I agreed to, we are going to eliminate 3,500 to get our numbers down.

Chairman CARPER. Additional, on top of what you have already done, or——

Mr. COMEY. He started. He marked 3,500 positions for elimination and I am continuing that. He took out almost $600 million last year and I am taking out over $700 million this year, unless the sequestration cap on us goes away.

Chairman CARPER. And one last quick question and then I will turn to Mr. Olsen. Once the 3,500 positions go unfilled or vacated, how many positions does that leave you in the FBI?

Mr. COMEY. We will be down to where we were in 2009. So, we are now at about 36,000 people. We will be down around 31,000 people.

Chairman CARPER. All right. Thanks very much. OK.

Mr. Olsen, thanks.

**TESTIMONY OF THE HON. MATTHEW G. OLSEN,[1] DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

Mr. OLSEN. Thank you very much, Chairman Carper, Ranking Member Coburn, Members of the Committee. Thank you for inviting me here today. I also want to thank you for your consistent support of the men and women at the National Counterterrorism Center and I would invite you to come out to NCTC and see our operations firsthand.

I am particularly pleased to be here with Jim Comey and Rand Beers. We are close partners in our common fight against terrorism.

It has been just over a year since I last testified before this Committee, and at that time, I pointed to Al-Qaeda core, as Director Comey referenced, really now as a shadow of its former self. That assessment remains true today. At the same time, Al-Qaeda and the senior leaders of Al-Qaeda in Pakistan are a leader, or remain the leader of an ideological movement, and that includes affiliated groups and followers worldwide, particularly in the Middle East and North Africa, and this results in a wide-ranging threat from a diverse and dedicated array of actors.

The recent attack at the Westgate Mall in Nairobi, which was linked to Al-Shabaab in Somalia, illustrates the type of threat we face from around the world: Committed extremists, the availability of weapons, and vulnerable targets. Along with January's attack at the gas facility in Algeria as well as last fall's attack in Benghazi, all of these attacks serve as sobering reminders of the persistent threat of terrorism that we face in these regions of the world.

Today, Al-Qaeda's core leadership in the Afghanistan-Pakistan border region is still really trying to navigate its response to the ongoing events in the Muslim world and working to promote a global jihadist movement. Additionally, unrest in the Middle East and North Africa, most notably in Syria, is creating opportunities for veteran jihadists to recruit and train what may be the next generation of militants, some of whom are less dogmatic in their embrace of Al-Qaeda's ideology but still support an anti-Western agenda, and these developments are really blurring the lines between terrorist, insurgent, and criminal groups operating in these regions.

Here in the United States, the attack on the Boston Marathon highlighted the danger of violent extremism at home, where terrorists who may have no formal or direct ties to Al-Qaeda but still adhere to that ideology can use simple tactics to wreak havoc on innocent victims. As the President observed in his speech at the National Defense University, today, a person can consume hateful ideology, commit themselves to a violent agenda, and learn how to kill without leaving their home.

So, NCTC's mission is to combat these threats both at home and abroad. We examine threat information. We develop leads. We work closely with domestic and international partners. And we develop strategic plans to help unify our efforts.

And as part of these responsibilities, we are coordinating and integrating the Intelligence Community's support, for example, to the

[1] The prepared statement of Mr. Olsen appears in the Appendix 65.

Winter Olympics in Sochi. I was just in Sochi last week and I had the opportunity to meet with Russian intelligence and security officials to discuss the threat picture that we face there and the security preparations for the games.

Closer to home, the dedicated workforce at NCTC works in concert with our partners, particularly FBI and DHS, to protect the homeland, and we are adapting as that threat evolves. I would like to take just a quick moment to share with you some of the measures that we have initiated over the past year.

First, in April, along with DHS and FBI, NCTC established a new organization called the Joint Counterterrorism Assessment Team (JCAT). This is the successor organization to the Interagency Threat Assessment Coordination Group (ITACG), which this Committee helped to establish but which was really no longer sustainable under current budget conditions. What JCAT does is bring together State and local first responders from around the country who come to NCTC to work side-by-side with Federal intelligence analysts to research and produce and share counterterrorism intelligence that is really tailored to the State, local, and Tribal communities, and they do this in an unclassified format as much as possible.

Outside of Washington, we continue to build our Domestic Representative Program. We have representatives in a number of cities now, and we just added Boston and Atlanta. These individuals are intelligence analysts, senior intelligence analysts who work in close coordination with the FBI and the Joint Terrorism Task Forces and the Fusion Centers to bring the national intelligence picture to the local level.

As the April attack in Boston demonstrated, there are times we will have little or no warning when a homegrown violent extremist mobilizes to violent action, and that is why we work closely with the Federal, State, and local officials as well as community partners to raise local awareness about the threat of terrorism as part of our countering violent extremist effort. It is through this whole of government approach that we are collaborating with community leaders to counter radicalization, recognizing, that it is community stakeholders who are best positioned to prevent the exploitation of our youth and to intervene when they spot signs of trouble.

On the pragmatic side, we recognize that we cannot prevent every attack, so we work closely, again, with DHS and FBI to prepare communities should they need to respond. For several years, we have been involved in collaborating with DHS, the Federal Emergency Management Agency (FEMA), and FBI to conduct awareness workshops throughout the United States and help cities assess their readiness to respond to a terrorist attack. One of our first such workshops was in Boston back in 2011, and we think that helped contribute to the effective response we saw in Boston to the Marathon attack.

Finally, to better detect and disrupt plots, we continue to refine and improve our counterterrorism data layer and our analysts' ability to have access to the information that they need to have access to that is collected by other government agencies. And it is our ability to examine a broad range of information, combined with sophisticated analytic tools and the expertise of our analysts, that is

necessary to provide the best all-source collaborative terrorism analysis.

In short, Mr. Chairman, after almost 10 years of service, NCTC has become a center of gravity in our Nation's fight against terrorism and it is our commitment to this team effort with communities throughout the country, with the government at all levels, and with the private sector that is at the core of our ability to identify and prevent the threat of terrorism.

Thank you very much.

Chairman CARPER. Thank you, each of you, for your testimony. Very interesting. Very helpful. Very timely.

The first question I want to ask, as promised, I want to go back to cybersecurity and I am going to ask you to—and you can just weave in and out in responding, but a couple of things I want to hear. How are we doing with the followup on the President's Executive Order? How is the National Institute of Standards and Technology (NIST) doing with respect to working on the framework? How does the private sector feel? What is the kind of feedback we are getting from the private sector as to how that is proceeding?

Describe, if you will, the roles, the interrelationship, the responsibilities, and how you cooperate and collaborate. Just talk to us about your respective roles and how you collaborate. And, finally, how could you work better together, collaborate better, collaborate smarter together? And what can we do to help you in that regard?

So those are a bunch of questions, but I think there is a theme to it, but just give us a good update, if you will. That will probably exhaust my 7 minutes. Thank you.

Rand, do you want to lead it off.

Mr. BEERS. Thank you, sir. Let me start with the Executive Order and the Presidential Policy Directive (PPD). With respect to the National Cybersecurity Framework that the National Institute of Standard and Technology has responsibility for drafting, the first draft of that is completed. It is available. We are seeking comment from the private sector and government officials at all levels as well as, obviously, the Congress. That draft was the result of a number of workshops and outreach efforts that involved both NIST and the Department of Homeland Security in order to find a way to make sure that we brought the best and the brightest together in order to produce this framework. The final framework is due in February and we certainly anticipate meeting that deadline.

In addition to that, we have been mapping the information sharing networks that exist within the government. We have been looking at the National Infrastructure Protection Plan (NIPP) that we are responsible for, weaving cyber and physical infrastructure together, because, obviously, a cyber attack may result in physical damage just as much as it might result in cyber damage.

And all of those deadlines that were set up in the Executive Order have been met up to date. The longest pole in that tent is the science and technology report that we owe in a couple of years. So, with respect to that, I think we are moving forward in line with the expectations.

With respect to collaboration, and obviously, Director Comey will comment on this, as well, what we have basically instituted is a call to any one of us, that is, to the Bureau, to the Department of

Homeland Security, or to the National Security Agency, will be responded to collectively because we each bring a particular expertise and particular activities that I think do allow us to most effectively help an affected business or government entity to respond to an intrusion.

The Bureau, obviously, has the investigative lead, and I will let the Director talk about that. Our responsibility is to, as quickly as possible, know what happened and provide outreach to others that will help them be able to prevent the same kind of an intrusion from happening to them. And the National Security Agency backs us up with all of the intelligence capabilities that they can bring to bear on an event.

With respect to the legislative issue that you asked, I think while we are moving forward as we can with executive authority, we really do continue to need your support in passing that legislation. The areas that we can receive help are, first, on information sharing, to make it easier for private sector firms to share information with us without crossing lines that are of concern to them, for instance, with respect to personal information. We need your help in creating incentives that would help firms adopt higher security practices in cyberspace. The framework will be a good guide on what to do. What we need your help in is helping them realize why they need to do that.

We can also benefit from additional law enforcement tools that were discussed in the draft legislation over a year ago.

We also, as Senator Coburn has mentioned, can use an update on FISMA, as we have at DHS gotten additional responsibilities while the Office of Management and Budget (OMB) remains in the policy lead on this, as well as additional hiring flexibility to allow us to hire in the same way that the National Security Agency can hire cyber expertise.

And, finally, a national data breach reporting requirement so that we can have a national reporting requirement rather than a patchwork of State reporting requirements on personal information. All of those would go a long way and can only be provided by you, the Congress of the United States.

Let me stop there and turn it over to Director Comey on his role.

Chairman CARPER. I have used up about 6½ minutes. I want to be responsible to my colleagues. I am going to come back and ask you to just keep that question in mind, because we will come back in the second round and drill down on it again, so Dr. Coburn.

Senator COBURN. Well, thank you for your testimony.

One of the concerns, if you watched any of the testimony yesterday and the questioning of who I presume to be our new Secretary, it is about transparency and responsiveness. Secretary Beers, we had forwarded to you all on October 18 asking information about the EB–5 system. What the legislative staff here on the Hill did was offer to brief us, and, of course, I do not want a briefing. I want the data and then we will take the briefing after we look at the data.

And the problem has been at Homeland Security with timely responses to Committee requests for information. I think I got a pretty firm "yes" from Jeh Johnson yesterday about being transparent with us as long as we are responsible in terms of what we are ask-

ing for. So I would hope that you would redirect the staff there to give us the information. We have a real problem on EB–5s, both in terms of national security and also fraud, and we need that information.

I have a letter going to Director Comey. It went October 1, along with Senator Chambliss and Senator Grassley, in regards to that same issue, and I would appreciate a response to that.

And then, Matt, we sent you a questionnaire on the Boston bombing—and not only did you all not respond, you did not respond to say—what you told us verbally was that the FBI was answering for you. For us to really have a good working relationship, some of the things that have to happen is communication. And if the FBI is answering for you, you ought to say, "The FBI is answering for us," rather than just not answer us, because all that does is raise the hair on the back of my neck, and I have a great working relationship with you through the Intelligence Committee and I trust you immensely. But just common courtesy would tell us we are going to let the FBI answer that.

Matt, when was the last time you got actionable intelligence from a Fusion Center? Other than Boston. Boston gave you some information. But I am talking actionable intelligence.

Mr. OLSEN. We work with the Fusion Centers really through the FBI Joint Terrorism Task Forces and through, I mentioned in my opening comments, our domestic representatives who work with the Fusion Centers. The Fusion Centers are largely there to support what is happening at the State and local level, and they certainly serve their State and local customers. I have had the opportunity to visit a number of Fusion Centers and they seem to be doing a good job in that regard.

It is not the case, however, that they would typically provide intelligence to, for example, me at the National Counterterrorism Center, where we are focusing more on national-level intelligence.

Senator COBURN. All right. So the point is, they are an all-hazards, mostly State and local initiative, and the fact is, they are mostly funded by Homeland Security. Yet the upward flow of information that is actionable intelligence is almost nothing. And so the question is, could some of those dollars be better used, as far as Federal dollars, at the NCTC or at the FBI, as the Director has said, in terms of what we have seen in terms of sequester.

I just wanted to make the point—you have not gotten any information that is actionable from a Fusion Center and very little of it goes to the Joint Terrorism Task Force, for an investigation. So it is not that—I am against them. It is that we ought to look at what they are really doing, which is mainly local and State, and it has as much to do with drugs and all these other issues that local law enforcement deal with more so than counterterrorism and the terrorism threat to the country.

Let us talk for a minute. One of the things that has to happen on cyber has been referred to, and Secretary Beers, you mentioned this, is the free flow of information from the private sector to you all. And the problem with that is, the liability concerns on private information. So, my question to each of you is: do you think it is proper that any cyber bill we put forward would create a liability

protection for the private sector in terms of sharing information with the government?

Mr. BEERS. Let me start, sir. That is one of the things that we want. Obviously, we want to make sure, together with you, that the liability protection that you are talking about is carefully crafted in order to ensure that it protects activity—information sharing that is legitimate under the terms of that and not a total blanket liability protection. But those are the kinds of things that would help with this so that they are more willing to share that information instead of having a long conversation between lawyers about the terms of the information sharing, which very much slows it down.

Senator COBURN. Right. And nobody is talking about a blanket liability. But the fact is, if a company is at risk, fiduciary risk, with sharing something that the government needs on a timely basis and we have not given adequate liability protection for that, we are never going to get the information on a timely basis. We may ultimately get it, but it will be past the point which we could have utilized it most effectively. Would you agree with that?

Mr. BEERS. Yes, sir.

Senator COBURN. Director Comey.

Mr. COMEY. Yes, Senator, I would. Since I was last in government, I have been the general counsel of two different private companies and so I know the concern in the private sector is that, and then a related concern, which is reputational damage. Will the government keep their information confidential? So they are worried on both fronts.

Senator COBURN. Right. Matt.

Mr. OLSEN. I do not have anything to add to that.

Senator COBURN. OK. Tell me about this National Cyber Investigative Task Force between the DHS, FBI, and NSA. We have had a couple of presentations, most of them in closed session, just so the American public can hear this. I was pretty impressed at the coordination and cooperation that I saw among the agencies, and if any of you would talk about that, I think it would be very good for the American people to see that, government is not always dysfunctional. You guys are really doing some stuff together across department and agency lines, and I think hearing about that would be very reassuring to the American public.

Mr. COMEY. I can say the first word about that, Senator. That was one of the first places I visited as Director, was to go and see the NCIJTF, and it is, as I said, a grouping of 19 agencies that all touch a piece of cyber. Cyber is sort of an evil layer cake. There are State actors trying to steal information. There are terrorists. There are organized criminal groups. There are "hacktivists." There are identity thieves. And there are a huge number of people in government worrying about different pieces of that layer cake, but until the NCIJTF was created, they were all sitting in different places worrying about it in different ways that were inefficient and conflicting.

So what this did was literally pull everybody together, get them all in the same physical place so they could figure out who should work what threat and how should it be worked, and then parse

that work out in the way that is most cost efficient and most effective for the American people.

It is a great news story. A lot of its achievements are things we cannot talk about in an open setting, but I agree with you. I think it is something the American people should be very happy about.

Senator COBURN. All right.

Mr. BEERS. Let me second Director Comey's remarks. It is an excellent way in bringing these people together, in addition to deciding who should take responsibility for a case, but to allow the people at the Task Force, when an incident comes up, to know who may have information about it and to pool that information so that when the lead investigator is determined, that investigator has all of that information.

We have had cases where one or the other of us has been contacted about dealing with something when the other of us was already running a parallel investigation to that kind of activity which provided absolutely critical information to resolving that particular case.

The other thing to keep in mind for the American people is these investigations are really hard because of the difficulty in getting attribution about who is actually doing it. But with dedicated investigators, we have brought down a number of these bad actors.

Mr. COMEY. And can I just add a word, Senator. I have worked a lot of different kinds of investigations in my career, and when you are doing a La Cosa Nostra investigation, you can deconflict by calling each other or setting up a meeting for next Wednesday. When the threat is moving at 186,000 miles per second, as a photon does on the Internet, there is no time to make that phone call. So the advantage of this, the genius of this is the FBI and DHS person are sitting next to each other. So, have you got this? Good. Go with that. We will give you this piece. And they can respond in the way that is needed.

Senator COBURN. Thank you.

Chairman CARPER. Senator Johnson.

## OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman.

I want to welcome everybody here and also thank you sincerely for your service.

I want to talk a little bit about just the actual threat level and the history of it, and so I want to start, first of all, and ask each one of you quickly, when do you believe the current, we will call it War on Terrorism, really began? Where did this all start? Secretary Beers.

Mr. BEERS. Sir, if we are talking about Al-Qaeda, I believe that we really first experienced it with the embassy bombings in Tanzania and Kenya in 1998.

Senator JOHNSON. OK.

Mr. BEERS. We had evidence of them before, for example, in Somalia during the U.S. intervention in Somalia, but that was where it really came to the fore in terms of my own personal experience.

Senator JOHNSON. Director Comey.

Mr. COMEY. I trace the current threat back to the 1980s in Afghanistan, a situation I worry about repeating in Syria, where peo-

ple were getting training and learning and meeting each other, out of which Osama Bin Laden formed the base Al-Qaeda.

Senator JOHNSON. Director Olsen.

Mr. OLSEN. I would agree with both my colleagues. I mean, this is a process that has evolved and we see today the changing threat, as Director Comey described, a metastasized threat. So, it is an evolving threat, but it can be traced back to the 1980s.

Senator JOHNSON. OK. So, my next question is—I realize the answer is going to have to be very subjective, but based on that history, that evolution, is the threat level higher today? I will start with you, Director Olsen.

Mr. OLSEN. It is a complicated answer. The threat level as we look at the threat is more dispersed geographically. The threat has moved out from the Afghanistan-Pakistan border region to broad swaths of areas that are largely ungoverned across North Africa and the Middle East. So, in some ways, it has become more significant from a geographic perspective and more complicated from an intelligence perspective.

I would not say that the threat to the United States of a 9/11-style attack is greater. In fact, I would say it is lower today than it was in 2001. So, the threat of that type of attack today is lower than it was 12 years ago.

Senator JOHNSON. Director Comey.

Mr. COMEY. I would agree with that. I think because we took the fight to the enemy and got our act together in the last 12 years in very important ways, the risk of that spectacular attack in the homeland is significantly lower than it was before 9/11. And what has popped up in its place are these, in the homeland, the risks of the smaller attacks, which are no less, obviously, concerning to us, but smaller, and similar overseas. The Hydra head is less able to attack us in the homeland, so it has pushed more overseas and gotten smaller and more disparate in the homeland.

Senator JOHNSON. Secretary Beers.

Mr. BEERS. I would concur with that and go back particularly to Matt's comment. The dispersion makes it a bigger challenge in terms of knowing what and where things might happen, but the "where" is more likely now to be overseas than it is to be in the homeland, which is not to say that we should drop our guard in any way.

Senator JOHNSON. So, you really do think that the threat is more severe in terms of a worldwide threat coming onto our shore as opposed to the homegrown terrorists, is that what you are saying?

Mr. BEERS. No, that is not at all what I am saying. I am saying, in terms of the consequences of a particular kind of attack——

Senator JOHNSON. It is going to occur overseas as opposed to in the homeland.

Mr. BEERS. The dispersion of the Al-Qaeda brand in North Africa, in Yemen, in Somalia, and in other places, and as it is appearing to manifest in Syria now, means that the kinds of activities that will be undertaken are likely to be undertaken overseas——

Senator JOHNSON. Oh, OK.

Mr. BEERS [continuing]. Rather than directed against the homeland. That is not to say that we still do not face a threat, and it

is certainly not to say that homegrown violent extremists are inconsequential. Far from it.

Senator JOHNSON. I have always felt that our strongest line of defense against any of these threats really is a strong intelligence gathering capability. To what extent has the NSA disclosures—how extensive has the harm been in terms of those intelligence gathering capabilities? Director Olsen.

Mr. OLSEN. I would echo the comments recently of Director Clapper, who characterized them as extremely damaging. There is no doubt that those disclosures have made our job harder. We have seen that terrorists, our adversaries, are seeking to learn about the ways that we collect intelligence and seeking to adapt and change the ways that they communicate in order to avoid our surveillance. So, it has made our job significantly harder.

Senator JOHNSON. How to repair the damage of it? Director Comey. I mean, what does Congress need to do? What do we need to resist, potentially?

Mr. COMEY. Well, I agree with what Matt said about the challenge. Just in 2 months on the job, I have seen changes in terrorist behavior in response to the disclosures about our communications intercept capabilities. I think that Congress just needs to make sure that we do not—if there are changes that need to be made at the margins or in oversight, that we do not make those at the expense of the core capabilities we need as a country.

Senator JOHNSON. Secretary Beers, what is your biggest concern that Congress might do that would just be a huge mistake?

Mr. BEERS. I think Director Comey characterized it. What we need to do is make sure that you are comfortable with the oversight, but not to throw the baby out with the bathwater in terms of lurching too far in terms of restrictions on our intelligence—our ability to collect intelligence.

Senator JOHNSON. Director Olsen, you were talking about going over to Russia for the Olympic games. Can you describe the common interests we may have with Russia? Can you describe a little bit about who really are some solid world partners in this War on Terrorism? Where do we have some common interests?

Mr. OLSEN. We have a number of very close partners around the world in our fight against terrorism, obviously, particularly in Europe and particularly the United Kingdom. In Russia, we face a common threat of violent extremists, and particularly in the North Caucasus area of Russia. So, there is a consistent threat stream coming from violent extremists in that area, from terrorists in that area. They are largely focused on Russian government targets, but, obviously, that is a concern as we approach the Olympics, which will be a very high-profile event in February.

Senator JOHNSON. Just a quick followup. Do you find Russian cooperation increasing or decreasing over the last, let us say, decade?

Mr. OLSEN. I would point to the last several months as a period of increasing cooperation, and Director Comey may be able to speak to this, as well, but since the Boston bombing, there has been an increase in cooperation with Russian intelligence authorities.

Senator JOHNSON. OK. Thank you.

Chairman CARPER. Thank you, Senator Johnson.

Senator Ayotte, welcome. Good morning.

**OPENING STATEMENT OF SENATOR AYOTTE**

Senator AYOTTE. I want to thank the Chairman and the Ranking Member. I want to thank each of you for what you do for our country. You have very important positions in keeping us safe.

Director Comey, I want to ask you about the attacks on our consulate in Benghazi over a year ago, on September 11. I guess the question that I have most of all, that you and I have talked about in the past when we met, why has not anyone been brought to justice? We are in a position now where I have seen public reports of individuals like Ahmed abu Khatalla, who is associated with Ansar Al-Sharia. The reports have been that he has been indicted in New York with others that have not been named, and yet no one has been brought to justice. Can you tell us why?

Mr. COMEY. Thank you, Senator. If charges are brought in a case and they are under seal, it is not something that I could talk about. What I can tell you is this is among the FBI's very highest priorities. I have a lot of people working very hard on it. We are committed to bringing to justice those responsible for the attack and the murder of our folks. These are often difficult cases to make, but as you have seen in our work—we never give up and we will never rest until we bring to justice the people responsible.

The challenge for me is I have twin goals. I want to bring them to justice successfully and I want to make sure that any witnesses I have stay cooperative with us and that the bad guys do not know what I might know or what I might be doing, and so I am limited in what I can say in an open forum.

Senator AYOTTE. Well, one thing that struck me is on October 5, there was the successful raid into Libya to capture Al-Libi, which I congratulate the FBI and everyone who worked, obviously, our military and intelligence agencies, on that capture. And it just led me to raise, of course, in my own mind, when we went into Libya on October 5, if there are individuals that need to be captured, why we would not capture them then, as well. And I know that may not be something you can answer in an open setting, but people are frustrated that these people have not been brought to justice. So, I do want your commitment that they will be brought to justice.

Mr. COMEY. You have it. I think the Al-Libi case, I hope, illustrates for the American people what I said before. We will never stop and we will never give up. He has been wanted, as you know, for well over a decade. So, the work will continue.

Senator AYOTTE. Well, let me ask you. Are you getting cooperation from Libya on this issue of capturing and seeing that those who committed the attacks on our consulate are brought to justice?

Mr. COMEY. I do not want to talk in particular about particular operations or particular conversations, but I think as we have said publicly, the Libyan government has been cooperative with us in this investigation.

Senator AYOTTE. Well, we expect them to be cooperative with everything, obviously, we have done and the support we have given them.

Let me ask you, in terms of the Al-Libi capture on October 5, as I understand it, he was captured on October 5, placed on a ship, and then was interrogated for—this is according to all public infor-

mation, now he has been publicly indicted—until the 12th, in which he was brought into civilian custody, is that right?

Mr. COMEY. I do not know the exact dates, but the general——

Senator AYOTTE. So, it is about a week of interrogation?

Mr. COMEY [continuing]. General contours sound right.

Senator AYOTTE. So, Mr. Beers identified the beginning of Al-Qaeda as the attacks on our embassies in Africa, and, of course, Al-Libi has been charged with those attacks on our consulate. He was a very major capture, was he not, of Al-Qaeda?

Mr. COMEY. He is alleged to be one of the founding fathers of Al-Qaeda.

Senator AYOTTE. That is right. So, yesterday, we had the nominee to take over for Mr. Beers, Jeh Johnson, and he described interrogation as a treasure trove, as an opportunity, of course, for us to gather information and protect our country. You would agree with that, would you not, Director Comey?

Mr. COMEY. Yes.

Senator AYOTTE. Was 7 days enough, long enough interrogation, in your view, to find out everything that Al-Libi knew about Al-Qaeda and its operations?

Mr. COMEY. I do not want to comment on the particular case. Longer is always better. More is always better. Interrogation, I agree with Jeh Johnson. Interrogation is a critical tool and is often a treasure trove——

Senator AYOTTE. So, here is our conundrum. Here is the problem we face. Let us take it out of Al-Libi for a moment. He was put on a ship instead of being brought to Guantanamo because, obviously, this has been a policy, political decision of the Administration of not wanting to put anyone in Guantanamo. But, is it practical that we can put everyone on ships, of his nature?

Mr. COMEY. That is a hard question for me to answer.

Senator AYOTTE. Well, I guess the question I have is, tomorrow, let us say we get Zawahiri. Let us say we get the current titular head, Ayman Al-Zawahiri, tomorrow. Where do we put him? You need to interrogate him, not only you, but our intelligence officials to protect our country. What do we do with him? I would hope that we are not going to only interrogate him for a week, so do you know what we do with him, where we detain him, how he is treated?

Mr. COMEY. I do not in particular. I am aware of a variety of options. My goal would be just what you said, to have our agents and our Intelligence Community colleagues have the opportunity to interrogate him to get that information.

Senator AYOTTE. Do you think he should be Mirandized?

Mr. COMEY. Who are you asking about? I am sorry.

Senator AYOTTE. Zawahiri. If we get Zawahiri tomorrow, when we capture him, do you believe that he should be read his Miranda rights?

Mr. COMEY. Well, I, as my predecessor did, believe that the more flexibility we have to delay the reading of those rights, the better. But, again, the reason I am hesitating is it would depend upon where he is and whether there was a court case pending against him and all those kinds of things. But, sure, the more flexibility, the better for us.

Senator AYOTTE. And that is because, obviously, you capture a known terrorist, someone who is the head of Al-Qaeda, you tell him he has the right to remain silent, that obviously could have the potential to interfere with your interrogation, is that right?

Mr. COMEY. Sure. It would end the interrogation. And in situations like that, it is not that I am looking for confessions to be able to use in a court——

Senator AYOTTE. No. You are using——

Mr. COMEY. I am trying to get intelligence——

Senator AYOTTE. You are looking for information to protect the country, right?

Mr. COMEY. Exactly.

Senator AYOTTE. And that is different than gathering—certainly, they can be concomitant and together, but the priority has to be in gathering information to protect the country, is that right?

Mr. COMEY. Sure, and that is the way we approach it.

Senator AYOTTE. Well, the one thing I will just say is that I worry about the Zawahiri situation, because right now, the Administration has chosen not to use Guantanamo. The Administration is putting people on ships. But Al-Libi, to only interrogate someone like that for 7 days, it seems to me that we are losing opportunities to gather intelligence. And I hope that—Director Comey, you are new to this position—that we can work on a policy for detention and interrogation that will allow you to fully interrogate the worst terrorists that continue to pose threats for our country. So, I thank you all for what you are doing.

Mr. COMEY. Thank you, Senator.

Chairman CARPER. Thank you, Senator Ayotte.

I want to return to my earlier question. Secretary Beers, you had a chance to respond to it. We are under cyber attack every day. It is not just something that could happen. It does happen, and it happens in a lot of different ways and a lot of different directions.

I want to come back to it, and my original question, Director Comey and Mr. Olsen, was are you guys working together? How well are your agencies working together? What are you doing better than you were? Where can you do better still? How can we help? Please.

Mr. COMEY. I think two things that I could add to the answer that Rand Beers gave you already, one is I agree very much what we are doing better together is talking to each other and sharing information very quickly so that we can discharge our responsibilities quickly. So that is my first response.

My second response is, it is our need to get information from the private sector quickly that is critical. Otherwise, we are patrolling—I picture us as police officers patrolling a street where the walls on either side of the street are 50-feet high. We can make sure that the street is safe, but we cannot tell what is going on in the neighborhood. That neighborhood in my metaphor is all the private networks and all the private companies that are the victims of these attacks. So, we need to find a way to lower those walls so that we can learn the information we need quickly to be able to respond to the attacks. That is what we could do better.

Chairman CARPER. How can we help?

Mr. COMEY. Well, I think, as Secretary Beers said, I think one of the things that is very important is to create incentives for private companies to cooperate, to address their concerns primarily about liability, and second, their concerns about their reputation. And so I think that liability issue sits with Congress that can offer them that protection. So, I think that is very important.

Chairman CARPER. Talk more about that liability protection.

Mr. COMEY. Well, private companies are concerned that if they turn over information, they will end up getting sued by people whose personal information may be somewhere in the data they supply, or competitors may complain about them turning it over, or that it will be used against them in some fashion in a government contract competition down the road. And all of these things make their general counsels, which I used to be, say, great idea. We really want to share. We do not want to hurt the stockholders of this company by sharing, so what is our protection? That conversation just took me 10 seconds to say it. That is a several hour conversation inside any company. In the meantime, that threat, as I said, has moved at the speed of light, and so that is just not sustainable.

Chairman CARPER. What are a short menu of options that we should consider in addressing those liability concerns?

Mr. COMEY. I do not think I am expert enough in the pending legislation to offer you a specific view, so I would defer to Secretary Beers, who I think knows it better than I.

Chairman CARPER. Is that true? Do you know better than he does?

Mr. BEERS. I have been at it longer, Senator.

Chairman CARPER. All right. Do you want to take a shot at that, a menu of options for us to consider on the liability side?

Mr. BEERS. Well, as explored with Senator Coburn, I think what we need is for the liability protection to create the willingness for the private sector to share information about a data breach as soon as they experience it, so that we can help them as quickly as possible and we can protect others as quickly as possible.

So, how the liability protection is constructed, I am not a lawyer. I cannot define that in the legal terms that you all need to put into the law. But I certainly would be ready and willing to help with technical assistance on trying to define precisely what that ought to look like, as we tried earlier on with the last attempt to write the legislation in this body.

Chairman CARPER. All right. Mr. Olsen.

Mr. OLSEN. I do not have anything to add on the cyber legislation.

Chairman CARPER. All right. Thank you.

Let us talk a bit about the lone wolves, the folks, American citizens in many cases, who become radicalized, in some cases by traveling abroad, being exposed to jihadist activities, in other cases just being radicalized here, over the Internet or maybe in their own communities. I worry a lot about that. I know you do, too. Share with us what we are doing to try to address that threat and how you are working together. How can we help you?

Mr. BEERS. Let me go ahead and start. In addition to the great investigative work that the Bureau does, the three of us, along

with the Department of Justice leadership, have a regular dialogue among ourselves about how to craft a common approach to assist in the identification of individuals, the prevention of them carrying out their acts.

We do this under three large categories of activity. The first is to look at all of the events that have occurred and see what transpired in those events so that we can create a body of knowledge about behaviors and indicators that can inform us and State and local law enforcement and citizens of what kinds of indicators might provide us with a warning of an event.

We then take that information and provide it to all of our law enforcement partners. We conduct training in association with that. We conduct exercises in association with that. And we, as Matt Olsen indicated, that is not just before the event, but also what do you do after an event has begun to occur. All of the active shooter training that we do is designed to assist in that, although it is a much broader resonance in terms of those kinds of events.

And then the last is community engagement, to talk to people in the communities, to hear what their concerns and issues are and to provide that information to them, as well. And all three of us participate in that effort, either as individual agencies or in concert with one another. That is the broad scheme of how we work together.

Chairman CARPER. All right. Director Comey, would you add to that, please.

Mr. COMEY. The only thing I would add is that with respect to the travelers—in some ways, the travelers are easier for us—they are still a huge challenge—than the homegrown violent extremist who stays in his basement the whole time, radicalizing himself through the Internet. There, it is a huge challenge, as Secretary Beers said, trying to develop a set of indicators. What are we looking for? What should we equip the police officers patrolling that neighborhood to look for? So, that is something we are focused on.

The travelers, we can see them come in and out of the country, and so figuring out smart ways to assess what they are doing and to have conversations with them that are useful to us is something we are working together on.

Chairman CARPER. Good. Mr. Olsen.

Mr. OLSEN. If I could just really echo the comments of my colleagues. I mean, the challenge of the homegrown violent extremist is exactly as Director Comey described. This could be an individual who does not travel, does not communicate, maybe a passive consumer of radical information on the Internet, so really does not hit any of the trip wires that help us discern when somebody is mobilizing to violence.

So, we are working closely together as a team to implement the strategy. The strategy has the three broad categories that Rand Beers laid out—engagement, training and expertise with State and local law enforcement, as well as countering the Al-Qaeda narrative.

We talked a minute ago about Fusion Centers. Fusion Centers do provide a very good way for us to help develop the expertise at the State and local level. Around the country, there are a million first responders between the police officers and firefighters. Those are

the individuals who are going to be most likely to see someone who is on that path from radicalization to mobilization. And helping equip them with how to find those signs is a key part of the strategy.

Chairman CARPER. All right. Thanks. My time has expired.

Let me just ask you, take 10 seconds apiece and answer this question. If somebody sees something—they are saying, see something, say something. If someone sees someone that they believe is being radicalized in their own community, maybe in their own family, who should they say something to? Rand.

Mr. BEERS. Usually, the first instance is the local law enforcement agencies.

Mr. COMEY. I Agree, and I would urge people, listen to that feeling on the back of your neck and do not write an innocent narrative over facts that initially strike you as strange. Just tell somebody.

Mr. OLSEN. And if I could just add, a key element of this is to build trust with those communities, particularly the American Muslim community, so they have the confidence and trust in our law enforcement agencies to, if they see something that gives them concern, to come forward.

Chairman CARPER. All right. Thanks so much.

Senator Levin, it is good to see you. You are recognized.

**OPENING STATEMENT OF SENATOR LEVIN**

Senator LEVIN. Thank you very much, Mr. Chairman.

Director Comey, let me start with you. The law now does not allow detainees to be brought from Guantanamo to the U.S. for detention and trial. Should this law be changed?

Mr. COMEY. That is——

Senator LEVIN. Should we allow people to be brought from Guantanamo to the U.S. for detention and trial? Can they be properly tried? Can they be safely detained?

Mr. COMEY. The policy question, I think, Senator, is one better answered by the Department of Justice. I know from my personal experience, though, terrorists can be safely detained and tried. I have been involved in many cases myself in civilian courts in the United States. So, that part, I can definitely answer and the answer is yes.

Senator LEVIN. Well, what is that personal experience?

Mr. COMEY. Well——

Senator LEVIN. More specifically, have we tried individuals for terrorism in Federal courts?

Mr. COMEY. Many we have. I was the U.S. Attorney in Manhattan after September 11, 2001, and we had cases pending then. We are very good in the United States at safely detaining bad people with all kinds of threat. We are successful in detaining them. The Bureau of Prisons, I used to supervise when I was Deputy Attorney General, and there is nobody better in the world. And our courts are, as they have proven in a track record going back to probably the largest case was the initial East Africa bombings case brought in the Southern District of New York, which was tried, and it is actually the case that Al-Libi was just arrested on. It is a long track record.

Senator LEVIN. Now, are trials that are held in Federal court more likely to be conducted in a speedy manner compared to trials before military commissions?

Mr. COMEY. I do not have enough experience—I guess we do not as a country—with the military commissions for me to say about that. So, what I can say is I do know the Federal courts have long been able to move these cases, protect classified information, and get them done in a reasonably prompt time.

Senator LEVIN. Now, the argument has been made that this bringing terrorists to trial, either directly for trial in the United States or from Guantanamo, somehow or other creates a security threat for those communities in which they are held. Do we have any evidence to support that kind of a conclusion?

Mr. COMEY. I do not know of any, Senator, with respect to a threat created in the area of a prison facility. Our ADMAX, our supermax prison in the high desert in Colorado, is fairly remote. I do not know of any threat surrounding that facility. We have housed in that facility some really bad people for a long time.

Senator LEVIN. And, Mr. Beers, is there any position that DHS has taken about any security threat from trying and detaining terrorist defendants?

Mr. BEERS. Sir, I do not have any information indicating any significant threat to a particular trial that has taken place.

Mr. OLSEN. Senator Levin, if I may, just to jump in for a moment here, I would want to fully endorse Director Comey's comments about the Federal courts. I share, at least in part, the experience of having been a Federal prosecutor and the ability of our Federal courts to handle these cases.

And the one element I would add is—what we have seen in certain cases, in certain important cases, is the ability to obtain intelligence information from individuals who are brought into that system. From my perspective at the National Counterterrorism Center, of course, it is very important that we do whatever we can to gain that intelligence, and we have been able to do that in a number of important cases where individuals have been cooperative and provided important information.

Senator LEVIN. Is there any evidence—or maybe, Director Comey and others, you can compare the kind of intelligence both in terms of quantity and quality that the FBI has been able to obtain from terrorist suspects compared to their being held by other elements of our Federal Government.

Mr. COMEY. Senator, I am not in a position to compare because I do not know enough about the track record in getting information by other agencies, so I can only speak to the FBI's, which is long, and it is one of the things we do best, is get information from people, especially bad guys.

Senator LEVIN. And is that also consistent with the guarantees in the law for interrogation of suspects?

Mr. COMEY. Absolutely.

Senator LEVIN. Let me ask you a question, Director, about a bill that Senator Grassley and I have introduced relative to U.S. States and the United States incorporating entities that have hidden ownership. Is there a problem from a law enforcement point of view in not knowing the real owners of corporations? In this regard, I think

you may be familiar with what happened at the G–20 summit, where 20 leaders, including President Obama, reached a consensus that it was time to stop creating corporations with hidden owners, and President Obama has issued a National Action Plan which calls for Federal legislation, such as we have introduced, to require our States to include on their incorporation forms a question asking for the names of the real owners of the corporation being formed.

Now, do you support that bill? Does the FBI want to know the real owners of corporations? Is there a law enforcement purpose, because we have had all kinds of letters from law enforcement groups, Federal Law Enforcement Officers Association (FLEOA), Fraternal Order of Police (FOP), Assistant U.S. Attorneys Association, on and on, saying it is critically important that you know the beneficial owners of corporations because, otherwise, suspected terrorists, drug trafficking organizations, and other criminal enterprises continue to exploit the anonymity afforded to them through the current corporate filing process. That is quoting the letter from the Federal Law Enforcement Officers Association.

Do you support, as Director of the FBI, our passing a bill which would require States to ask one question on the incorporation forms: who are the real owners, who are the beneficial owners of the corporation that you seek to incorporate? And if you do support it, will you tell us why?

Mr. COMEY. I do not know enough about the bill in particular to have a position. I am sure the Department of Justice is working on it. But I agree with your premise. It is very important to our investigations across a whole range of cases to be able to learn that information.

Senator LEVIN. Why?

Mr. COMEY. Because——

Senator LEVIN. Give us examples. Why does it make a difference in law enforcement?

Mr. COMEY. Well, if you are conducting an investigation of a transnational organized crime group that is involved in human trafficking or drug smuggling and they are laundering their money through a particular corporate entity, connecting that entity to the bad guys is going to be a critical step in your investigation. I mean, and you could take that and make it an analog in any different kind of a terrorism financing case, a bank fraud case, a Ponzi scheme. All of those require you to find the people who are hiding behind particular names or shells.

Senator LEVIN. Thank you. My time is up.

Chairman CARPER. And just to followup on the question, that exchange that you just had with Senator Levin, this is an issue that he has pursued for some time. And, interestingly enough, the States are uncomfortable with the manner that it has been pursued. The States, especially the States that have expressed their concern through their Secretaries of State, and we have encouraged our own Secretary of State in Delaware to work with, partner with other Secretaries of State across the country to meet with the FBI, engage in a conversation with the FBI and other law enforcement agencies to find a way that addresses the concerns that Senator Levin has expressed and that you, and I think many Americans,

would share, but to do so in a way that the States do not find overwhelmingly difficult to administer. I think there is a sweet spot there and there is a negotiation that has begun. We appreciate the participation of the FBI and other law enforcement agencies in that discussion.

Back to Senator Coburn.

Senator COBURN. Thank you.

Director Beers, you mentioned a minute ago the National Suspicious Activities group—what was the full name of that?

Mr. BEERS. "National Suspicious Activities Reporting Initiative."

Senator COBURN. This morning, a news article broke that 4,904 people, personal Social Security numbers, addresses, and professions, and lots of other detail came out of the DHS, whose Customs and Border Protection (CBP) was leading an investigation on some information about how to get around a lie detector test and a book that was sold. And if you read this report—I do not know if you are familiar with this or not——

Mr. BEERS. No, I have not seen it, sir.

Senator COBURN [continuing]. But I would tell you, this is really concerning to me. First of all, it looks sloppy on its face in terms of the number of people. And what I would direct you to is today's McClatchy news story.

But this is the kind of thing where, because it is not done right, it looks to be very inappropriate. As a matter of fact, in the story, it is quoted that the agencies will keep this information for long periods of time on these individuals, and the American people are going to want to know why and what did they do wrong. Because they wanted to read a book, now the Federal Government has shared all our information with 20-some other agencies, including our personal data.

I think there is a balance to where we are going and I would love for you to both brief my staff and also respond to this news story, if you would, later today. I know I am catching you off guard, but we need to protect ourselves, but we also need to protect the Fourth and First Amendments. To me, on the face—and I will reserve final judgment until I hear from you—this is way overboard and way beyond, and I would hope you would address this.

Director Comey, as you know, Senator Graham has held up and is holding up all nominations of the President coming before the Senate because, in his opinion, the Congress ought to have the right to interview and discuss what happened in Benghazi with the survivors. That has been resisted. And I have two questions for you. No. 1 is why does the Congress not have the right to do that? And No. 2 is, is Senator Graham inappropriate in trying to have the American people know what happened in Benghazi by interviewing those survivors?

Mr. COMEY. My reactions are, I do not know. This is the first question. And no as to the second question. It does not strike me as inappropriate. As I said in response to an earlier question, my interests are in making sure that we balance the FBI's need to be able to protect our witnesses and find those people and bring them to justice, but I do not see anything inappropriate with the inquiry.

Senator COBURN. Well, but it is my understanding he has been told he cannot interview those survivors. Is that correct?

Mr. COMEY. Certainly not by me. I do not know. I——

Senator COBURN. The FBI has no problem with Congress interviewing the survivors of Benghazi?

Mr. COMEY. No.

Senator COBURN. All right. Thank you.

One of the concerns that I hear from the private sector, Secretary Beers, on the Executive Order—and, by the way, I compliment the President on his Executive Order on cyber. I think they listened well. They built a good plan. And, so far, it has been executed very well. So, I congratulate him and you on what has been done on that.

But, one of the concerns is about what is coming with the Executive Order in terms of regulations, one of the things that I believe is stifling our economy now, is just tremendously excessive, and if we want private data shared with the government so we can actually protect us. Do you have any concerns on that part, or do you have any feel for what we are going to see in terms of regulations?

Mr. BEERS. Sir, at this particular point in time, as we negotiated the original cyber bill that was considered in this body and in this Committee, it was not our intention to seek regulation in association with that. It was a very light touch. I think that remains our posture with respect to going forward. The part of the Executive Order that seeks to catalog regulatory authorities is an effort to pull that together to see what authorities do currently exist that allow regulation that is already underway——

Senator COBURN. You would——

Mr. BEERS [continuing]. And see where we go from there. We have not completed that particular——

Senator COBURN. You would agree that voluntary compliance, if people were made aware of it and made aware of the benefits of it, is a better scenario than forced compliance, or at least forced compliance should come after we see a failure of voluntary compliance? Would you agree to that?

Mr. BEERS. Yes, sir.

Senator COBURN. All right. Thank you. I have no further questions.

Chairman CARPER. Senator Johnson.

Senator JOHNSON. Thank you, Mr. Chairman.

I would like to followup on questioning by both Senator Ayotte and Senator Coburn on Benghazi. Director Comey, for 14 months, it has been the consistent excuse of this Administration that the reason Members of Congress do not have access to the survivors of Benghazi is because of the FBI investigation. I mean, you are aware of that, correct?

Mr. COMEY. I am not, Senator. I am not.

Senator JOHNSON. So, just getting back to what Senator Coburn said, there should be no reason that the FBI investigation should be used as an excuse for us not to have access to question those witnesses, whether it is in an open hearing or in a secure briefing setting?

Mr. COMEY. As the FBI Director, I do not have an objection to it. I do not know whether the prosecutors would feel differently or there is some other reason I am not thinking of, but speaking from my perspective, yes, I do not have an objection to that.

Senator JOHNSON. Director Olsen, I would just like to talk about the difference between our desire to prosecute and the difference between gathering intelligence. I mean, from my standpoint, with the threats that you are far more aware of than I am, to me, it sounds like intelligence gathering is a far higher priority than bringing people, I guess, to eventual justice, particularly when we can hold them as unlawful enemy combatants. Can you just kind of discuss the difference between the desire to prosecute, which we all want people brought to justice, but the need, the absolute requirement for intelligence gathering?

Mr. OLSEN. I think there is no conflict in that. In other words, from everything I have seen in my work at the National Counterterrorism Center and before, the No. 1 goal in any of these instances involving terrorist suspects is to gather intelligence. That is the overriding objective. At the same time, we need to have an option for disposition, and with respect to, for example, Abu Anas Al-Libi, who we discussed, this was an individual who was indicted and where a disposition option was readily available in the Federal courts. But every case is different and every case is treated on the basis of the facts presented, and in every case, intelligence gathering is the priority, and that is what I have experienced——

Senator JOHNSON. I made a trip down to Guantanamo with Senator Ayotte and we spoke to the people they are continuing to interrogate over a very long period of time, the detainees down there. The very strong opinion of those individuals doing those interrogations say that the most effective interrogation occurs over years, where you gain their confidence, and slowly and surely you obtain the little threads of information, the types of threads that, I think, eventually led to the killing of Osama Bin Laden. Do you disagree with that? I mean, to me, I think it is absurd that we think we can actually gather the types of intelligence that is possibly there in a week on a ship, or a couple days before we Mirandize somebody. Do you disagree with that?

Mr. OLSEN. I mean, as a general proposition, I think it is clear that the longer opportunity we have to gather intelligence, to interrogate someone, the better. There are——

Senator JOHNSON. So, do you not believe we really ought to be using that absolute first class facility down in Guantanamo to detain these individuals so we can gather the type of intelligence we need?

Mr. OLSEN. I mean, in every case, there are going to be other considerations that are going to come into play, and that, in fact——

Senator JOHNSON. Any higher consideration than gathering the intelligence we need to keep the homeland safe?

Mr. OLSEN. There are going to be other considerations, and that was, indeed, what was in play with Abu Anas Al-Libi. So, again, though, the No. 1 goal is to gather intelligence, and that is what I have seen in these cases.

Senator JOHNSON. OK. Well, I wish that were the top priority. It does not seem to be so.

Secretary Beers, on May 23, 2012, we held a hearing in this Committee on the very unfortunate events in Cartagena. We were pretty well led to believe by the then-Director of the Secret Service

that was a one-time occurrence. I really wanted to believe that. I think it is incredibly important that the Secret Service has total credibility and that their important mission of securing high government officials and national security information is paramount. In my capacity as Ranking Member on a Subcommittee that had oversight of that, we continued to dig into exactly what happened in Cartagena, hoping it was a one-time occurrence. It does not appear that it was.

We have, through whistleblower accounts, found out that similar instances occurred in 17 countries around the world. And, again, that is just a limited snapshot. We have had very limited access to individuals that might know better. Just the other day, two Secret Service individuals were disciplined for sexual misconduct in a hotel here in Washington. One of those men, Ignacio Zamora, we have come to find out actually was involved in the Cartagena incident and interviewed Secret Service personnel.

The question I have for you is we have been waiting for a culture report from the Inspector General's (IGs) office now for 18 months. Do you know when that culture report will be released?

Mr. BEERS. Sir, I do not have a specific date. I know that it is near completion and we are expecting it shortly. But I cannot give you——

Senator JOHNSON. Do you think 18 months is kind of an inordinate amount of time to take to determine something I think is so critically important, to find out whether there is a real cultural problem in the Secret Service?

Mr. BEERS. Obviously, we would prefer to have the report sooner rather than later, sir.

Senator JOHNSON. Can I get your commitment to check into that and get that report completed and released as soon as possible?

Mr. BEERS. Yes, you have it.

Senator JOHNSON. OK. Thank you. No further questions, Mr. Chairman.

Chairman CARPER. Dr. Coburn, please.

Senator COBURN. I just had one other thought. As we went through the Boston Marathon bombing and we look at the Tsarnaevs, the one thing that was never covered is the parents came here under an asylum visa, except the parents are back home and have been for a number of years. Has anybody looked at our techniques, processes, requirements for granting asylum to individuals, because, obviously, with the ability to return home to their home city from which they were granted asylum in the first place, something has changed. Either we got it wrong or something markedly changed in Chechnya. I do not think that is the case. So, has anybody looked at that? And I know that is a State Department issue probably more than Homeland Security, or maybe it is not. Any comments on that?

Mr. BEERS. Sir, let me start. The Tsarnaev family sought asylum from Kyrgyzstan, where they had moved to avoid the violence in their home area of Dagestan. Their request for asylum was that they were being discriminated against in Kyrgyzstan for being from Dagestan and that was the basis of the initial granting. So, that was the way that it happened, and then they, as you quite correctly say, chose later on for presumably personal reasons to go back to

the place that they were actually from, that they were actually born in. Those are the facts of the case.

With respect to the asylum, yes, we are looking at this as a regular issue, since DHS is a participant in the granting of asylum, because, in part, it leads often to legal permanent resident status and naturalization. So, we are very much a part of that.

Senator COBURN. All right. Thank you very much.

Chairman CARPER. Senator Ayotte.

Senator AYOTTE. Thank you.

Director Comey, I wanted to followup on a discussion that we had on the JTTF and the Memorandums of Understanding (MOU), because when Commissioner Davis had testified before our Committee about the Boston bombing, and I think all of us agree that there was great cooperation there and the Boston Police Department did a phenomenal job, along with the Federal partners, he had some concerns about how the MOU was operating, and you and I talked about that, and I wanted to followup with you on as to where we are with the communication on the JTTF for the Memorandum of Understanding. He was concerned that his local officers, the information was not flowing downward.

Mr. COMEY. Thank you, Senator. Yes, that is a concern that we have been discussing with the major city chiefs and the sheriffs. I had a lunch meeting last week with them to followup on that. So, it is a work in progress, but I think we are going to—our goal is to, when you and I discussed, which is to make sure there are not impediments, either real or perceived, and so his concern is being acted on. I do not have a date for when it will be done, but it will be very soon.

Senator AYOTTE. Good. I would very much love if you would report back to the Committee to just give us that answer, because I know it is an issue that is of importance to you, just so we know that this is operating and the information is flowing correctly downward and upward.

Mr. COMEY. Sure. I will.

Senator AYOTTE. Thank you. Also, Mr. Olsen, I wanted to ask you about your testimony. You mentioned something about the withdrawal of coalition forces from Afghanistan could enable core Al-Qaeda veterans to reconstitute there. Right now, the Administration, we are in a key moment with regard to what happens in Afghanistan, decisions that are going to have to be made on what the follow-on force will be in 2014. And so I guess I want to hear from you, does it matter? I have heard some people say, what can we accomplish there, and I was intrigued by what you said because I share the belief that we could have a reconstitution of Al-Qaeda or other terrorist groups there. So, could you enlighten us on that.

Mr. OLSEN. I mean, I think from an intelligence perspective, we are concerned about Afghanistan and Pakistan and the border region, no doubt, because of the presence of extremist groups, including the remnants of core Al-Qaeda in that region. We have seen that there has been an interest in Al-Qaeda in parts of Afghanistan, particularly Northeastern Afghanistan, and it is just going to be an issue that we are going to have to monitor very closely after 2014 to see what types of activities Al-Qaeda or other allies of Al-

Qaeda, for example, the Haqqani network, undertake in that region.

Senator AYOTTE. And, in fact, have we not seen reactivity by Al-Qaeda, or activity by Al-Qaeda in Iraq with what is happening there right now. We were not able to come to an agreement on a follow-on force in Iraq and now we are certainly seeing some follow-on there. Can you describe that?

Mr. OLSEN. Sure. Senator, we have seen an uptick over the last several months in violence in Iraq, much of it, we believe, perpetrated by Sunni extremists in Iraq, almost all of it focused on Iraqi targets, not U.S. targets necessarily. But, certainly, there has been an uptick in the violence in that country.

Senator AYOTTE. And we certainly want to avoid the scenario where Afghanistan becomes a launching pad for terrorists again, do we not?

Mr. OLSEN. Absolutely.

Senator AYOTTE. All right. Thank you all.

Senator COBURN. [Presiding.] Senator Levin.

Senator LEVIN. Thank you. I just have a few more questions.

Director, you indicated that you do not have a personal problem with Congress interviewing the witnesses from Benghazi but that you have not talked to your prosecutors, is that what you said?

Mr. COMEY. I do not know. I have not discussed it with the Department of Justice to see whether there are separate concerns about—from the Assistant U.S. Attorneys handling the matter about it. And when I said witnesses, I thought the question was about the survivors, which are the U.S. personnel who were there.

Senator LEVIN. Correct.

Mr. COMEY. Yes.

Senator LEVIN. Is it possible that you would have a different opinion if you talked to those prosecutors?

Mr. COMEY. It is always possible, sure.

Senator LEVIN. OK.

Mr. COMEY. I do not know.

Senator LEVIN. My other question has to do with going back to the beneficial ownership issue of corporations and the national security problems that are created when we do not know who owns the corporations. We have some, apparently, testimony or some indication from some of the Secretaries of State that the FBI could obtain—and other law enforcement agents could obtain corporate ownership information from the Internal Revenue Service (IRS) on a form, I guess it is called SS–4, but the corporations have to fill out those forms to get a U.S. Taxpayer ID Number. Does that work from the FBI's perspective, to try to get the important information that you described from the IRS instead of from the applications for corporate incorporation?

Mr. COMEY. I do not know enough to say, Senator. I just do not know.

Senator LEVIN. So you are not familiar with the argument that the FBI could get that information from the IRS?

Mr. COMEY. I am not.

Senator LEVIN. Thank you. Those are the only questions that I have, and I just want to thank you all.

Mr. OLSEN. Senator Levin, if I could go back to your question with respect to Benghazi, the one point I would like to offer to the Committee is over the course of the last year and several months since the Benghazi attacks, we have presented a number of briefings to Members of this Committee as well as a number of other members, probably over a dozen briefings that presented a multimedia presentation, including surveillance video, overhead imagery, witness statements describing every facet that we had from an intelligence perspective about those attacks. So, we have had a number of opportunities to present everything that we know from an Intelligence Community's perspective about the attacks in Benghazi. We would certainly offer that again if the Committee was interested in seeing that.

Senator LEVIN. Well, I was just curious about the Director's comment about not having talked to the prosecutors and whether or not that might impact his opinion as to whether or not for some reason Congress should not have access to those survivors. I do not know of any reason, either, by the way, I have to tell you. I think this whole thing has been not handled appropriately, but that is not the point. The point is, I do not see any reason myself why Congress should not have access to anybody Congress wants to have access to. Whether it has overdone it or not, I will leave that up to my own personal opinion and to others to resolve. But, I do not have a personal problem, either.

But, I, sure as heck, if I knew prosecutors had a problem with it, I would want to hear their view before I reached my conclusion. I was kind of surprised that the Director said, well, it is his opinion that there is no problem, but the prosecutors may have a different approach. So, that was the reason I was pressing the Director on this issue, and I can leave it at that.

Going back just to clarify one question about some of the positions that Secretaries of State have taken about the FBI going to the IRS to get the beneficial ownership information, would you find out and give us an answer for the record as to whether or not the FBI believes that is a satisfactory alternative to knowing the beneficial owners from the incorporation documents? Would you let us know for the record?

Mr. COMEY. Sure, Senator.

Senator LEVIN. Thank you.

Chairman CARPER. [Presiding.] All right. I have a couple of closing questions, and then I will give you an opportunity, if you want, just to make a short closing statement of your own, so think about that while I ask these questions.

Probably most Americans are concerned about their personal security in this country, either from crime in their own communities or own States or the threat of a terrorist attack. I think people are more mindful of the threat of cyber attacks than they have ever been, and we are reminded of those threats every day. People in this country are also concerned about their own privacy and the ability to have their privacy protected, and sometimes there is a tension between those two desires. We all want to be safe. We also want to make sure that our rights to privacy are protected.

Please talk about the tension that exists between those two rights and concerns and how we are trying to strike the right balance, please. Mr. Olsen, do you want to go first.

Mr. OLSEN. Sure. This is an issue, obviously, that is front and center today, and I can assure you, Mr. Chairman, and the Committee that it is an issue that is part of what we think about every day at the National Counterterrorism Center, and I know it is true from my experience at the other places I have worked, including the National Security Agency and the Department of Justice.

Particularly with respect to where I am now, at the National Counterterrorism Center, we are charged with the responsibility of preventing terrorist attacks. We do that by integrating and analyzing information. We understand that we need to have access to a lot of information, government-collected information, in order to do that, in order to analyze that information, look for particular threads, look for threats, share that information, again, with agencies like the FBI and others who can act upon it.

But we also understand that in so doing, in handling that information, we are responsible for being stewards of that information and that we are entrusted by the American people with protecting it. And it is part of our training, it is part of everything we do in terms of having access to information that we understand the laws and the policies and the regulations that apply to protecting that information to ensure that we do so in a way that is consistent with the civil liberties and privacy of all Americans.

Chairman CARPER. What further could you say to the American people who have these concerns about the right to privacy and their concern it is being violated or could be violated? What more could you say to reassure them that this is, indeed, a concern that the Administration and those with whom you work are mindful of?

Mr. OLSEN. Well, I think what I would say is that, again, the training and the oversight that we are subject to is unlike anything I have seen anywhere in the world, and it surpasses that which we experienced 10 years ago or even 5 years ago. So, the degree of oversight that we are subject to by Congress, by the judicial branch, by other elements of the executive branch, I believe should give the American people confidence that we are handling this information in a way that is appropriate and that secures privacy and civil liberties.

That said, we depend on the confidence of the American people in being able to do our job, so we are committed to being as transparent as possible in how we do that in order to continue to gain and maintain their confidence.

Chairman CARPER. All right. Director Comey, we have people that are concerned that folks at NSA are reading their e-mails, looking at their text messages, listening to their telephone conversations. What can you say to reassure almost all Americans that is not a concern they need to have, or can you?

Mr. COMEY. The first thing I would say is I agree very much with Director Olsen, that this is something every American should care about. Every American should care about how the government is using its authorities to protect them and where the government is also being mindful of the liberties that make this country so special. And what I tell folks is, look, our Founders were geniuses.

They divided power and created three parts of government to check power.

So, if you care about these issues, and everybody should, you should first ask, is the government working? Is there oversight? How is that oversight being done? Is it balanced? And the second thing is, I tell people, you should participate. Everybody should ask questions about how government is using its authorities and ask whether the system is working.

I happen to think the angel is in those details, that what has gotten lost in a lot of the discussion about how we use our authorities is just how the design of the Founders is operating to balance and to oversee the use of those authorities.

The challenge for all of us who are in charge of protecting the American people is finding the space in American life to have that conversation, because it cannot be on a bumper sticker. It requires me to say, look at how Congress oversees me. Look at how the Inspector General oversees me. Look at what the courts do. Look at what I report on. And that seems kind of boring, but that is the most important part of what we do, to show people that the government is working.

Chairman CARPER. All right. Thank you. Secretary Beers.

Mr. BEERS. I would certainly associate myself with the comments of both of my colleagues. The only thing that I would add is as a practical and operational matter at DHS, we have a Privacy Office with a Chief Privacy Officer, and we involve them in all of our projects to both collect, store, and share that information. Almost none of it is what you would call intelligence, but it is information and it is private information about applications for citizenship or travel information or visas. There is a lot of it and it is certainly one of the major activities that we engage in order to ensure that we are good stewards of that information as we obtain, store, and share.

Chairman CARPER. Should there be a similar kind of entity within, say, NSA that also, or the Foreign Intelligence Surveillance Court (FISA Court), focuses on privacy, as well?

Mr. BEERS. What works for us is what works for us, sir. I do know that they do have individuals who work on these issues with their staff, just as Director Olsen mentioned they do at NCTC. It just happens that, uniquely, we have an office that is formally part of the organization with a Chief Privacy Officer.

Chairman CARPER. Could you say to the American people with assurance that the gathering of all this information—and I realize it is impossible for NSA to actually listen to every telephone conversation, to read every e-mail, to be mindful of all the text messages that might be sent—but is there some way that you could reassure the American people that all the effort that is underway that we are talking about is actually for some good purpose, but actually for a demonstrated purpose because it has made us safer again and again and again? Can you provide any reassurance along those lines?

Mr. COMEY. What I can tell you, Senator, and the American people, is this is an agency that is not some rogue actor, the NSA. We work very closely with them. They have a very strong compliance culture. And they are overseen in many different ways in their ac-

tivities. What I say to folks who discuss it with me is, look, if you think the law ought to change, well, that is a discussion to have with Congress. But I have seen no indication that the NSA is acting outside the law or outside the scope of their oversight responsibilities. I just know from working with those folks, they are obsessed with compliance and with staying within the law.

Chairman CARPER. Mr. Olsen.

Mr. OLSEN. I would agree with Director Comey, and I, as I mentioned, served as the General Counsel at the National Security Agency. It is an extraordinary agency and it is an agency that is committed and, I think, using Director Comey's word, obsessed with compliance. They have a Chief Compliance Officer. They have an Inspector General. They have a General Counsel's Office. The leadership on down reiterates and reinforces the importance of complying with the law and the civil liberties and privacy of Americans. They follow the law when it comes to the collection of information involving U.S. persons. They do not indiscriminately collect information around the world. They serve to protect American lives, and that is what I saw when I served there.

Chairman CARPER. All right. Thank you.

Let us turn to the issue of dirty bombs, devices that could use radiological material, could sicken a lot of people, could cause significant psychological and, really, economic damage on a community. The Nuclear Regulatory Commission (NRC) in the Department of Energy's, I think it is the National Nuclear Security Administration, I believe they are responsible for the security of radiological sources. I think there was a GAO report, I want to say it was about a year ago, maybe September of last year, an audit that revealed that the U.S. medical facilities that house radiological material still face some challenges securing their supplies from potential theft.

Director Olsen, I do not know if you have any thoughts that you could give us, but what is the Intelligence Community's assessment of the likelihood that Al-Qaeda or one of its affiliates will seek to acquire radiological materials in order to try to make a dirty bomb?

Mr. OLSEN. I think what I can say in this setting is that we have seen over time some degree of interest along those lines, but nothing at this point that I would consider to be more than the sort of most basic aspirational type of interest by a terrorist organization. And I am not familiar with the report that you referenced.

Chairman CARPER. OK. And, Director Comey and Secretary Beers, what roles do your agencies play in preventing terrorists from building and potentially detonating a dirty bomb in the United States?

Mr. COMEY. I could probably answer for both of us. We share a responsibility that, at the FBI, we execute through our Weapons of Mass Destruction Directorate, one of whose responsibilities is to work with DHS to understand what are the potential sources of materials that terrorists could use to harm us and what are the trip wires we put in place so that we can know if something suspicious is happening around that material.

Chairman CARPER. All right. Secretary Beers.

Mr. BEERS. The only thing that I would add is we do have the ability to at least screen with radiation detectors at our ports of

entry. Obviously, it is possible that you could shield that information, but at least it gives us a first order sensor system to try to determine whether or not that information comes into the United States. We have also, through our grants program, helped State and local authorities obtain first order radiation detectors so that they can also look for that material within the country. But the key here is that we and the Bureau work together very much on this kind of effort.

Chairman CARPER. OK. Good. We talked a little bit earlier about travel, terrorist travel, going to a place for a while overseas and in a place from which they can freely travel back to the United States. Let me just ask each of you, what are we doing to better track and monitor people traveling to war zones and terrorist safe havens and then deciding to return to the United States? Mr. Olsen.

Mr. OLSEN. It is an important question and a matter of significant concern for us, Mr. Chairman. In particular, I would reference Syria as a place that we are concerned about because of the ongoing conflict there and the presence of extremist elements, including a group connected to Al-Qaeda such that it has become a place where literally thousands of individuals from other countries have gone to Syria to join in the fight, a number of them to join with Al-Nusra, this group that is connected to Al-Qaeda.

At NCTC, we work closely with the FBI and DHS to track the travel of any individuals that we have identified as an extremist and to, if appropriate, place those individuals on the watch list. We maintain the central database of known and suspected terrorists. That central database for the government provides a resource for all of our agencies as well as some of our partners around the world to identify those individuals and then to do what we can to look for the ways in which they are traveling, the facilitation routes, how they are funded, where they are going, and to disrupt their travel if possible, but at least to identify them so if they do return to their home country, and especially, obviously, the United States, we have a handle on what their activities are.

Chairman CARPER. All right.

Mr. BEERS. Let me add to that. This is truly an integrated effort. We sit together in terms of trying to pull together the lists of individuals that we have identified as potential threats to the United States. We also have a program with our, particularly our European allies because of the visa waiver program, to share information that they and we might have nationally with one another in order to add to the database that we have of the individuals who are of concern.

We at DHS also support this effort through our travel analysis, looking for people who we do not know might have gone to Syria—or might have gone to Syria for nefarious purposes. We have a number of indicators that help us identify individuals who we might want to speak to at ports of entry as they return to the United States.

I do not want to go into the details of that because I do not want to give away the way we actually do that, but we have a number of techniques which will allow us to identify somebody who it is not clear in terms of their travel record leaving the United States and coming back that they were anywhere near Syria. But there are

other indicators that can give us indications that we might want to talk to those individuals, and that is part of finding the unknowns as opposed to tracking the knowns, which I think we are pretty good at.

Chairman CARPER. Good. Thank you for responding to that question.

That is the last question I have except this is an opportunity for you, if you would like to each just give a short closing statement, please. And it could be something that has come to mind, something that you want to reiterate, something that you heard another colleague say that you think is worth emphasizing. Go ahead, please.

Mr. OLSEN. Well, Mr. Chairman, first, let me just thank you and this Committee for holding the hearing and really for your consistent and steadfast support for the Intelligence Community and for all of our efforts with respect to protecting the homeland.

The one issue, I think, that comes to mind goes back to Director Comey's opening comments, and that is on the budget. We are struggling, like all other government agencies, to deal with the sequester cuts, and this is a real issue that strikes at the core of our workforce and it is something that I think bears raising in this forum.

Chairman CARPER. And I am glad you did. Thank you.

Mr. OLSEN. But, otherwise, I would just offer, again, to continue to work closely with you and the Committee going forward for whatever you need from us as we work together.

Chairman CARPER. Great. Thank you. Director Comey.

Mr. COMEY. Mr. Chairman, I would just thank you for having this hearing. These conversations are critically important to the American people. They should demand to know how we are doing our jobs and how we are using the power we have been given and we ought to answer and have those conversations. I should not be doing anything—we should not be doing anything we cannot explain. Sometimes it has to be in a closed setting so that the bad guys do not know what we are doing, but these conversations are what the Founders intended, so thank you.

Chairman CARPER. You are welcome, and thank you. Secretary Beers.

Mr. BEERS. I certainly would be remiss in not piling on the budget question. It obviously affects us enormously at DHS, with 240,000-plus individuals and a vast array of programs.

The second point I would make is the point that we talked repeatedly about. We really do need the cyber legislation. I know that you and this Committee are trying to do something on that, but as we have sat here and told you and you have told us that this is a critical vulnerability that the United States faces, not having that legislation leaves that vulnerability open and we owe it to the American people to be able to protect them and protect them better.

Chairman CARPER. Well, those are all really good notes on which to close.

I want to, again, thank you for your preparation, for clearing your schedules to be with us and spend time with us.

Dr. Coburn said to me that it is too bad the other Members of our Committee could not have been here to hear this and to participate in the conversation. All of them have several Committee hearings going on simultaneously and it is just difficult for them to go to every one of them. But about half of our colleagues were able to join us for part of it. Their staffs were, in many cases, here, but also watching on closed-circuit television back in their offices, as you know.

Director Comey, this is the first time that you have been before us to testify and I am very impressed by the way you handled yourself. These other two fellows are seasoned pros and they lived up to their reputation.

Rand, thank you for taking on all these responsibilities over at DHS and doing them well while we work very hard to try to get a Secretary confirmed and a Deputy Secretary confirmed so you can be a little less frenetic.

Thank you very much, and I think the hearing record is going to remain open for 12 days. That is until November 25, at 5 p.m., for the submission of statements and questions for the record.

And with that, this hearing is adjourned. Thank you again very much.

[Whereupon, at 12:07 p.m., the Committee was adjourned.]

# APPENDIX

**Opening Statement of Chairman Thomas R. Carper**
**"Threats to the Homeland"**
**November 14, 2013**

*As prepared for delivery:*

Today's hearing will consider threats to the U.S. homeland from terrorists, cyber attackers, homegrown extremists and lone wolf offenders. The objective of the hearing is for this committee to get a better understanding of how these threats have evolved over the past year and if our national security agencies are keeping up with these ever-changing threats.

Twelve years ago, our country's sense of security was upended when Al-Qaeda launched the most significant attack on U.S. soil since Pearl Harbor. In the years since that tragic day, we have made significant progress in combatting the terrorist threat to the homeland.

Our aviation system is more secure. Our borders are stronger. Our government agencies share more terrorist intelligence than ever before. Our first responders are better prepared to deal with disasters and terrorist attacks. Americans are safer because of these efforts. While we have made great strides, our system for preventing terrorist attacks is not perfect.

One of my guiding principles is—if it's not perfect, make it better. In this spirit, this committee will continue its work to improve America's defenses against terrorism and other threats. Part of this process means understanding that the threat is also evolving. If we are to make America safer from these threats – and secure the homeland – we must do a better job of anticipating these evolving threats.

We do a good job at fighting the last war, but to secure the homeland we must be better at anticipating the next war. We know that the threat from al Qaeda has changed over the past decade.

We are now dealing with a number of splinter groups, including Al Qaeda in the Arabian Peninsula which was responsible for the Christmas Day attack in 2009 and which continues its efforts to attack us to this day. And we know that American citizens, as well as Canadian and European nationals, have taken up arms in Syria, Yemen, and Somalia. The threat that these individuals could return home to carry out attacks is real, and troubling.

Even as our borders and ports of entry have become more secure, there are still those within our borders who have become radicalized by online al-Qaeda propaganda and seek to carry out their own attacks against the U.S. And there are other threats to our domestic security – unrelated to al-Qaeda – which we must be prepared to address.

As the September attack on the Washington Navy Yard and the shooting at the Los Angeles airport two weeks ago demonstrate, there are a variety of threats to federal personnel and federal facilities that we must be prepared to defend against. However, nowhere is the need to prepare for the next attack more pressing than in the cybersecurity realm.

In the words of former FBI Director Robert Mueller, cyber threats may 'equal or surpass the threat of terrorism in the foreseeable future.' With a few key strokes, hackers can shut down our electric grid, release dangerous chemicals into the air we breathe, or disrupt our financial markets.

Now more than ever, we must come together to pass cybersecurity legislation that strengthens our defenses against these cyber threats. The threat is too great, the potential consequences too severe, to do nothing. Today's hearing will explore these threats, as well as others.

We will hear testimony from the leaders of the Department of Homeland Security, the National Counter Terrorism Center and the Federal Bureau of Investigation about the greatest dangers to the homeland and the steps our government is taking to further secure our country.

The findings from today's hearing will help continue our process of recalibrating our homeland defenses to address our current threats, as well as prepare for tomorrow's threat. It will also help us ensure that we have a government in place that can connect the dots before terror comes to our shores. I look forward to working with our witnesses and the members of this committee as we seek to defeat these threats and keep Americans safe from those who wish to do us harm.

###

**Statement for the Record**

**Acting Secretary Rand Beers**

**U.S. Department of Homeland Security**

**Before the**

**United States Senate**

**Committee on Homeland Security and Governmental Affairs**

**November 14, 2013**

**Introduction**

Thank you, Chairman Carper, Ranking Member Coburn, and Members of the Committee. I appreciate the opportunity to appear before the committee to discuss the Department of Homeland Security's (DHS) efforts to prepare for, protect against, respond to and recover from threats facing our nation and the American people.

At the outset, I want to thank Federal Bureau of Investigation (FBI) Director James Comey and National Counterterrorism Center (NCTC) Director Matthew Olsen for their strong collaboration as together we work to meet the shared responsibility of keeping our nation safe. I also want to thank Congress for your guidance and support over the past four years, and indeed, since the Department's founding ten years ago.

In addition, I would like to urge Congress to swiftly confirm Jeh Johnson, President Obama's nominee to be our nation's next Secretary of Homeland Security. I have known Jeh for a long time. He cares deeply about the mission of this department and will bring considerable skill, intellect, experience, and dedication to our nation's efforts to address evolving threats. In short, he will be an excellent Homeland Security Secretary.

Let me also say at the outset that the entire DHS family continues to mourn the loss of Transportation Security Officer Gerardo Hernandez, who was killed in the shooting at Los Angeles International Airport on November 1st.

As you know, Officer Hernandez was the first TSA officer killed in the line of duty. This senseless act of violence reminds us of the dangers our men and women on the frontlines face every day, and the very real sacrifices they often make on our behalf. We continue to work closely with the FBI and our state and local law enforcement partners to fully investigate this crime and ensure justice is served. As always, our security posture, which at all times includes a number of measures both seen and unseen, will continue to respond appropriately to protect the American people.

Of course, DHS relies on many partners from across our nation to meet our diverse missions. In this way, homeland security is not the charge of a single department or agency, but the responsibility of all of us, from our largest city police force to smallest law enforcement jurisdiction, our biggest company to smallest independent business, from the Whole Community to each individual within those communities.

This "homeland security enterprise" is integral to our nation's ability to address threats in a timely and comprehensive fashion. For this reason, DHS has worked with partners all across our country to build critical capabilities at the state, local, tribal, and territorial levels, share information, protect infrastructure in partnership with the private sector, enhance preparedness and resilience, and address new and evolving threats, such as those in cyberspace.

Since DHS's creation ten years ago, our country is stronger, better equipped to handle threats, and more nimble in our ability to respond and recover. Our progress is a testament to the hard work of more than 240,000 DHS employees and our strong partnerships with Federal, state, and

local officials, including law enforcement and emergency managers, non-profit and faith-based organizations, and an engaged and vigilant public.

Nevertheless, we know threats to the homeland continue to evolve. As we have seen in recent months with the Boston Marathon attacks, we face a dynamic threat environment that includes threats from abroad as well as those that originate within our borders. These threats can come from international terrorist organizations, groups inspired by terrorist ideology but with no operational connections to core groups or affiliates, as well as lone wolves, often with no particular ideological motivation, yet still intent on doing widespread harm.

Within the context of U.S.-based violent extremism, we know that al-Qa'ida, its affiliates, and allies use propaganda to inspire prospective U.S.-based supporters to conduct terrorist attacks in the West and especially the homeland. Lone offenders – prime targets of al-Qa'ida's English-language messaging, such as the online magazine Inspire – tend to favor plots involving the use of easily acquired weapons against local targets. These lone offender plots are especially challenging because they can be tactically simple and adaptable, complicating disruption by authorities.

However, although we are concerned about the threat posed by al-Qa'ida or individuals inspired by al-Qa'ida, the threat posed by violent extremists is a broader threat not limited to a single ideology. Because the threat environment constantly evolves, DHS must consider all types of violent extremism, while ensuring we do not inappropriately focus upon individuals who may be engaging in legal, constitutionally-protected behavior, such as political speech. To this end, DHS focuses its attention on individuals who are inspired not merely by specific ideologies, but are inspired to violence and/or specific criminal activity as a means of furthering their ideological objectives. Many communities and rural counties nationwide face such threats.

Lone offenders and small groups of individuals are one of the greatest and most difficult threats to counter. In recent years, we have observed several acts of violence by lone offenders against military targets, as well as attempted attacks targeting civilian populations by individuals inspired by extremist ideology. Domestic terrorism, and those individuals not inspired by foreign terrorist groups, remains a persistent threat.

Today I will discuss how DHS works with our partners to address these and other threats, building on our work over the past ten years while implementing new programs and initiatives to ensure we remain agile and adaptable, learn and apply lessons from past attacks, and continue to protect individual liberties and privacy while supporting our economy.

**Guarding Against Terrorism**

Guarding against terrorism is the founding mission of DHS. While this is not our only mission, it has been our primary focus since our inception. DHS recognizes that we cannot prevent all threats all the time, nor can we guarantee the safety of every community against all hazards. Our chief operating principle, therefore, has been to work with partners at all levels to enhance our collective ability to detect and deter high-risk threats as early as possible, build capabilities to respond to them when required, and enhance our ability to quickly recover after the fact.

*Building State and Local Capacity*

DHS has worked to get information, tools, and resources into the hands of state, local, tribal, and territorial officials. We have done so by focusing on four key priorities: (1) improving the sharing of both classified and unclassified information regarding potential threats to the homeland; (2) building grassroots analytic capabilities at the state and local levels; (3) standardizing how we train state, local, tribal, and territorial law enforcement to recognize behaviors and indicators that have historically been associated with terrorism and report suspicious activities; and (4) increasing community awareness and encouraging the public to report suspicious activity to law enforcement.

A cornerstone of this effort has been our support for state and major urban area fusion centers. To date, DHS has deployed 96 Office of Intelligence and Analysis (I&A) personnel to fusion centers throughout the country to coordinate with intelligence and law enforcement personnel. We also have deployed 71 Homeland Secure Data Network (HSDN) systems across the country to provide access to Secret information and intelligence.

Moreover, we have trained state and local analysts at fusion centers to ensure they have the necessary skills and expertise to analyze and place intelligence and information from the Intelligence Community within local and regional contexts to produce relevant and timely products. And we have developed tailored products to meet the needs of our state and local partners and expanded distribution to ensure relevant and appropriate information is shared with those who need it.

*Providing Training and Resources*

We provide support through a variety of training and exercises to our law enforcement and community partners. DHS has worked closely with the FBI on the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) to ensure frontline law enforcement receive training in how to appropriately report suspicious activity while protecting individual rights and liberties.

We have worked with the Department of Justice (DOJ), including the FBI, and NCTC on Countering Violent Extremism (CVE) training and outreach, with three primary goals. First, we are working to better understand the phenomenon of violent extremism through extensive analysis and research on the behaviors and indicators associated with violent extremism. Second, we are addressing the dynamics of violent extremism by strengthening our partnerships with a broad and diverse range of domestic and international partners from state and local governments and law enforcement, to faith-based organizations and community groups.

Since 2011we have worked with law enforcement partners to develop CVE training to ensure frontline law enforcement officers understand behaviors potentially indicative of violent extremist activity. As part of this effort, we recently launched a joint DHS/DOJ-FBI web-based portal that contains training materials for law enforcement and first responder training practitioners, as well as hundreds of additional tools and resources for countering the threats from violent extremism, terrorist activity, and mass casualty attacks.

We are leveraging our resources to help law enforcement and the private sector to address active shooter situations. For example, we have hosted Active Shooter Workshops and training sessions for law enforcement to discuss lessons learned from past active shooter situations and best practices. Working with commercial facilities, we developed training to better prepare store managers and hourly personnel to respond to a potential active shooter incident. We also created a new active shooter page on the DHS website – www.dhs.gov/active-shooter-preparedness – with resources designed for law enforcement as well as the public on how to respond to active shooter incidents.

The Federal Law Enforcement Training Center (FLETC) offers active shooter training and resources to numerous law enforcement agencies at the federal, state, local, tribal, and territorial levels. FLETC also collaborates with partners at DOJ and in academia to take a holistic approach to developing strategies aimed at preventing incidents of multiple casualty violence. Bringing together subject matter experts from a cross-section of pertinent disciplines, including law enforcement, academia, law, health administration, medicine, private security, and education, FLETC hosted two summits during Fiscal Year 2013 to further the national dialogue on preventing multiple casualty violence, specifically addressing concepts such as information-sharing across jurisdictions and community-based prevention models.

The DHS Office of Health Affairs is working with other Federal agencies to develop Federal guidance for fire, EMS, and law enforcement on the medical response to Improvised Explosive Device (IED) and Mass Shooting incidents. DHS is planning interagency engagements with fire, EMS, and law enforcement stakeholders over the next six months on this issue.

The Federal Protective Service (FPS) provides coordination and assistance to Federal agency officials on Occupant Emergency Plan (OEP) development. These plans are intended to minimize risk to personnel, property, and other assets within a Federal facility by providing a facility-specific response plan and evacuation procedures for occupants. FPS also provides agency-specific evacuation training and drills which incorporate work place violence and active shooter awareness training.

Because an engaged and vigilant public is vital to our efforts to protect our communities, DHS has continued expansion of the "If You See Something, Say Something™," campaign to more than 250 states, cities, transportation systems, universities, and private sector entities nationwide to encourage the public to play an active role in reporting suspicious activity.

*Building Capabilities to Counter Improvised Explosive Devices (IEDs)*

Through the Office for Bombing Prevention (OBP), DHS partners with both public and private sector partners to build capabilities to prevent, protect against, respond to, and mitigate bombing incidents such as the Boston Marathon attack. OBP conducts Bombing Prevention training and Multi-Jurisdiction IED Security Planning workshops to assist with the development of IED security plans to integrate assets and capabilities from multiple areas and emergency service sectors in responding to an IED attack. The workshop and plan development is a systematic

process that fuses counter-IED education, capability analysis, training, and planning tailored to the unique requirements of high-risk jurisdictions.

OBP hosts the Bomb-making Materials Awareness Program (BMAP), a joint OBP-FBI program that promotes private sector, point-of-sale awareness, and SAR training to prevent misuse of dual-use explosive precursor chemicals and components commonly used in IEDs. BMAP cultivates prevention opportunities by building a network of aware and vigilant private sector partners who serve as the Nation's counter-IED "eyes-and-ears."

OBP maintains TRIPwire, an online, information-sharing network for bomb squad, law enforcement, and other emergency services personnel. TRIPwire shares critical information with public and private sector partners during periods of heightened alert or following IED-related incidents. Following the Boston Marathon attack, for example, use of TRIPwire increased to nearly 600,000 hits alone on April 16th.

The Administration is undertaking efforts to enhance counter- IED prevention, protection, response, and mitigation. DHS is supporting programmatic coordination and implementation of the National Policy for Countering IEDs, and with our interagency partners we are working across the Federal government to ensure programs are being properly integrated and leverage the knowledge and resources available to ensure public and private sector partners have the capabilities to counter IED-related threats.

*Boston Marathon Response*

The results of our efforts are communities across the United States that are better equipped to handle a variety of threats, including terrorism. We need only look at the timely and well-coordinated response to the despicable Boston Marathon attack to see how investments in building state and local capacity contributed to an effective, integrated response by the Boston community – one that ultimately prevented more lives from being lost on that horrible day.

In previous years, DHS provided homeland security grants to the City of Boston and Commonwealth of Massachusetts to equip and train special response teams in improvised explosive device detection, prevention, response, and recovery. We supported more than a dozen exercises in Boston, including one that focused on a large, mass-casualty event and involved hundreds of responders last November. And we supported the creation of the Medical Intelligence Center to enable information sharing across the Boston medical community.

The President declared a state of emergency on April 17, allowing the Federal Emergency Management Agency (FEMA) to coordinate the provision of emergency protective measures in response to the attack. The well-executed emergency response that immediately followed the Boston Marathon attack was the product of years of planning, training, and investment in building state and local capacity. Without the selfless service of so many heroic individuals and first responders, the toll from this attack could have been far greater, and this terrible tragedy could have been even worse. Already DHS has brought together law enforcement, first responders, and others involved to examine the response and identify lessons that we may apply in the future to prevent such attacks and ensure an effective response if they occur.

*Enhancing Inbound Targeting of Passengers and Cargo*

As this committee knows well, threats from abroad, in particular those directed at our aviation system, have continued to evolve over the past decade. In addition to the attempted terrorist attack against Northwest Airlines Flight #253 on Christmas Day in 2009, we have seen the attempted bombings of cargo planes bound from Yemen in 2010. Last year, the international community also thwarted a plot that would have targeted a U.S-bound airliner with explosives.

Al-Qa'ida in the Arabian Peninsula (AQAP) remain the Al-Qa'ida affiliate about which we have the greatest concern because of its demonstrated and continuing interest in advancing plots to attack the homeland, particularly the aviation industry. We remain concerned that AQAP continue to seek ways to circumvent existing security measures, using tactics that are creative and increasingly sophisticated. Despite the death of Anwar al-Aulaqi, the group's master bomb maker and other key leaders remain alive, and the group almost certainly maintains the intent and capability to attack the homeland with little to no warning.

We have responded to such threats comprehensively and in a manner that underscores the international scope of the aviation system. Shortly after the 2009 Christmas Day plot, DHS launched a major international initiative to address existing security vulnerabilities in aviation. In 2010 the International Civil Aviation Organization (ICAO) General Assembly unanimously supported a historic new Declaration on Aviation Security. This Declaration provided a unified vision for strengthening security in the areas of information collection and analysis, information sharing and passenger vetting, the development of security standards, and deployment of technology.

Since that time, governments and aviation industry partners have worked to meet the objectives of the Declaration, including adapting to new and emerging threats, and addressing them swiftly and decisively; and raising the level of security through assistance and capacity development. As of January of this year, 19 countries have deployed or piloted Advanced Imaging Technology (AIT) in their major airports to screen passengers for metallic and non-metallic threats, including weapons, explosives, and other objects concealed under layers of clothing. In addition, the Transportation Security Administration (TSA) now has agreements with 64 foreign governments permitting Federal Air Marshals to be present on international U.S. carrier flights.

Importantly, we have continued to build a layered approach to aviation security that includes the prescreening of passengers; the deployment of new technologies; training of airport security and law enforcement personnel to better detect behaviors potentially associated with terrorism; and strengthening of air cargo security. We are integrating this risk-based, intelligence driven approach into everything we do to identify passengers and cargo that warrant additional scrutiny, providing the most effective transportation security in the most efficient way possible.

To become more risk-based, we have sought to leverage information to identify threats earlier and share that information with our foreign counterparts and aviation sector partners. In April of 2012, the United States ratified a new agreement with the European Union to continue the transfer of Advance Passenger Information/Passenger Name Records (API/PNR), an important

milestone in our collective efforts to protect the international aviation system from terrorism and other threats. Analysis of API/PNR data allows us to better identify passengers we should pay more attention to before they arrive at the airport.

We also leverage information to enhance our inbound targeting operations through programs like the Pre-Departure Targeting Program and Immigration Advisory Program (IAP), which help identify high-risk travelers likely to be inadmissible to the U.S., and make recommendations to commercial carriers to deny boarding. From Fiscal Year 2010 to 2012, U.S. Customs and Border Protection (CBP) worked with our partners in the airline industry to prevent 8,984 high risk travelers from boarding aircraft to the United States as a result of its Pre-Departure and Immigration Advisory/Joint Security Programs.

CBP also operates preclearance operations at 15 locations in five countries, allowing for the complete security screening and formal determination of admissibility of travelers to the United States before they board a U.S-bound flight. In Fiscal Year 2012, CBP processed 15.6 million travelers through preclearance operations.

Through the Visa Security Program, U.S. Immigration and Customs Enforcement (ICE) also has deployed agents to high-risk visa activity posts overseas to identify potential terrorist and criminal threats before those individuals are granted a U.S. visa. And to further enhance visa-screening efforts, ICE, CBP and the Department of State (DOS) are collaborating on an automated visa application screening process that broadens the scope for identifying potential derogatory information prior to visa adjudication and issuance, and synchronizes reviews of the information across these agencies. Since the program's inception in January 2013, more than 1.9 million visa applications have been received and 1,304 have been returned to DOS for disapproval, including 950 for security-related reasons.

*Air Cargo Security*

With respect to air cargo security, DHS has worked with partners around the world to recognize National Cargo Security Programs (NCSPs) that further strengthen international air cargo security. As of September 2013, TSA has recognized the programs of 37 countries, which account for approximately 67 percent of inbound cargo to the United States on passenger aircraft.

We are also formalizing and expanding our Air Cargo Advance Screening (ACAS) pilot, a joint effort between TSA and CBP that enables members of the air cargo industry to send and receive advance security filing data for their air cargo, which helps us identify high-risk shipments for enhanced screening. As of September 2013, there are 81 entities participating in the ACAS pilot and over 100 million shipments have been successfully processed.

Moreover, today 100 percent of all air cargo on passenger aircraft that depart U.S. airports, or airports which serve as the last point of departure to the U.S., is screened to provide a level of security that is commensurate with the level provided by screening of passenger checked baggage. TSA Transportation Security Specialists (TSSs) verify compliance with security requirements, including screening, for all air carriers which operate into the United States.

More broadly, DHS continues to work with international organizations such as ICAO, World Customs Organization (WCO), and Universal Postal Union (UPU) to develop broad air cargo and mail security guidelines and standards. This strategy is designed to enlist other nations, international bodies, and the private sector in increasing the security of the global supply chain by adopting new inbound cargo targeting rules, institutionalizing a supply chain approach to security, implementing additional and enhanced screening for all cargo identified as high risk, and improving sharing of advanced cargo data and electronic shipping information.

*Facilitating Trade and Travel*

While these measures are important, we have not forgotten our imperative to facilitate lawful trade and travel to and from the United States. Accordingly, DHS has focused on leveraging information and technology to expedite legitimate travelers consistent with our risk-based approach. TSA has implemented various measures to focus its resources and improve the passenger experience at security checkpoints by applying intelligence-driven, risk-based screening procedures and enhancing its use of technology, including deployment of AIT machines to nearly 160 airports nationwide.

We also have expanded popular and successful trusted traveler programs such as Global Entry and TSA Pre✓™. Global Entry expedites pre-approved, low risk air travelers entering the United States, in many cases allowing them to clear customs and immigration processing within minutes. Similarly, TSA Pre✓™ provides expedited screening for airline travelers.To date, more than 18 million travelers have experienced TSA Pre✓™ at 100 airports nationwide.

In July, TSA also announced a new process that will allow even more U.S. citizens and Lawful Permanent Residents to enroll in TSA Pre✓™ by enabling them to apply online and visit an enrollment site to provide identification and fingerprints. TSA also offers expedited screening to more low-risk travelers by using information already provided by passengers through its existing Secure Flight program requirements. This process allows TSA to maintain its high security standards and create greater efficiency while offering more travelers the benefit of expedited screening through TSA Pre✓™ lanes.

And with respect to the facilitation of cargo, we have continued to strengthen and expand the Customs-Trade Partnership Against Terrorism (C-TPAT), our trusted shipper program that provides validated members with expedited customs processing.

**Enhancing Border Security and Combating Transnational Crime**

Of course, effective border security is essential to a safe, secure homeland. Over the past four and a half years, DHS has invested historic resources to protect our borders and prevent illegal cross-border activity. Because of these investments in manpower, technology, and infrastructure, our borders are now better staffed and protected than any time in our nation's history.

We have doubled the number of Border Patrol agents from approximately 10,000 in 2004 to more than 21,000 agents today. We have reinforced law enforcement capabilities at the ports of entry, increasing our numbers of CBP personnel from 17,279 customs and immigration inspectors in 2003, to more than 21,000 officers and 2,400 agriculture specialists today.

Supplementing this increase in personnel, we have made unprecedented investments in border infrastructure and technology, including the deployment of integrated fixed towers, mobile surveillance units, and thermal imaging systems along the borders, as well as new technology at the ports of entry, including Non-Intrusive Inspection and Radiation Portal Monitor technology to identify contraband and weapons of mass effect. We have expanded aerial coverage of the border as well, including Unmanned Aerial Systems that now cover the entire Southwest border from California to Texas, and 950 miles along our Northern border, providing critical aerial surveillance assistance to personnel on the ground.

CBP is also working closely with the DHS Science & Technology Directorate (S&T) to identify and develop technologies to improve our surveillance and detection capabilities on our land and maritime borders. This includes investments in tunnel detection and tunnel activity monitoring technology, low-flying aircraft detection and tracking systems, maritime data integration/data sharing capabilities, supply chain cargo security, and improved border surveillance tools.

We also have made our ports of entry more efficient through investments in technology and new requirements for secure travel documents as part of the Western Hemisphere Travel Initiative (WHTI). To date, more than 19 million individuals have obtained Radio Frequency Identification (RFID) technology-enabled secure travel documents that can be verified electronically in real-time to establish identity and citizenship and have reduced average vehicle processing times by 20 percent. CBP also conducts active lane management at land border ports as conditions warrant to accommodate trusted travelers and those with RFID-enabled documents.

By every traditional measure, this deployment of personnel, technology, and resources has led to unprecedented results. In addition to the historic lows in illegal alien apprehensions achieved over the past four years – down 50 percent from Fiscal Year 2008 – we have increased seizures of illegal drugs, weapons, and contraband. From Fiscal Years 2009 to 2012, CBP seized 71 percent more currency, 39 percent more drugs, and 189 percent more weapons along the Southwest border as compared to Fiscal Years 2006 to 2008.

Nationwide, CBP officers and agents also seized more than 4.2 million pounds of narcotics and more than $100 million in unreported currency through targeted enforcement operations. At U.S. ports of entry, CBP also arrested nearly 7,900 people wanted for serious crimes, including murder, rape, assault and robbery in FY 2012.

Additionally, in Fiscal Year 2012, Border Enforcement Security Task Forces (BESTs) made 2,812 criminal arrests, 853 administrative arrests, and federal prosecutors obtained 1,879 indictments and 1,671 convictions in BEST-investigated cases. BESTs consist of more than 1,000 members who represent more than 100 Federal, state, tribal, territorial, and international law enforcement agencies who have jointly committed to investigate transnational criminal activity along the Southwest and Northern borders and at our nation's major seaports.

Along our maritime borders, the United States Coast Guard (USCG) actively contributes to our successful border security efforts. In Fiscal Year 2012, USCG seized over 107 metric tons of cocaine and 56 metric tons of marijuana destined for the United States; seized 70 drug trafficking vessels, detained 352 suspected smugglers; conducted over 11,600 annual inspections of U.S. flagged vessels; and conducted more than 9,000 Port State Control and Security examinations on foreign flagged vessels

Through prioritized enforcement investigations and operations, ICE Enforcement Removal Operations also removed record numbers of criminals from the United States while increasing its efforts to combat transnational criminal activity. In Fiscal Year 2012, approximately 55 percent, or more than 225,000, of the individuals that ICE removed from the United States were convicted of felonies or misdemeanors — a more than 96 percent increase since Fiscal Year 2008. Overall, 96 percent of ICE's removals fell into one of its priority categories of national security or public safety threats, repeat immigration violators, or recent border crossers. ICE also achieved significant success in its efforts to combat Transnational Criminal Organizations (TCOs). Since Fiscal Year 2011, ICE has disrupted or dismantled 285 of the most dangerous TCOs and individuals.

With respect to its counterterrorism mission, ICE-Homeland Security Investigations (HSI) remains DHS's largest partner in FBI Joint Terrorism Task Forces (JTTFs), where ICE-HSI special agents serve as leads or co-case agents on counterterrorism investigations where ICE's unique immigration or trade authorities are viewed as the most likely avenue to deter, disrupt or dismantle terrorist networks or terrorist attacks against the homeland.

In Fiscal Year 2012, ICE-HSI special agents assigned to JTTFs initiated 614 counterterrorism investigations, 129 of which focused specifically on charges for material support to terrorism. ICE HSI special agents arrested 532 subjects of investigations for various administrative or criminal charges including material support to terrorism, import/export violations, benefit fraud, financial fraud and violations of the Immigration and Nationality Act.

**Protecting Critical Infrastructure and Cyber Networks**

DHS coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. Working with the Sector-Specific Agencies established in PPD-21, DHS supports critical infrastructure owners and operators in preparing for, protecting against, mitigating from, responding to, and recovering from all-hazards events, including cyber incidents, terrorist attacks, and natural disasters. These activities promote the safety and security of the American public and ensure the provision of essential services and functions, such as energy and communications. To achieve this goal, DHS works with a variety of public and private partners to identify and promote effective solutions for security and resilience that address the risks facing the nation's critical infrastructure.

One lesson we have learned over the years is the need to work directly with stakeholders to enhance security and resilience of infrastructure. To this end, DHS has strategically deployed Protective Security Advisors across the United States to provide public and private sector

stakeholders with access to steady-state DHS risk-mitigation tools, products, and services, such as training and voluntary vulnerability assessment programs, in addition to supporting officials responsible for planning and leading National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) events. Protective Security Advisors support the response to all hazard incidents through field level coordination and information sharing, and provide expertise on reconstituting affected critical infrastructure.

Through the Protective Security Advisors, DHS also conducts onsite risk assessments of critical infrastructure and shares risk and threat information with state, local and private sector partners. In addition to helping owners and operators become more aware of the risks, hazards, and mitigation strategies, we are also helping them measure and compare their levels of security and resilience and how they can improve. In the last year, DHS conducted more than 900 vulnerability assessments and security surveys on critical infrastructure to identify potential gaps and provide the owners and operators with options to mitigate those gaps and strengthen security and resilience.

*Cybersecurity*

Our infrastructure protection efforts also include working closely with the private sector to protect our nation's information and communications technology against agile and sophisticated cyber threats. DHS is responsible for securing unclassified federal civilian government networks and working with owners and operators of critical infrastructure to help them secure their networks. We also coordinate the national response to significant cyber incidents and create and maintain a common operational picture for cyberspace across the government including building an integrated consequence analysis capability to evaluate critical infrastructure impacts from incidents, threats, and emerging risk.

This is critical, time-sensitive work, because we confront a dangerous combination of known and unknown cyber vulnerabilities, and adversaries with strong and rapidly expanding capabilities. Threats range from denial of service attacks, to theft of valuable trade secrets, to intrusions against government networks and systems that control critical infrastructure. These attacks come from every part of the globe, every minute of every day, and are continually increasing in seriousness and sophistication.

*DHS Cyber Roles*

Over the past four and a half years, cybersecurity has emerged as a top priority for DHS through our efforts to secure unclassified federal civilian government networks, work with critical infrastructure owners and operators, combat cyber crime, build a national capacity to promote responsible cyber behavior and cultivate the next generation of frontline cybersecurity professionals – all while keeping a steady focus on safeguarding the public's privacy, civil rights, and civil liberties.

To protect federal networks, DHS is deploying technology to detect and block cyber intrusions and developing continuous diagnostic capabilities, while providing guidance on what agencies need to do to protect themselves. For example, DHS deploys network intrusion detection and

prevention technology under a program known as Einstein. Through the Continuous Diagnostics and Mitigation (CDM) program, DHS is also taking a dynamic approach to fortifying the cybersecurity of computer networks and systems by providing capabilities and tools that enable network administrators to know the state of their respective networks at any given time, understand the relative risks and threats, and help system personnel to identify and mitigate flaws at near-network speed. When both programs are implemented, they will provide complementary protections across the "dot-gov" domain, further protecting the government's infrastructure and the nation's data.

DHS also works closely and regularly with owners and operators of critical infrastructure to strengthen their facilities through on-site risk assessment, mitigation, and incident response, and by sharing risk and threat information with the goal of strengthening the network defenses against outside attacks, maintaining system integrity, and preventing theft of proprietary information and trade secrets. For example, we provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities following the recent series of denial of service attacks. DHS is also home to the National Cybersecurity & Communications Integration Center, an around-the-clock cyber situational awareness and incident response center that has responded to nearly 500,000 incident reports and released more than 26,000 actionable cybersecurity alerts to public and private sector partners over the past four years.

Last year, our U.S. Computer Emergency Readiness Team (US-CERT) also resolved approximately 190,000 cyber incidents and issued more than 7,450 alerts – a 68 percent increase from 2011. And our Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 177 incidents while completing 89 site visits and deploying 15 teams to respond to significant private sector cyber incidents.

*Cybercrime*

To combat cyber crime, DHS relies upon the skills and resources of USSS and ICE, and works with a variety of partner organizations and agencies to investigate cyber criminals. Since 2009, DHS has prevented $10 billion in potential losses through cyber crime investigations and arrested more than 5,000 individuals for their participation in cyber crime activities.

On July 25th, for example, DOJ announced the indictment of several individuals who directed a prolific criminal cyber hacking organization. USSS dismantled this transnational cybercrime ring after the group conspired in a worldwide hacking and data breach scheme that targeted major corporate networks and stole more than 160 million credit card numbers, which resulted in hundreds of millions of dollars in losses – the largest such scheme ever prosecuted in the United States. In Fiscal Year 2013, USSS cyber investigations accounted for over 1,000 arrests globally and prevented over $1.1 billion in fraud loss to U.S. financial institutions.

In 2001, Congress mandated USSS to establish a nationwide network of task forces to "prevent, detect and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." Currently, USSS hosts 31 Electronic Crimes Task Forces (ECTF) that the Department leverages by combining the resources of academia, the private sector, and Federal, state and local law enforcement agencies.

USSS also collaborates with the State of Alabama to operate the National Computer Forensics Institute (NCFI), the nation's only federally-funded training center dedicated to instructing state and local officials in digital and cyber crime investigations. USSS opened the NCFI with a mandate to provide state and local law enforcement, legal and judicial professionals a free, comprehensive education on current cyber crime trends, investigative methods and prosecutorial challenges. Since its opening in 2008, the state-of-the-art facility has trained more than 2,400 state and local police officials, prosecutors, and judges from all 50 states and three U.S. territories. These NCFI graduates and members of the ECTFs represent over 1,000 state and local government agencies nationwide.

A recently executed partnership between ICE and USSS also will expand participation in the existing ECTFs to enhance their respective cyber investigative strengths, while maintaining their separate identities. And DHS is a partner in the National Cyber Investigative Joint Task Force, which serves as a collaborative entity that fosters information sharing across the interagency for investigating national security cyber threats.

*Additional Collaboration and Coordination*

At DHS, we have consistently stated that cybersecurity transcends national borders and requires operational collaboration, strategic dialogue, and an increased security and resilience of global supply chains. DHS works closely with the Department of State and our international partners to enhance information sharing, increase situational awareness, improve incident response capabilities, and coordinate strategic policy issues. DHS also works with international law enforcement partners to share expertise and resources to combat electronic crimes such as identity theft and intellectual property infringement, network intrusions, and a range of financial crimes.

For example, through the U.S.-EU Working Group on Cybersecurity and Cybercrime, DHS and our international counterparts develop collaborative approaches to a wide range of cybersecurity and cybercrime issues. ICE also works with international partners to seize and destroy counterfeit goods and disrupt websites that sell these goods. Since 2010, ICE and its partners have seized over 2,000 domain names associated with businesses selling counterfeit goods over the Internet. Additionally, USSS Cyber Operations Branch maintains an established collaboration of Cyber Working Groups with their international law enforcement partners in the Netherlands, the Baltic states, and Ukraine.

DHS also partners closely with the DOJ and Department of Defense to ensure that there is a whole of government approach with respect to responding to cyber incidents and threats. While each agency operates within the parameters of its authorities, our overall federal response to cyber incidents of consequence is coordinated among our three agencies. Where agency authorities overlap, as in law enforcement, protection, and response, we also directly coordinate with and support each other. This synchronization ensures that all of our capabilities are brought to bear against cyber threats and enhances our ability to share timely and actionable information with a variety of partners.

*Science and Technology*

DHS S&T supports a range of cyber security research and development efforts, targeting near-term and future capabilities that will carry through major improvements in cyber security of the homeland security enterprise.

For example, S&T contributed to protocols that help to protect Internet users from being covertly redirected to malicious websites, most critically including the Domain Name System Security Extensions technology, which helps prevent theft, fraud, and abuse online by blocking bogus page elements and flagging pages whose Domain Name System identity has been hijacked. S&T is also driving improvements through a Transition to Practice Program that will take some of the most promising federally funded cyber security technologies currently available and enable their transition into successful use.

S&T is also providing a key role in a multi-agency government wide effort directed by Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity and leading the Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience tasking to develop a national research and development plan for critical infrastructure security and resilience.

*Recent Executive Actions*

Cybersecurity remains a priority for the Administration, and while these accomplishments are significant, we need Congress to enact a suite of comprehensive cybersecurity legislation in order to be able to best meet this growing threat. We appreciate the efforts made in the last Congress to pass bipartisan cybersecurity legislation, but the inability to get this done has required the President to take executive action.

EO 13636 on Improving Critical Infrastructure Cybersecurity – issued in February of this year – supports more efficient sharing of real-time cyber threat information with the private sector. It also directs DHS to develop a voluntary program to promote the adoption of a new Cybersecurity Framework and assist the private sector in its implementation.

PPD 21 on Critical Infrastructure Security and Resilience directs the executive branch to strengthen our capability to understand and share information about how well critical infrastructure systems are functioning and the consequences of potential failures. And it calls for a comprehensive research and development plan to guide the government's effort to enhance market-based innovation.

These documents reflect input from stakeholders across government, industry, and the advocacy community. Furthermore, they help ensure that we protect individual privacy and civil liberties through transparent processes, additional stakeholder engagement – including consultation with the Privacy and Civil Liberties Oversight Board, privacy advocates and the public – and assessments releasable to Congress and the public by the privacy and civil liberties officials of the participating agencies in the cybersecurity programs envisioned by EO 13636 and PPD 21. Importantly, EO 13636 calls for us to work *within* current authorities and increase voluntary

cooperation with the private sector. It does *not* grant new regulatory authority or establish additional incentives for participation in a voluntary program.

In partnership with the Federal interagency, DHS established an Integrated Task Force to lead implementation of these executive actions. The task force has conducted more than 100 working sessions thus far and has already produced several deliverables. Among them are an Incentives Report that analyzes potential government incentives that could be used to promote the adoption of the Cybersecurity Framework, a description of critical infrastructure functional relationships, instructions on producing unclassified cyber threat reports to help critical infrastructure partners prevent and respond to significant threats, a method to identify and prioritize nationally and regionally significant cyber infrastructure assets, recommendations on incorporating security standards into acquisition planning and contract administration, and a process to expedite security clearances for the private sector.

Nevertheless, we continue to believe that a comprehensive suite of legislation is necessary to build stronger, more effective, public-private partnerships on cybersecurity. Specifically, Congress should enact legislation to:

- Incorporate privacy and civil liberties safeguards into all aspects of cybersecurity;
- Further increase information sharing, and establish and promote the adoption of standards for critical infrastructure;
- Give law enforcement additional tools to fight crime in the digital age; and
- Create a National Data Breach Reporting requirement.

DHS is committed to securing our nation from growing cyber threats and ensuring critical infrastructure is protected in partnership with the private sector, while safeguarding the public's privacy, civil rights, and civil liberties. We continue to urge Congress to take additional action to help us meet this important responsibility.

**Conclusion**

Chairman Carper, Ranking Member Coburn, and Members of the Committee: thank you for your steadfast partnership and support of DHS. Together, we have accomplished a tremendous amount to more effectively address the many threats facing the United States. But we know our work is not done and we must continue to be flexible and agile in a changing threat environment.

I look forward to working with each of you in the weeks and months ahead to build on our successes over the past ten years as we continue to meet our solemn responsibility to the American people. Thank you again for the opportunity to appear before the Committee today.

**Statement of**
**The Federal Bureau of Investigation**
**Before the**
**Committee on Homeland Security and Governmental Affairs**
**United States Senate**
**At a Hearing Entitled**
**"Homeland Threats and Agency Responses"**
**November 14, 2013**

## Introduction

Good morning, Chairman Carper, Ranking Member Coburn, and Members of the Committee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

Today's FBI is a threat-focused, intelligence-driven organization. Every FBI professional understands that preventing the key threats facing our nation means constantly striving to be more efficient and more effective.

Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and to our communities.

These diverse threats illustrate the complexity and breadth of the FBI's mission and make clear the importance of its partnerships. We cannot do it alone. To accomplish its mission, the FBI relies heavily upon its partners around the globe.

In fact, our national headquarters and local field offices have built partnerships with just about every federal, state, local, tribal, and territorial law enforcement agency in the nation. Our agents and professional staff also work closely with law enforcement, intelligence, and security services in foreign countries, as well as international organizations like Interpol.

By combining our resources and leveraging our collective expertise, we are able to investigate national security threats that cross both geographical and jurisdictional boundaries.

It is important to emphasize that the FBI carries out this broad mission with rigorous obedience to the rule of law and protecting the civil rights and civil liberties of the citizens we serve.

### Counterterrorism

Counterterrorism remains our top priority. The FBI works with our law enforcement and Intelligence Community (IC) partners to integrate intelligence and operations, and to detect and disrupt terrorists and their organizations.

As the Boston bombings this past April illustrate, the terrorist threat against the United States remains very real. We face a continuing threat from homegrown extremists, especially those who act alone or in small cells. Homegrown Violent Extremists (HVEs) present unique challenges because they do not share a typical profile, and their experiences and motives are often distinct, which makes them difficult to identify and their plots difficult to disrupt. Al-Qa'ida and its affiliates continue to encourage extremists in the West to follow this model by engaging in individual violent attacks and have already incorporated the Boston bombings in their propaganda. The Boston Marathon bombing suspects are from the North Caucasus, but the links, if any, between the bombing and that region remain unclear. We currently assess the threat from North Caucasus-based militants to the Homeland to be minimal as they remain focused on fighting against Russian security forces in the North Caucasus.

The Boston bombing also demonstrated the devastating potential of an improvised explosive device (IED) crafted from simple components, which could inspire other extremists to use such tactics. The devices used in Boston were similar in design to instructions widely available online. In addition to the Boston attack, over the past two years we have also seen extremists attempt to detonate IEDs or bombs at such high profile targets as the Federal Reserve Bank in New York, the U.S. Capitol, and commercial establishments in downtown Chicago, Tampa, and Oakland. Fortunately, these attempts, as well as many other plots, were thwarted. Yet the threat remains.

Overseas, the terrorist threat is similarly complex and ever-changing. We are seeing more groups engaged in terrorism, a wider array of terrorist targets, greater cooperation among terrorist groups, and continued evolution and adaptation in tactics and communication. Al-Qa'ida and its affiliates, especially al-Qa'ida in the Arabian Peninsula (AQAP), continue to represent a top terrorist threat to the nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, the attempted bombing of U.S.-bound cargo planes in October of 2010, and a disrupted plot to conduct a suicide bomb attack on a U.S.-bound airliner in April 2012.

Beyond the Middle East, threats emanating from Africa remain a concern to the FBI. Al-Shabaab, based in Somalia, recently attacked the Westgate Mall in Nairobi, Kenya. The FBI continues to assess that al-Shabaab lacks the intent to conduct or directly support attacks in the United States, as doing so would not be consistent with the group's strategic aims of establishing an Islamic state in Somalia and defeating the Somali and foreign troops obstructing their efforts to do so. We expect Kenya to remain the primary focus of the group's external attacks, though other nearby countries participating in military offensives against the group, such as Ethiopia and Uganda, remain at risk as well. Nonetheless, the FBI remains concerned that externally focused elements affiliated with the group are likely to aspire to attack the West and the U.S. Additionally, domestic extremists could draw inspiration from the group's propaganda and the Westgate Mall attack to employ similar tactics in the Homeland.

In North Africa, al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) continues to grow its operational reach and safe haven into Libya, and Mali, threatening U.S. and Western interests in the region. The FBI assesses AQIM, its affiliates and allies, and aspirant groups in the region pose a low threat to the Homeland in the short- to mid-term, but pose a high threat to U.S. and Western interests in the region, especially at embassies, hotels, and diplomatic facilities in

Tunisia and Libya. Since 2009, AQIM has a demonstrated capability to target Western interests, most notably through kidnap for ransom techniques. Since 2011, AQIM splinter groups, along with Libya- and Tunisia-based Ansar al-Sharia extremists, have increasingly proven their anti-Western ideologies through high-profile attacks on the U.S. consulate in Benghazi, Libya, the U.S. Embassy in Tunis, Tunisia; British oil facilities in Algeria, and a French-owned mine in Arlit, Niger. Such attacks against U.S. interests will likely continue, especially as extremists continue to fight for autonomy and control against governments which they perceive are receiving assistance from the United States.

With respect to West Africa, the FBI assesses that Nigeria-based Boko Haram does not currently pose a threat to the Homeland. Boko Haram does, however, aspire to attack U.S. or Western interests in the region. Boko Haram demonstrated its capability for such attacks in its 2011 vehicle-borne IED attack on the United Nations headquarters in Abuja, Nigeria. Current counterterrorism pressure from Nigerian military and police forces has limited Boko Haram's ability to execute various operational plans against Western targets; however, communications, training, and weapons links between Boko Haram and AQIM, al-Shabaab, and AQAP, may strengthen Boko Haram's capacity to conduct terrorist attacks against U.S. or Western targets in the future.

To combat these threats, the FBI relies upon its 103 Joint Terrorism Task Forces (JTTFs) across the nation and 63 Legal Attache (LEGAT) Offices around the world. The FBI has added approximately 70 JTTFs since 9/11. Investigators, analysts, linguists, and SWAT experts from dozens of U.S. law enforcement and intelligence agencies comprise the JTTFs. The JTTFs serve as critical force multipliers that follow up on all terrorism leads, develop and investigate cases, and proactively identify threats and trends that may impact the region, the nation, and the world.

Since 9/11, JTTFs have been instrumental in breaking up cells like the "Portland Seven," the Northern Virginia jihad group, and the Daniel Patrick Boyd cell in North Carolina. They've foiled attacks against military institutions and personnel in New Jersey, New York, Maryland, Washington, Texas, and Virginia. They have disrupted plots against government and civilian targets across the country including the al-Qa'ida plot against the New York City Subway in 2009. They have traced sources of terrorist funding, responded to anthrax and other suspected weapons of mass destruction threats, halted the use of fake IDs, and arrested subjects who possessed deadly weapons and explosives.

To better address the evolving threat, the FBI has also established the Countering Violent Extremism (CVE) Office. This office leverages FBI resources and works with federal counterparts to empower our local partners to prevent violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the United States to commit acts of violence. The FBI is leading efforts to conduct outreach, and raise community awareness, while upholding civil rights and liberties.

**Cyber Threats**

The diverse threats we face are increasingly cyber-based. Much of America's most sensitive data is stored on computers. We are losing data, money, and ideas through cyber intrusions. This

threatens innovation and, as citizens, we are also increasingly vulnerable to losing our personal information. That is why we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.

The FBI has built up substantial expertise to address cyber threats, both in the homeland and overseas.

Here at home, the FBI serves as the executive agent for the National Cyber Investigative Joint Task Force (NCIJTF) which joins together 19 intelligence, law enforcement, and military agencies to coordinate cyber threat investigations. The FBI works closely with our all our partners in the NCIJTF, including the National Security Agency (NSA) and the Department of Homeland Security (DHS). We have different responsibilities, but we must work together on cyber threat investigations to the extent of our authorities and share information among the three of us following the principle that notification of an intrusion to one agency will be notification to all.

While national-level coordination is important to securing the nation, teamwork at the local level is also essential. After more than a decade of combating cyber crime through a nationwide network of interagency task forces, the FBI has evolved its Cyber Task Forces (CTFs) in all 56 field offices to focus exclusively on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each CTF partners with many of the federal agencies that participate in the NCIJTF at the headquarters level. This promotes effective collaboration and deconfliction of efforts at both the local and national level.

Through the FBI's Legal Attache offices around the globe and partnerships with our international counterparts, we are sharing information and coordinating cyber investigations more than ever. We have Special Agents working alongside our foreign police department partners, they work to identify emerging trends and key players in the cyber crime arena.

It is important to note that we are also coordinating closely with our federal partners on the policy that drives our investigative efforts. Although our agencies have different roles, we also understand that we must work together on every significant intrusion and to share information among the three of us following the principle that notification of an intrusion to one agency will be notification to all.

In addition to cooperation within the government, there must be cooperation with the private sector. The private sector is the key player in cyber security. Private sector companies are the primary victims of cyber intrusions. And they also possess the information, the expertise, and the knowledge to address cyber intrusions and cyber crime in general. In February 2013, the Bureau held the first session of our National Cyber Executive Institute, a three-day seminar to train leading industry executives on cyber threat awareness and information sharing.

One example of an effective public-private partnership is the National Cyber Forensics and Training Alliance, a proven model for sharing private sector information in collaboration with law enforcement. Located in Pittsburgh, the Alliance includes more than 80 industry partners from a range of sectors, including financial services, telecommunications, retail and

manufacturing. The members of the Alliance work together with federal and international partners to provide real-time threat intelligence, every day.

Another initiative the FBI participates in, the Enduring Security Framework, includes top leaders from the private sector and the federal government. This partnership illustrates that the way forward on cyber security is not just about sharing information, but also about solving problems together.

We intend to build more bridges to the private sector in the cyber security realm. We must fuse private-sector information with information from the Intelligence Community and develop channels for sharing information and intelligence quickly and effectively.

In the last several years, the distribution of malicious software through networks of infected computers, or "botnets," by online criminals has emerged as a global cybersecurity threat. As a response, the FBI developed Operation Clean Slate, a broad team effort to address this significant threat. Operation Clean Slate is the FBI's comprehensive public/private approach to eliminate the most significant botnet activity and increase the practical consequences for those who use botnets for intellectual property theft, or other criminal activities.

In April 2013, the FBI implemented this plan and identified the Citadel Botnet as the highest priority botnet threat. Citadel is a type of malware known as a "Banking Trojan." This type of malicious software is designed to facilitate unauthorized access to computers to steal online banking credentials, credit card information, and other personally identifiable information (PII).

Focusing on the Citadel malware, Operation Clean Slate identified the specific actors: the coders who create the botnet, the herders who aggregate victim computers and the users who utilize the botnet. We also identified intended or actual victims of the botnet.

The FBI and its global partners then took action against Citadel. Through court ordered authorizations and leveraging industry partnerships, more than 1,400 controlling components of the botnet were disrupted, essentially ceasing its operations. Once these controlling components were rendered inoperable, it is estimated Operation Clean Slate freed more than 2.1 million robot computers from this malicious network.

The FBI must continue to develop and deploy creative solutions in order to defeat today's complex cyber threat actors. Instead of just building better defenses, we must also build better relationships, overcoming the obstacles that prevent us from sharing information and, most importantly, collaborating.

**Active Shooter Threats**

The recent shootings at the Navy Yard in Washington, D.C., the Los Angeles Airport, and the Westfield Garden State Plaza Mall, demonstrate that communities across America continue to face active shooter and mass casualty incidents. Since the Sandy Hook tragedy last December, the FBI has been working with the Department of Justice's Bureau of Justice Assistance to

provide tactical "active shooter" training to law enforcement agencies across the country. In conjunction with this training, the FBI and DOJ, working with our HHS, Education, and DHS partners, have developed an Active Shooter brochure and planning guides to complment this effort.

Over the past year, one hundred FBI agents have attended the Advanced Law Enforcement Rapid Response Training (ALERRT) school and trained other officers in life-saving tactics. The 16-hour Basic Active-Shooter course prepares first responders to isolate a threat, distract the threat actors, and end the threat. In addition, during the month of April, the FBI conducted two-day conferences and table top exercises with state, local, tribal, and campus law enforcement executives. The purpose of these conferences was to ensure that the ALERRT brought FBI field offices and law enforcement command staff together to discuss best practices and lessons learned from mass shooting incidents. We have hosted two-day conferences on active shooter situations at most of our 56 field offices nationwide followed by tabletop exercises based on real-life incidents.

These incidents have also given rise to collaboration among behavioral experts, victim assistance specialists, and other personnel to work through best practices, including how to best react to active shooter and mass casualty incidents. We are continuing our efforts with a new table top exercise specifically designed for campus law enforcement. This is an issue that impacts all of us, and the FBI is committed to working with our partners to protect our communities.

**Conclusion**

Chairman Carper, Ranking Member Coburn, I thank you for this opportunity to testify concerning the diverse threats facing the nation and the FBI's ongoing efforts to combat them. The FBI's efforts and successes would not have been possible without your support and the support of the American people. I would be happy to answer any questions you might have.

**Hearing before the Senate Committee on Homeland Security and Governmental Affairs**
**The Homeland Threat Landscape and U.S. Response**
**November 14, 2013**

**The Honorable Matthew G. Olsen**
**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 consistent support of the men and women at the National Counterterrorism Center, and I would encourage you to visit us to see our operations first-hand. I am particularly pleased to be here today with DHS Acting Secretary Rand Beers and FBI Director James Comey. We are all close partners in the fight against terrorism.

It has been just over a year since I last testified before this Committee. Last year I testified that, "Al-Qa'ida core is a shadow of its former self, and the overall threat from al-Qa'ida in Pakistan is diminished." That assessment remains true today. However, al-Qa'ida is still the ideological leader of a movement that includes affiliated groups and followers worldwide. As a result, the terrorist threat to the United States remains persistent, emanating from a dedicated and diverse array of actors.

Al-Qa'ida's core leadership in the Afghanistan-Pakistan border region is still navigating its response to ongoing events in the Muslim world and working to ensure the survival of the global jihadist movement. Additionally, political change and unrest in the Middle East and North Africa are creating opportunities for veteran jihadists to recruit and train the next generation of militants, some of whom are less dogmatic in their embrace of al-Qa'ida's ideology, yet support its anti-Western agenda. These developments are blurring the lines between terrorists, insurgents, and criminal groups operating in these regions.

Here in the United States, the attack against the Boston Marathon in April 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. Coupled with January's attack at the In Amenas gas facility and September's attack at a Nairobi shopping mall, these attacks could portend a terrorist interest in softer, less symbolic and less protected targets.

Confronting these threats and working with resolve to prevent terrorist attacks remains NCTC's overriding mission. We continue to monitor threat information, develop leads, work closely with domestic and international partners, and develop strategic plans to combat our terrorist adversaries. With our partners, we have taken important steps, but much work remains. The dedicated professionals at NCTC, along with our partners across the government and overseas, remain steadfast and committed to sustaining and enhancing the effort to protect the nation.

In the remainder of my statement, I will begin by examining the terrorist threats to the homeland and to U.S. interests. I will then describe NCTC's role in addressing these threats and some of the key initiatives we have adopted.

**TERRORIST THREAT OVERVIEW**

***Pakistan-Based Al-Qa'ida Core.*** Despite core al-Qa'ida's diminished leadership cadre, remaining members will continue to pose a threat to Western interests in South Asia and will attempt to strike the Homeland should an opportunity arise. Al-Qa'ida leader Ayman al-Zawahiri's public efforts to promote individual jihad in the West through propaganda — most recently in his 9/11 anniversary video statement—have increased. At the same time,the Pakistan-based group's own capabilities have diminished. Operationally, core al-Qa'ida has not conducted a successful operation in the West since the 2005 London bombings.

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 to these regions, encouraging cadre and associates to support and take advantage of the unrest.

The withdrawal of Coalition forces from Afghanistan may exacerbate the unsteady security trends in the country, and has the potential to create an environment in which core al-Qa'ida veterans reconstitute the remnants of the group. Al-Qa'ida's historical ties to Afghanistan make the country an attractive operating area, especially if the group can leverage its longstanding relationships with Afghan insurgents who supported it in the years preceding 9/11. At the same time, the draw of other active jihadist fronts, such as Syria, is likely to stem the flow of future al-Qa'ida recruits to the Afghanistan-Pakistan region.

***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 even after the death of its leader Hakimullah Mehsud in November. Its claim of responsibility for the September attacks against a Christian church in Peshawar that killed close to 80 civilians and a Pakistani general officer underscore the threat the group poses inside the country. TTP also remains intent on attacking the United States. TTP twice this year publicly reaffirmed the group's desire to attack the US and its allies.

The Haqqani network is one of the most capable and lethal insurgent groups in Afghanistan and poses a serious threat to the stability of the Afghan state as we approach 2014 and beyond. The Haqqani network's continued ability to launch major attacks in Kabul and the

east suggests the Haqqanis will remain a viable challenge to Afghan government control in the eastern and central provinces post 2014.

We remain concerned by the Haqqani network's continued willingness to harbor al-Qa'ida, the Haqqanis' strength in eastern Afghanistan and its close partnership with al-Qa'ida militants. The Haqqanis have conducted numerous high-profile attacks against U.S., NATO, Afghan government, and other allied nation targets. The most significant attack was the 18-hour multi-pronged assault against military, security, and government facilities in Kabul and three other cities in April 2012. We assess the Haqqanis are likely to carry out additional high-profile attacks against Western interests in Afghanistan.

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 United States 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's Affiliates: A Persistent Threat to the United States and Overseas Interests**

***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 West, its awareness of Western security procedures, and its efforts to adapt.

AQAP also presents a high threat to U.S. personnel and facilities in Yemen. In response to credible al-Qa'ida threat reporting in early August, 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. In addition, over the past year AQAP has kidnapped Westerners in Yemen and carried out numerous small-scale attacks and several large-scale operations against Yemeni government targets, demonstrating the range of the group's capabilities.

AQAP continues its efforts to radicalize and mobilize 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.

***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 US persons—mostly ethnic Somalis—who have traveled to Somalia since 2006.

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 the mid-September attack and hostage crisis at a mall in Kenya was linked to al-Shabaab, it is unknown what element of the group planned the attack. The attack demonstrated that the group continues to support targeting regional and Western interests across East Africa, as part of its campaign to remove foreign forces aiding the Somali Government.

Al-Shabaab since 2011 has lost many former urban strongholds in southern Somalia and suffered from internal strife. We do not yet know the long-term effects of the recently reported death of Omar Hammami—an American citizen who created propaganda, recruited, and fought for al-Shabaab—will have on the group and its outreach to foreign fighters.

***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, however the groups maintain safe haven in the less populated areas of northern Mali and continue to plot retaliatory attacks. Elsewhere in the region, AQIM is taking advantage of permissive operating environments across much of North Africa to broaden its reach. AQIM is seeking to collaborate with local extremists, including Ansar al-Sharia groups in Libya and Tunisia, as well as Boko Haram and Ansaru in Nigeria, which share the intent to target Western interests. In late October AQIM ransomed four French hostages for a reported payment of over 20 million Euro, which will increase the group's operational capability and further its outreach efforts.

In August, former AQIM commander Mokhtar Belmokhtar's battalion merged with local extremist ally Tawhid Wal Jihad in West Africa, establishing the new extremist group al-Murabitun, which will almost certainly seek to conduct additional high profile attacks against Western interests across the region. Belmokhtar has played a leading role in attacks against Western interests in Northwest Africa this year, with his January attack on an oil facility in In-Amenas, Algeria and double suicide bombings in Niger in May.

Since late 2012, Nigeria-based Boko Haram and its splinter group Ansaru have claimed responsibility for three kidnappings of Westerners, raising their international profile and highlighting the growing threat they pose to Western and regional interests.

***Al-Qa'ida in Iraq.*** Al-Qa'ida in Iraq (AQI), also known as the Islamic State of Iraq and the Levant, is at its strongest point since its peak in 2006 and this year has significantly increased its pace of attacks. The group is exploiting increasingly permissive security environments in Iraq and Syria to fundraise, plan, and train for attacks.

AQI has maintained an experienced cadre of operatives in Iraq. The group's amir last year initiated a campaign of attacks against prisons to free members, which culminated this July in high-profile coordinated attacks on two Iraqi prisons that freed hundreds of prisoners.

In addition, AQI continues to operate in Syria, where the group has recruited many foreign fighters, including Westerners. AQI's growing cadre of Westerners in Syria probably bolsters the group's pool of external operatives who could be used to target the west.

***Syria.*** We are monitoring the activities of several other extremist groups fighting against the Asad regime in Syria, including the al-Qa'ida-associated al-Nusrah Front. Al-Qa'ida in Iraq founded al-Nusrah Front in late 2011 to act as its operational arm in Syria, although the two groups split following a public dispute in April 2013. Al-Nusrah Front has mounted suicide, explosive, and firearms attacks against regime and security targets across the country and provides limited public services to the local population.

Al-Nusrah Front's leader, Abu Muhammad al-Jawlani, in April 2013 pledged allegiance to al-Qa'ida leader Ayman al-Zawahiri, publicly affirming the group's ties to al-Qa'ida. Many moderate opposition groups fight alongside al-Nusrah Front and other Sunni extremists in Syria and depend on extremists for resources, including weapons and training.

Since early 2012, thousands of fighters from around the world—including the United States—have traveled to Syria to support oppositionists fighting against the Asad regime, and some have connected with extremist groups, including al-Nusrah Front. This raises concerns that capable individuals with extremist contacts and battlefield experience could return to their home countries to commit violence.

Multiple actors are now present in Syria and we are focused on any non-state actors inside or outside of Syria who may seek to acquire Syria's now-acknowledged chemical weapons stockpile. The United States is monitoring the weapons sites and remains concerned about the security of these weapons given the escalation of violence in Syria. We're working to monitor and help counter those who may seek to acquire these deadly weapons.

**Other Terrorist Threats**

***Iranian Threat.*** 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.

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.

The defense of the Syrian regime is an Iranian national priority, and Iranian military forces, including individuals from the Qods Force, are in Syria working with Hizballah to bolster Asad. Iran and Hizballah have built a militia to defend the regime, which could also be used as a lever for Iranian influence if Asad were to fall, with Iraqi Shia fighting alongside the pro-regime

forces. Because of the value Iran places on defending the Asad regime, a U.S. strike in Syria could put U.S. interests, especially those in Iraq, in danger of retaliatory attacks by Iran and its surrogates.

***Lebanese Hizballah.*** Lebanese Hizballah remains committed to conducting terrorist activities worldwide and the group's activities could either endanger or target U.S. and other Western interests. The group has engaged in an increasingly aggressive terrorist campaign in recent years and will probably continue this pace of operations.

The European Union designated Hizballah's "military wing" as a terrorist organization on 22 July 2013, following the March conviction of a Hizballah member in Cyprus, a July 2012 bus bombing in Bulgaria, and the group's intervention in Syria. Since the start of unrest in Syria in early 2011, Hizballah has closely coordinated with Iran to provide a range of support critical to the Asad regime. In many cases Hizballah is no longer concealing its efforts to develop, train, and equip a sizeable pro-regime militia while it likely is also contributing thousands of its own fighters.

***Leftist/anarchist terrorist threat.*** The suicide attack against the U.S. Embassy in Ankara earlier this year illustrated the continuing threat to U.S. interests posed by politically motivated groups like the Turkish leftist terrorist group Revolutionary People's Liberation Party/Front (DHKP/C). The February attack killed a Turkish security guard at the entrance to the Embassy compound. This, together with additional attacks against Turkish government targets and the group's proclamations, demonstrate its operational viability and continuing threat to U.S. interests in Turkey.

**Homegrown Violent Extremists**

Homegrown Violent Extremists (HVEs) remain the most likely global jihadist threat to the Homeland. While the threat posed by HVEs probably will broaden through at least 2015, the overall level of HVE activity is likely to remain 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.

The Boston Marathon bombing in April underscores the threat from HVEs who are motivated, often with little or no warning, 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 use to detect commitment to violence. We are concerned that HVEs could view lone offender attacks as a model for future plots in the United States and overseas. The perceived success of previous lone offender attacks combined with al-Qa'ida and AQAP's propaganda promoting individual acts of terrorism is raising the profile of this tactic.

Many HVEs lack advanced operational training, which forces them to seek assistance online from like-minded extremists or pursue travel to overseas jihadist battlegrounds to receive hands-on experience. Recent political unrest in many parts of North Africa and the Levant,

including in Syria, affords HVEs opportunities to join militant groups overseas. Foreign terrorist groups could leverage HVEs to recruit others or conduct operations inside the US or overseas.

HVEs make use of a diverse online environment that is dynamic, evolving, and self-sustaining. This online extremist 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 an extremist identity, supplies grievances, and provide HVEs the means to connect with terrorist groups overseas.

Looking ahead, we assess HVEs probably will continue gravitating to simpler plots that do not require advanced skills, communication with others, or outside training. We assess HVEs probably will move towards more active shooter events such as Nidal Hassan's attack at Ft. Hood, the recent Navy Yard shooting, or Anders Breivik's mass shooting at a political youth camp in Norway. HVEs stress targeting military personnel, bases, facilities, recruiting stations, and places where military personnel gather.

**NCTC's ROLE**

NCTC's serves as the primary U.S. government organization for analyzing and integrating all terrorism information. As we enter into our tenth year of service, we have stayed true to our mission statement: "Lead our nation's effort to combat terrorism at home and abroad by analyzing the threat, sharing that information with our partners, and integrating all instruments of national power to ensure unity of effort."

***Intelligence Integration and Analysis.*** NCTC continues to serve as the primary organization in the U.S. government for integrating and assessing all intelligence pertaining to international terrorism and counterterrorism. NCTC has a unique responsibility to examine all international terrorism issues, spanning geographic boundaries to identify and analyze threat information, regardless of whether it is collected inside or outside the United States. To better detect and disrupt an attack, we continue to refine and improve our counterterrorism data layer and our analysts' access to intelligence from across the community. These accesses, leveraged by our skilled and diverse interagency workforce, and combined with our sophisticated analytic tools, are absolutely necessary in developing our best all-source, collaborative terrorism analysis.

***Leading the Intelligence Community's Terrorism Warning Program.*** NCTC chairs the Interagency Intelligence Committee on Terrorism (IICT), which is the Intelligence Community's terrorism warning body. The IICT—which is comprised of the "Warn 8" Agencies (CIA, DHS, DIA, FBI, NCTC, NGA, NSA, and DOS)—is responsible for the publication of Community-coordinated terrorist threat warning products including IICT Alerts and Advisories. These products warn of threats against U.S. personnel, facilities, or interests. The IICT also issues Standing Advisories for areas with persistently high threat environments, and Assessments and Memorandums on other terrorism issues. The IICT serves several thousand customers, from senior policy makers, to deployed military forces and state and local law enforcement entities.

***Watchlisting and TIDE.*** NCTC hosts and maintains the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support. NCTC has developed and maintains the Terrorist Identities Datamart Environment (TIDE) on known and suspected terrorists and terrorist groups. In this role, NCTC advances the most complete and accurate information picture to our partners to support terrorism analysts.

***Situational Awareness and Support to Counterterrorism Partners.*** NCTC supports our counterterrorism partners at both the federal and state and local levels. In particular, our unique, centralized access to intelligence information on terrorist activity enables our analysts to integrate information from foreign and domestic sources and to pass that information in a timely manner to other agencies.

***Strategic Operational Planning.*** NCTC is charged with conducting strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities. In this role, NCTC looks beyond individual department and agency missions toward the development of a single, unified counterterrorism effort across the federal government. NCTC develops interagency counterterrorism plans to help translate high level strategies and policy direction into coordinated department and agency activities to advance the President's objectives. These plans address a variety of counterterrorism goals, including regional issues, weapons of mass destruction-terrorism, and countering violent extremism.

**Key NCTC Initiatives**

In the past year, NCTC implemented several new initiatives, many stemming from past lessons learned, to advance our ability to identify and prevent terrorist attacks.

***Joint Counterterrorism Assessment Team.*** This past April, NCTC, DHS, and FBI established the Joint Counterterrorism Assessment Team (JCAT) as the successor to the Interagency Threat Assessment Coordination Group (ITACG). Since 2007, through the combined efforts of FBI, DHS, and NCTC, the ITACG set the standard for information sharing between the Intelligence Community and state, local, tribal, and territorial partners. However, because of budget constraints, the ITACG construct as codified in law was not sustainable. Recognizing the importance of preserving these crucial information sharing functions, NCTC, in partnership with FBI and DHS, established the new JCAT.

JCAT is where public safety professionals—law enforcement, emergency medical services, fire service, intelligence, homeland security, and public health officials—are making a difference in the counterterrorism community. JCAT members are state and local first responders and public safety professionals from around the country. They work at NCTC side-by-side with federal intelligence analysts from NCTC, DHS, and FBI to research, produce, and share counterterrorism intelligence responsive to state, local, tribal, and territorial needs.

JCAT is focused on producing clear, relevant, and federally coordinated intelligence on significant international terrorism events that have the potential to impact local or regional public safety conditions here at home. JCAT does so by ensuring counterterrorism intelligence

intended for those defending our communities is presented, whenever possible, in an unclassified format that resonates with the first responder and public safety communities. JCAT serves as an advocate for the first responder community, creating awareness and an understanding of the first responder's role in counterterrorism within the IC while providing advice and recommendations on how best to tailor intelligence to satisfy the needs of those protecting our communities.

***NCTC/DIA Integration Efforts.*** DIA and NCTC have a strong relationship dating back to the formation of NCTC's predecessor, the Terrorist Threat Integration Center in 2003. DIA officers, like many others from across the community, helped create and stand up NCTC. More recently, in November of 2012, NCTC and DIA signed a Memorandum of Agreement that co-located many of DIA's strategic counterterrorism analysis personnel at NCTC. As this Committee knows, this partnership provides a model within the IC for collaboration and integration and it is yielding results.

In the first six months, DIA and NCTC jointly produced over 120 finished intelligence products—meaning that the authorship included officers from both DIA and NCTC. Such collaboration allows senior policy makers and Congress to benefit from intelligence analysis informed by unique DoD expertise and NCTC perspectives in a single product.

Joint finished intelligence production is most visible, but DIA/NCTC collaboration and integration spans across the CT spectrum, from watchlisting andwarning, to support to CT operations and policy deliberations.

***Strategic Snapshot of the Worldwide Terrorist Threat to U.S. Interests.*** As part of its effort to improve overall terrorist threat situational awareness in the aftermath of the attack on the U.S. Temporary Mission Facility in Benghazi, NCTC began producing a Strategic Snapshot of the Worldwide Terrorist Threat to U.S. Interests. This graphical product is intended to display countries where NCTC assess there is a credible threat of terrorist attack against U.S. persons or facilities, or where the overall security environment causes us to assess a heightened risk of terrorism. More detailed city/region specific Counterterrorism Threat Orientation Graphics are being produced collaboratively with the support of our National Geospatial-Intelligence Agency detailees. Originally mechanisms to support State Department's diplomatic security effort, these products are now used regularly by senior customers throughout the government.

***TIDE improvements.*** This year, NCTC reduced a historic backlog of Department of State Consular Consolidated Database (CCD) records consisting of visa information on known and suspected terrorists that are already in TIDE and/or watchlisted in the Terrorist Screening Database (TSDB). NCTC reduced the backlog by 88 percent while identifying the known or suspected terrorist CCD records of greatest significance for immediate analyst processing.

In 2013, in accordance with Homeland Security Presidential Directive-24/National Security Presidential Directive-59, NCTC delivered thousands of biometric files on known or suspected terrorists (KSTs) to the Terrorist Screening Center. As a result, these KSTs will have their biometric data properly placed into the watchlisting systems of various screening agencies.

***Kingfisher Expansion.*** Kingfisher Expansion (KFE) went live in June 2013 and leverages improved technology to provide speed and accuracy to the visa adjudication process.

KFE examines 100 percent of the approximately 11 million visa applicants each year to identify any connections to terrorism by comparing applicant data to the classified data holdings in TIDE, reducing unwarranted counterterrorism security advisory opinions (SAOs) by 80 percent and saving State Department millions of dollars annually in SAO processing costs. KFE is an interagency program with a secure on-line vetting platform that allows FBI, DHS, and the Terrorist Screening Center to participate in the applicant reviews. This allows for a more comprehensive and coordinated response back to State Department.

***NCTC Domestic Representatives Expansion.*** NCTC continues to build upon its domestic representative program, having now deployed officers to serve as counterterrorism liaison representatives in ten cities around the country, including Boston and Atlanta this year. These officers partner with FBI-led JTTFs and with fusion centers, bringing the national counterterrorism intelligence picture to regional federal, state, local, and tribal officials. The NCTC representatives engage with counterterrorism partners at all levels and provide analytic insights drawn from the full catalogue of counterterrorism intelligence collection.

***Countering Violent Extremism.*** As our understanding of the threat evolves, so too must our approach to defeating it. As the April attack in Boston demonstrates, we may have little to no warning when a homegrown violent extremist mobilizes to violent action. Over the past year, NCTC has continued our work with federal, state and local officials as well as community partners to expand efforts to raise community awareness about the threat of terrorist radicalization and recruitment. This coordinated approach ensures centralized policy direction and assessment, but accommodates local and community-based programs that vary across the country. Therefore, working side by side with interagency partners, we are building whole-of-government approaches focusing on expanding government and community understanding and response of all forms of violent extremism, including al-Qa'ida-inspired radicalization to violence in both the real and online environments.

***Continued Joint Counterterrorism Awareness Workshop Series (JCTAWS).*** For several years now NCTC has been collaborating with DHS/FEMA and the FBI to conduct Joint Counterterrorism Awareness Workshops throughout the United States that enable cities to assess and enhance their response plans and capabilities in the face of evolving terrorist threats. Of note, one of our first JCTAWS events was in Boston in 2011.

JCTAWS is a two day event, typically sponsored by a municipal law enforcement agency that engages all sectors of the community. Workshop participants are briefed on current threats, case studies of past attacks and responses, and the medical community's planning efforts for a mass casualty event. NCTC develops an exercise scenario specific to the city, depicting a complex terrorist attack that uses active shooters, explosives, and coordinated communication (including manipulation of social media) to terrorize a region. Senior commanders, operational responders, and members of the private sector discuss their responses to the scenario, and work to identify shortfalls in capabilities, resources, and plans.

* * *

Chairman Carper, Ranking Member Coburn, and members of the Committee, I appreciate the opportunity to testify before you this morning, and I look forward to answering your questions.

**Post-Hearing Questions for the Record**
**Submitted to The Honorable Rand Beers**
**From Senator Tom A. Coburn, M.D.**

**"Threats to the Homeland"**

**November 14, 2013**

| | |
|---|---|
| **Question#:** | 1 |
| **Topic:** | lessons learned report |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** In June, John Cohen, now DHS acting head of intelligence, briefed committee staff on issues relating to the Boston bombing. He told staff then that DHS was "in the process of doing a significant after-action and lessons learned report" that, he said, would help the department's efforts to counter violent extremism. Mr. Cohen said it would be ready in several weeks, and that he would brief us on the effort when it was completed. Our committee has attempted to conduct a review of the events leading up to the Boston Marathon bombing. We have not received a briefing on that effort from DHS, and have been unable to get an update on whether the review was ever completed. Our aim is to figure out how we can make our systems work better to improve our ability to stop future bombings. Has your agency conducted an "After Action" review or prepared any sort of "Lessons Learned" document? If you have, will you provide those to our committee? If not, can you explain why this has not been done?

**Response:** The events in Boston have highlighted how close coordination among Federal, State, and local officials is critical in the immediate aftermath and response to terrorist attacks and reinforces the principle and value of whole community contributions, including from the general public. Both the work leading up to the Boston Marathon, in the form of bombing prevention efforts such as conducting multi-jurisdictional improvised explosive device planning and risk mitigation training as well as the quick action following the event, demonstrate the significant progress that has been made over the past ten years. Following the tragic events in Boston, DHS has identified several lessons learned, and continues to improve its practices to increase security. DHS is prepared to brief the committee on its findings, and these overall efforts.

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | TECS 1 |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Can you explain what the threshold is to create a record in the TECS database about an individual? Will you provide a copy of CBP's policy on TECS record creation to the committee?

**Response:**
*The response to this question has been classified as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and is on file in the committee offices.*

**Question:** Will you provide a copy of CBP's policy on TECS record creation to the committee?

**Response:**
*The response to this question has been classified as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and is on file in the committee offices.*

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | policies |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Can you please tell us what, if any, policies or changes you have made to improve our systems moving forward so that we are better equipped to prevent attacks like what occurred in Boston?

**Response:** DHS is continually reviewing its policies and practices related to systems that support operations, including screening and vetting, information sharing, and joint-collaboration with interagency partners. For instance, DHS had implemented several enhanced practices to inbound and outbound port of entry procedures for screening suspicious travelers prior to the attacks in Boston. Additionally, in light of the attack in Boston, DHS conducted a review of its name-matching capabilities, and identified and implemented improvements in the software used to detect variations in names derived from the Cyrillic alphabet. DHS had refreshed guidance to its officers at the JTTFs, to ensure they continue to work effectively with their interagency partners. DHS is prepared to brief the committee on these efforts.

| | |
|---|---|
| **Question#:** | 4 |
| **Topic:** | TECS 2 |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** While we don't want to track people permanently, we need to strike the appropriate balance. Currently how long should a person remain on a watch-list in TECS after being the subject of an FBI investigation?

**Response:**
*The response to this question has been classified as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and is on file in the committee offices.*

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | contracts |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** How can agencies accurately determine what material should be classified and ensure they are not over-classifying materials? Are we? If so, why? How much of the extensive increase to documents considered classified is linked to government service contracts that contain excessive proprietary information?

**Response:** Agencies, including DHS, can accurately determine what material should be classified and prevent over-classification by ensuring all original classification authorities are appropriately trained and that all original classification decisions they make are clear, precise, and promulgated in a security classification guide. Additionally, agencies can develop classification management professionals to assist original classifiers in writing guides that are clear, unambiguous, and in harmony with existing guides and that measure up against the requirements of classification. At DHS, the Office of the Chief Security Officer (OCSO) performs this role. Every original classification decision must be promulgated through a security classification guide, and every guide must be reviewed by OCSO staff before final approval to ensure classification criteria have been met. At a minimum, guides are reviewed every five years to ensure that they are still current.

In addition to addressing classification in the first instance, agencies can further prevent over-classification through a robust and viable training program directed at persons who perform derivative classifications. Individuals authorized to perform derivative classification actions must be educated and knowledgeable of the requirements and processes for performing such actions in order for them to ensure that the actions they take are consistent with the classified or unclassified status of the source materials upon which they are basing a classified decision, and thus ensuring the proper classification of information. Within DHS, all derivative classifiers are required to attend such training at least once every two years and failure to do so can result in the loss of their derivative classification authority. Furthermore, OCSO has established a Security Compliance Review Program (SCR) that reviews components administrative security classification programs at least once every eighteen months and the Department has in place a self-inspection program that requires individual offices to review their classification programs at least once per year. These SCRs and self-inspections include reviews of classified documents in all forms to assess if classification actions are proper and that classified materials created by DHS are properly marked.

Concerning the total increase in classified documents, the Standard Form (SF) 311, "Agency Security Classification Management Program Data", records the total number of agency original and derivative classification decisions. It is submitted yearly to the

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | contracts |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

Information Security Oversight Office (ISOO). Although the totals have increased over the past few years, this has been attributed to counting classified emails, webpages, and increased sharing in electronic form, whereas in past years documents were only counted if printed. As propriety information is not classified (neither being owned nor controlled by the government, thus not meeting a prerequisite for classification), none of the increase can be attributed to government service contracts containing proprietary information.

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | SPOT program |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** TSA began deploying the SPOT program in fiscal year 2007—and has since spent about $900 million—to identify persons who may pose a risk to aviation security through the observation of behavioral indicators. GAO suggests that there is an absence of scientifically validated evidence for using behavioral indicators to identify threats to aviation security. Can you tell me how we have spent almost $1 billion on a program that has no evidence of working?

**Response:** The Transportation Security Administration (TSA) disagrees with the assertion that there is no evidence that the program works and non-concurred with the recommendation to limit program funding contained within the Government Accountability Office's (GAO) recent report.

TSA behavior detection procedures, including observational assessments and the equally important verbal interaction with passengers, are an essential element in a dynamic, risk-based layered security system. Behavior detection techniques have been an accepted practice for many years within the law enforcement, customs and border enforcement, defense, and security communities, both in the United States and internationally. To that end, TSA requested a validation study, which was completed in 2011 by the Department of Homeland Security Science and Technology Directorate (DHS S&T). The validation study confirmed that TSA's program as implemented was substantially better at identifying high-risk passengers than a random selection protocol.

TSA appreciates GAO's work to identify opportunities to improve the process, and TSA will continue to work diligently to address the issues identified by GAO. TSA has already established a partnership effort with DHS S&T, academia, industry and other government and community stakeholders to enhance behavior detection and provide the tools to quantify its effective contribution to security. One such effort that has been underway since early 2012 is the Behavior Detection Optimization project, which is developing a more effective and efficient behavior detection process. TSA will incorporate revisions to the behavior detection protocol and then validate the new process beginning in the spring of 2014.

| | |
|---|---|
| **Question#:** | 7 |
| **Topic:** | FISMA |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** The DHS Inspector General recently released a report which identified problems at DHS's cyber security center, including challenges with information sharing, training, and problems that occurred during a "cyber emergency" simulation. Similarly, the Inspector General's most recent audit of DHS's compliance with FISMA found that many of the Departments components and headquarters offices weren't complying with DHS's own guidelines. Based on the problems that the DHS IG identified in DHS's cyber programs, is DHS ready to monitor and manage all other agencies' cyber security under FISMA?

**Response:** The Department of Homeland Security (DHS) has two distinct roles related to operational cybersecurity, in addition to other cyber-related efforts within the Department. The Office of Cybersecurity and Communications (CS&C) is focused on enhancing the cybersecurity posture of Federal departments and agencies as well as that of the nation's critical infrastructure through a suite of products and services. CS&C programs inform system owners and operators and establish approaches and solutions that are available to system owners and Federal Chief Information Officers' (CIO) to implement within their networks. CS&C looks at the DHS information technology network operations and security as one customer within a larger homeland security and critical infrastructure enterprise. CS&C does not have direct operational cybersecurity responsibilities within any agency, which is reserved in all cases for the Chief Information Security Officer (CISO) and appropriate agency staff. This relationship applies within DHS, as CS&C provides mission-oriented support through the provision of cybersecurity approaches and solutions and the DHS OCIO retains full responsibility for internal operations. Within this general delineation of responsibilities, CS&C has made significant progress in partnering with Federal civilian agencies to achieve tangible results. A specific case is CS&C's Continuous Diagnostics and Mitigation (CDM) program, where participation agreements are in place covering over 100 Federal agencies, including 23 of 23 CFO Act agencies. CS&C also partners with agencies on intrusion detection and prevention and incident response to great effect.

The partnership between the program side of DHS cybersecurity (CS&C) and internal cybersecurity operations (OCIO) is strong. This partnership goes beyond organizational proximity. OCIO, recognizing the sensitivity of its data and criticality of its mission support requirements, is an early adopter of CS&C programs, including CDM. DHS's OCIO is on track for inclusion in CDM contracts progressing toward award in Fiscal Year 2014. This will result in tangible and quantifiable improvements in DHS's operational security posture.

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | DHS's cyber programs |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Based on the problems that the DHS IG identified in DHS's cyber programs, is DHS ready to lead in the area of information sharing with the private sector? Why has DHS been unable to comply with the NIST cyber security standards, the same regulations the private sector are expected to adapt?

**Response:** Information sharing through partnerships is the Department of Homeland Security's (DHS) expertise and contributes to its mission. DHS is already conducting information sharing activities across all 16 Critical Infrastructure (CI) sectors. Through these partnerships DHS is able to help support the securing of our Nation. As part of the information sharing efforts, DHS builds privacy and civil liberties protections into these partnerships from the beginning.

Through programs like the Cyber Information Sharing and Collaboration Program (CISCP) and the Enhanced Cybersecurity Services (ECS) program, DHS is able works with CI entities to reduce their own cyber risk and more effectively keep sensitive data and critical systems secure. DHS continues to increase and coordinate the sharing of cyber threat indicators with private sector companies. With DHS's National Cybersecurity and Communications Integration Center (NCCIC), our Nation has a centralized location where operational elements involved in cybersecurity and communications are coordinated and integrated. NCCIC partners include all Federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The center's activities include providing greater understanding of cybersecurity and communications situational awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

For the past two years, DHS's Office of Cybersecurity and Communications (CS&C) has been working closely with stakeholders across the CI and key resources sectors, including through the ECS program to define and implement the technical mechanisms required to enable real-time (or near real-time) sharing of cyber threat information for the purposes of Computer Network Defense (CND). These open, community-defined efforts, named STIX/TAXII (Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information), are now being implemented and deployed within the Federal Government and the private sector.

For example, since April 2013, the DHS Cybersecurity Information Sharing & Collaboration Program (CISCP) has been publishing STIX-based "indicators" to its members. In addition, the NCCIC is transitioning all its products to be STIX-based by

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | DHS's cyber programs |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

the end of 2014. Within the private sector, entities such as FS-ISAC have implemented a STIX/TAXII-based intelligence repository and have been using it operationally since May 2013 to exchange indicators of malicious activity within their sector. Additionally, major information technology vendors such as Microsoft and Hewlett Packard have announced STIX/TAXII-based initiatives. By working closely with the private sector across the CIKR spectrum, DHS has begun to enable widespread automated information sharing for CND.

Additionally, DHS's Office of Intelligence and Analysis (I&A) expanded outreach and engagements for key critical infrastructure sectors, with an emphasis on providing unclassified cyber threat intelligence. I&A cyber analysis increased unclassified cyber threat presentations to key customers by 344%, from FY2012 to FY2013. In FY2013, I&A cyber analysts made 179 presentations to the private sector (e.g., Corporate Security Symposiums, Information Sharing and Analysis Center Conferences, individual trade organizations and corporations), state governors (e.g., National Governors Association, Massachusetts, Vermont), state and local leaders (e.g., Los Angeles Police Department, New York City Policy Department, State Criminal Investigative Agencies, Kentucky Homeland Security Advisor, Maryland Homeland Security Advisor), among numerous other briefings to include federal leaders and partners. I&A provided tailored analysis of cyber threat activity to various customers to develop a common, baseline understanding of cyber threats and enable decision-makers to protect against, prevent and mitigate cyber threats.

Working with these key stakeholders in the critical infrastructure and private sectors, the Administration is continuing its efforts to strengthen the security of our Nation while ensuring robust protections of privacy and civil liberties. These efforts include implementation of the President's Executive Order 13636 on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21 on Critical Infrastructure Security Resilience.

As part of Executive Order 13636, DHS is developing a voluntary program for critical infrastructure cybersecurity enhancement and the adoption of the Cybersecurity Framework in close collaboration with public and private sector stakeholders. The voluntary program will promote the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure. Specifically:

- The voluntary program will link critical infrastructure community stakeholders with DHS and other programs, services, and capabilities across the Federal Government and industry.

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | DHS's cyber programs |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

- The voluntary program will be created to support and promote the adoption of the Cybersecurity Framework developed by industry, convened by the National Institute of Standards and Technology (NIST).

To promote the use of the Cybersecurity Framework and its associated security principles and concepts, the voluntary program will provide a linkage to DHS, NIST, and other Federal Government programs and resources to strengthen the security and resilience of the nation's critical infrastructure by enhancing owner and operator cybersecurity. Outside of the Executive Order/Presidential Policy Directive efforts, DHS fully supports the standards development of NIST. For implementation of other NIST standards and best practices such as NIST Special Publication 800-53 Revision 3 security controls for all system security authorizations, DHS remains ready to assist all of our partners in implementation as requested. As to the specifics of the DHS Office of the Chief Information Officer (OCIO) implementing the controls outlined in SP 800-53, the National Protection and Programs Directorate would defer to DHS OCIO on that matter.

| | |
|---|---|
| **Question#:** | 9 |
| **Topic:** | Fort Hood |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** This Committee released a report on the Fort Hood shooting in 2009, which called for a "comprehensive approach" to address "Counter Violent Extremism" and homegrown terrorism, and that means someone should be in charge of coordinating the implementation of the national strategy. Which agency is ultimately responsible for coordinating our efforts to combat homegrown terrorism?

**Response:** The White House released the *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States* (SIP) in December 2011. The SIP articulates three primary goals: (1) enhancing federal engagement with, and support to, local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise; and (3) countering violent extremist propaganda. The SIP calls for a whole-of-government approach, and directs the Department of Justice, Federal Bureau of Investigation, Department of Homeland Security, and National Counterterrorism Center to collaborate and coordinate implementation, rather than appoint a lead agency.

The Department has responsibility for implementing a range of CVE initiatives outlined in the Administration's SIP. This role includes leveraging the Department's analytic, research, and information capabilities, engaging state and local authorities and communities to bolster pre-existing local partnerships, and supporting state, local, tribal, and territorial law enforcement and communities through training, community policing practices, and grants. DHS works closely to coordinate and collaborate on these efforts with the National Counter Terrorism Center (NCTC), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and other interagency and community partners. In addition, the Department is working with its Federal, state, local, tribal, and territorial partners to fully integrate CVE awareness into the daily activities of law enforcement and local communities nationwide.

| | |
|---|---|
| **Question#:** | 10 |
| **Topic:** | DHS programs |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** In 2011, then-Chairman of the Joint Chiefs of Staff Navy Admiral Mike Mullen stated: "I've said many times that I believe the single, biggest threat to our national security is our debt." In the current fiscal environment, Congress is going to have to make some extremely difficult decisions regarding the funding of homeland security, military, intelligence community and even counterterrorism. What DHS programs and activities would you recommend be assessed for possible reduction or elimination? What programs do you see as essential in maintaining or possibly increasing our security?

**Response:** Harmonizing like organizational functions and minimizing unnecessary duplication or overlap is a continual effort for large complex organizations. At DHS, the Under Secretary for Management provides leadership to these efforts. A review of the redundancy of administrative and mission support functions within the national capital region is underway. Further, the Office of Policy is leading the Quadrennial Homeland Security Review and DHS Strategic Plan, which also speak to ongoing efforts to mature and strengthen the Department. DHS leadership continues to work towards identifying and achieving greater efficiencies.

The DHS budgeting process prioritizes mission areas to ensure that there are sufficient funds available for programs that are essential to maintain our Nation's homeland security needs. As such, the Department's budget maintains the Administration's robust border security efforts, while facilitating legitimate travel and trade with historic deployments of personnel at our 329 ports of entry. Our budgeting also continues the Administration's efforts to more effectively focus the enforcement system and our finite resources on the identification and removal of public safety threats, criminal aliens, and other high-priority individuals, funding more than 30,500 detention beds to accommodate the current mandatory population as well as the non-mandatory Level 1 and 2 criminal populations. Further, DHS is continuing the Administration's unprecedented initiatives to defend private sector and Federal Government networks, the Nation's critical infrastructure, and the U.S. economy from cyber attacks that occur daily while keeping a steady focus on safeguarding the public's civil rights and civil liberties.

We have also endeavored to fully fund the Administration's efforts to ensure the safety of the traveling public from constantly evolving terrorist threats, both foreign and domestic, and continue the Administration's efforts to build state and local law enforcement and emergency management capabilities. We have continued funds to strengthen the Chemical Facilities Anti-Terrorism Standards and to provide robust support for the

| | |
|---|---|
| **Question#:** | 10 |
| **Topic:** | DHS programs |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

Ammonium Nitrate Security Program. Additional priorities include the Department's vulnerability assessments and security surveys of critical infrastructure (e.g., cybersecurity), as well current, groundbreaking Research and Development work to provide knowledge products and innovative technology solutions for mission needs across the homeland security enterprise.

| | |
|---|---|
| **Question#:** | 11 |
| **Topic:** | information sharing programs |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** We have seen many problems in DHS's information sharing programs. Our bipartisan PSI investigation found that DHS's fusion center program was providing little value for the federal counterterrorism mission. Earlier this year, the DHS IG reported that the Department's main solution for homeland security information sharing – the Homeland Security Information Network—has been used ineffectively. In light of the April Boston bombing terrorist attack, and September's shooting spree at the Navy Yard, how can DHS ensure that its systems and processes, including information sharing, work effectively to detect and disrupt terrorist and other threats?

**Response:** The Department believes the PSI report fundamentally misstated the role of the federal government in supporting fusion centers and overlooked the significant benefits of this relationship to both state and local law enforcement and the federal government. Despite our concerns with the Report, the Department closely examined each of the Report's recommendations, and our examination determined that most of the Report's recommendations were already addressed, or had been subsequently addressed through partnerships across the federal government.

However, building on the capabilities that have been implemented across the national network of fusion centers over the past several years, the Department has continued to deploy systems and implement processes that facilitate the sharing of information to address terrorism, as well as a variety of other threats, as exemplified in the Navy Yard shooting. For example, DHS currently uses a variety of resources and methods for sharing homeland security information with our stakeholders, including our deployed cadre of intelligence officers, as well as federally-sponsored classified and unclassified information sharing systems located at fusion centers across the country. Routine information sharing practices include providing intelligence and threat briefings to our state, local, tribal, territorial (SLTT) and private sector partners, hosting analytic chats via teleconferences and classified Secure Video Teleconferences, and sharing unclassified and classified analytic products via the Homeland Security Information Network (HSIN) and Homeland Secure Data Network (HSDN), respectively.

By sharing information via these mechanisms, our SLTT partners are better informed of the threat environment, and better enabled to identify and report suspicious activities. Additionally, joint efforts between DHS and the Federal Bureau of Investigation (FBI), such as the Nationwide SAR Initiative (NSI), help ensure that this reported information is appropriately shared with federal partners and the Intelligence Community. With timely, accurate information on potential terrorist threats, fusion centers can directly contribute to

| | |
|---|---|
| **Question#:** | 11 |
| **Topic:** | information sharing programs |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

and inform investigations initiated and conducted by federal entities, such as the Joint Terrorism Task Forces.

Through our efforts to deploy personnel and information sharing systems, train frontline personnel on indicators of threats, and enable frontline officers and analysts to collect, analyze and share information, DHS has provided our SLTT partners with the necessary capabilities to effectively identify, detect, and disrupt acts of terrorism, as well as other threats.

We remain committed to improving our ability to share the information necessary to detect and prevent attacks against the homeland, and we are working closely with our partners across all levels of government to enhance our efforts to meet this challenge.

| | |
|---|---|
| **Question#:** | 12 |
| **Topic:** | funding |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Can you define DHS' strategic mission statement and how the Department organizes priorities and funding for those priorities based on the Department's strategy?

**Response:** The first Quadrennial Homeland Security Review (QHSR) Report, submitted to Congress in February 2010, focused on defining and rearticulating what is homeland security. It set forth a unifying vision of homeland security: to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. The QHSR also established a framework of five homeland security missions to align the diverse operational activities and resources of the Department:

1. Prevent terrorism and enhance security;
2. Secure and manage our borders;
3. Enforce and administer our immigration laws;
4. Safeguard and secure cyberspace;
5. Ensure resilience to disasters.

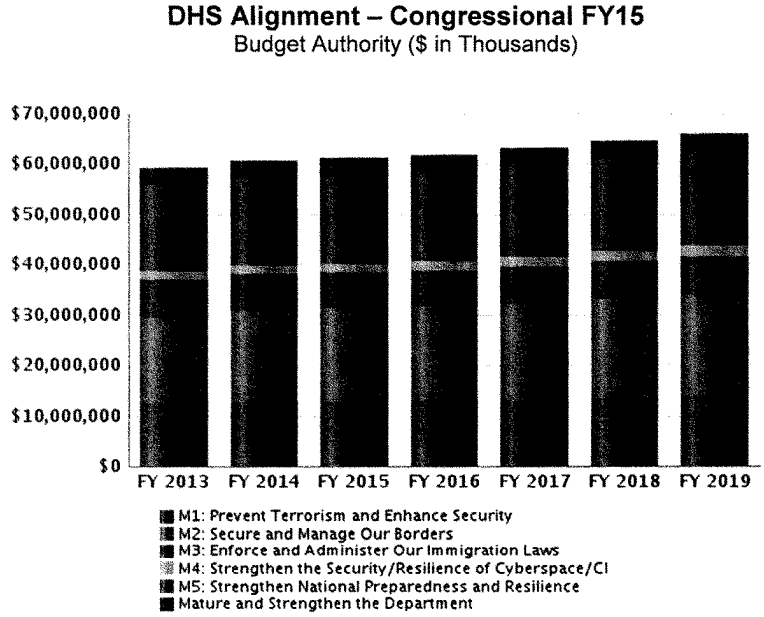
These missions are enterprise-wide, and not limited to the Department of Homeland Security. The 2014 QHSR further solidified these responsibilities.

The Department of Homeland Security uses the Planning, Programming, Budgeting and Execution (PPBE) process to manage its resources. In the planning phase, strategic goals and priorities of the Department are identified within the context of the QHSR missions, as well as other areas of focus identified by the Department, and risk assessments are conducted to prioritize the capabilities necessary to accomplish the missions of the Department. Since the first QHSR, the Department has aligned its resources through the Future Years Homeland Security Program (FYHSP) by mission and focus areas using the Department's PPBE process. As the missions and goals are refined, the FYHSP reflects the changes (see Figure 1). For FY 2017-2020, the PPBE planning phase will incorporate both the QHSR framework and the missions and goals of the DHS strategic plan along with other inputs to reflect changes in the security environment.

Components are then tasked with annually proposing a Resource Allocation Plan (RAP) that is guided by the priorities laid during the planning phase and considers the Departments' strategic mission in the context of the fiscal environment. Subsequently in the programming phase, DHS focuses on developing a five-year program plan and allocating resources to support Department mission, goals, objectives, and priorities. The decisions made during the programming phase form the basis of the President's Budget

| | |
|---|---|
| **Question#:** | 12 |
| **Topic:** | funding |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

developed during the budgeting phase leading to the application of resources for effective mission delivery during the execution phase.



| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | terrorism threats |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** If the terrorism threats remain real—as the ongoing terrorist attacks around the world suggest—is it appropriate for DHS to expand its mission from counterterrorism to "all-hazards preparedness?"

**Response:** DHS's mission, as established by statute and policy, has always included both preventing terrorism and preparing for disasters of all types. Among the five missions specified for DHS in the 2010 Homeland Security Review (QHSR) are "Preventing Terrorism and Enhancing Security" (Mission 1) and "Ensuring Resilience to Disasters" (Mission 5). The 2014 QHSR is still under way but will not significantly change these responsibilities.

Preventing terrorism is the cornerstone of homeland security. However, border management, immigration enforcement, critical infrastructure security and resilience, and all-hazards emergency management are critical homeland security mission responsibilities that reach across DHS components and the enterprise. These responsibilities relate to, but are not exclusively concerned with, terrorism.

| | |
|---|---|
| **Question#:** | 14 |
| **Topic:** | border |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** The Council on Foreign Relations reported that the apprehension rate along the border was between 40 to 55 percent. According to CRS, approximately 45,000 to 55,000 people were killed along the border between 2006 and 2012, largely due to drug-related violence. There is also a concern about the potential for drug trafficking organizations to work with other threats (like nation states or terrorist groups). Should border security become a greater DHS priority because of the potential for spill over violence from the drug trade?

**Response:**
*The response to this question has been classified as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and is on file in the committee offices.*

| | |
|---|---|
| **Question#:** | 15 |
| **Topic:** | southern border |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** What measures are DHS taking, or will be implemented, to ensure we do not allow the escalating violence to migrate across our southern border into U.S. territory?

**Response:**
*The response to this question has been classified as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and is on file in the committee offices.*

**Question:** Additionally, what is being done to track terrorist organizations who could potentially utilize DTOs in order to infiltrate the United States and carry out attacks on our soil?

**Response:**
*The response to this question has been classified as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and is on file in the committee offices.*

| | |
|---|---|
| **Question#:** | 16 |
| **Topic:** | law enforcement |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** It has been a little over a year since the Mexican presidential election; many have feared a real challenge to making sure the strong cooperation between the U.S. and Mexico trickles down to law enforcement. What needs to be done to make sure that the strong cooperation can be sustained into the future and exists on the ground where this cooperation really matters most?

**Response:**
*The response to this question has been classified as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and is on file in the committee offices.*

| | |
|---|---|
| **Question#:** | 17 |
| **Topic:** | Port Security Grant Program |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Congress has appropriated approximately $2.7 billion for the Port Security Grant Program. A recent report by the DHS IG's office states that the Department has not developed performance metrics for this grant program, even though the Post-Katrina Emergency Management Reform Act directed FEMA to develop performance metrics for all of DHS's homeland security grants. Why is it taking so long to meet a requirement in law that is seven years overdue? When will these performance metrics be developed?

**Response:** The Federal Emergency Management Agency (FEMA) has made progress in assessing grant effectiveness under the National Preparedness Goal (the Goal) and National Preparedness System (NPS), which established measurable goals and objectives that enable FEMA to systematically evaluate changes in state-wide preparedness. Each year, FEMA reports on grantees' progress toward closing capability gaps in the National Preparedness Report (NPR). FEMA submitted the second NPR to the President March 30, 2013.

For the Port Security Grant Program (PSGP), FEMA works with the United States Coast Guard (USCG) and port security stakeholders to develop and implement frameworks that enable assessment of grant award allocation against maritime risks, which vary from port to port. PSGP uses a comprehensive risk methodology to determine program grouping and grant funding allocations each year. This risk methodology captures threat, vulnerability, and consequence data for each eligible port entity, derived from subject matter experts in the Department of Homeland Security (DHS) as well as from publicly available data sources. This risk analysis provides DHS with an in-depth picture of each eligible port area's risk landscape, which informs how FEMA prioritizes grant funding to address the highest risks facing the port.

Additionally, FEMA relies on the expertise of each port's Area Maritime Security Committee (AMSC), which is comprised of stakeholders from private organizations, local law enforcement and first responders, to identify gaps or vulnerabilities in port security through the development of Area Maritime Security Plans (AMSPs) and Facility Security Plans (FSPs). Using these plans, AMSCs help ensure grant awards are applied to address the areas of greatest need, including the prevention of, detection of, response to, mitigation of, and/or recovery from attacks involving improvised explosive devices and other non-conventional weapons. The Captain of the Port reviews projects submitted for grant award in order to verify and prioritize port security gaps and vulnerabilities. Completion of PSGP projects reduces identified port security gaps and vulnerabilities.

| | |
|---|---|
| **Question#:** | 17 |
| **Topic:** | Port Security Grant Program |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

A Federal level review by FEMA and USCG validates each port's priorities and ensures that grant awardees are addressing National program priorities. In Fiscal Year (FY) 2011 and FY 2012, over $300 million was directed towards the implementation of projects identified in AMSPs and FSPs by port authorities, facility operators, and state and local government agencies that provide port security services.

In order to ensure the proper administration of grant funds, both pre- and post-award, FEMA currently tracks and reports the performance measure, "Percent of preparedness grant funds released to grantees within 270 days," for grant programs within FEMA's Transportation Infrastructure Security Branch, which includes PSGP. For FY 2013, 97 percent of grant funds were released to grantees within 270 days.

FEMA continues to work with USCG to develop and implement comprehensive outcome measures to further monitor the effectiveness of the PSGP.

| | |
|---|---|
| **Question#:** | 18 |
| **Topic:** | investigating |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Recent media reports accuse CBP of investigating people who purchased books related to how to beat a polygraph. The story describes how CBP apparently collected a list of approximately 4,900 people who were suspected of acquiring information related to beating polygraphs. According to the media report, some of these people were simply private citizens. Is this type of inquiry consistent with the Department's legal standards for investigations?

**Response:**
*The response to this question has been classified as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and is on file in the committee offices.*

| | |
|---|---|
| **Question#:** | 19 |
| **Topic:** | SPP |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** According to the Consolidated and Further Continuing Appropriations Act, which passed Congress in 2013, the TSA Screening Partnership Program (SPP) was specifically addressed in an excerpt "In addition, as TSA implements new statutory requirements for privatized screening, TSA is expected to disapprove any new contract application where privatized screening does not currently exist if the annual cost of the contract exceeds the annual cost to TSA of providing Federal screening services." Does TSA use its own internally calculated cost numbers to set a maximum allowable bid price for SPP contracts? Please provide all costs associated with airport security screening, to include the methodology and source data used in the cost calculations?

**Response:** The Transportation Security Administration (TSA) uses its own internally calculated cost number, reviewed by Department of Homeland Security Cost Analysts from the Office of Program Accountability and Risk Management, to establish a "cost efficiency" for an airport with an approved Screening Partnership Program (SPP) application. This number is published in a Request For Proposal (RFP), and potential vendors must propose a price less than or equal to this number to be eligible for an award of a screening contract. This applies to all airports whether they are already participating in SPP or new to the program. Estimating Federal screening (where security screening is provided by Federal employees) costs follows this basic model:

- An airport has a specific number of employees needed for screening as defined by the Staffing Allocation Model (SAM).
- The number of screening employees is multiplied by an airport and position specific wage rate, benefit rate, and a premium pay rate.
- Compensation for administrative staff, based on TSA staffing business rules, is included.
- New hire costs, due to expected attrition, are calculated and included.
- Uniforms, real estate, and consumable supplies are all included.
- Overhead costs are assumed based on airport headcount and included in the estimate.
- Workers Compensation is calculated and included.
- The use of the National Deployment Force is factored in based on previous TSA experience.
- Imputed costs such as Retirement, Corporate Tax Adjustment and General Liability Insurance are calculated, but not included in final estimates since these costs do not impact TSA's budget.
- An annual inflation adjustment is applied to these estimates.

| | |
|---|---|
| **Question#:** | 19 |
| **Topic:** | SPP |
| **Hearing:** | Threats to the Homeland |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

- Transition costs are included. TSA follows guidance consistent with the Office of Management and Budget (OMB) Circular A-76, calculating ten percent of the personnel costs in the base year estimate as consideration for transition costs.

There are a number of variables used in estimating Federal costs. These items are outlined in the table below and include variables such as attrition, wage rates, and facility costs. Whenever possible, TSA uses actual, airport specific data to calculate the most exact estimate possible.

| **Variable** | **Source** |
|---|---|
| Attrition | Actual prior year payroll and separation data by airport and category. |
| Staffing Allocations by pay band | SAM Model, which has been audited by the Government Accountability Office |
| Wage Rates by pay band | Actual Private contractor data and actual payroll data from the National Finance Center (NFC). Rates adjusted for inflation per OMB. |
| Benefits (Fringe Rate) Percentage by Band | Payroll data from NFC |
| Premium Pay Rate Percentage by Band | Payroll data from NFC |
| Federal Security Director (FSD) Staff | Allocation from TSA's established Federal Security Director Staff model. |
| New Hire Costs | Standard rates used by TSA for all new Transportation Security Officer hires. Based on the standard DHS Cost Model. |
| Uniforms | Standard national reimbursement allowance negotiated through collective bargaining and provided by national contract. |
| Consumables and Facilities | Actual private contractor cost, or in the case of a current federal airport, actual rent and facilities costs and consumable costs based on current budgetary allocations to the airport. |
| Other Direct Airport Costs (Admin supplies, National Deployment Force, etc.) | Annual cost estimated by various TSA program offices on demand when airport estimate is calculated. |
| Incremental General & Administrative Costs | Actual costs and budgeted allocations for relevant programs from the TSA financial system. |
| Workers Compensation | Most recent annual actual liability incurred by TSA and paid through the Department of Labor. |
| Imputed Retirement Costs | Calculated by TSA in accordance with managerial cost accounting standards. |

**U.S. Department of Justice**

Office of Legislative Affairs

Office of the Assistant Attorney General

*Washington, D.C. 20530*

June 20, 2014

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance of FBI Director James B. Comey, Jr., before the Committee on November 14, 2013, at a hearing entitled "Threats to the Homeland."

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Peter J. Kadzik
Principal Deputy Assistant Attorney General

Enclosures

cc: The Honorable Tom Coburn
Ranking Minority Member

**Responses of the Federal Bureau of Investigation**
**to Questions for the Record**
**Arising from the November 14, 2013, Hearing Before the**
**Senate Committee on Homeland Security and Governmental Affairs**
**Regarding "Threats to the Homeland"**

**Question Posed by Senator Coburn**

**1. Can you please tell us what, if any, policies or changes you have made to improve our systems moving forward so that we are better equipped to prevent attacks like what occurred in Boston? Please describe any plans you have for strengthening terrorism related information sharing?**

**Response**:

In the wake of the Boston Marathon bombing on April 15, 2013, we have reviewed both our internal procedures and our information sharing practices. For example, our internal review included the assessment of Tamerlan Tsarnaev. Although the FBI conducted a thorough assessment of Tamerlan based on the limited information provided by the Russian Government in 2011, in October 2013 we provided to all field offices guidance designed to standardize the investigative steps undertaken in all counterterrorism assessments and the manner in which results must be documented.

We have also reviewed our information sharing practices, particularly as they relate to the Joint Terrorism Task Forces (JTTFs). In the summer of 2013, then Deputy Director Sean Joyce reinforced to all FBI Special Agents in Charge the fact that JTTFs are intended to facilitate the sharing of FBI information with our intelligence and law enforcement partners for the purpose of protecting the United States against national security threats. The Deputy Director reiterated existing guidance regarding JTTF access to Guardian, which is the FBI case management system for handling initial threat information for counterterrorism, counterintelligence, and cyber incidents and suspicious activities. The Guardian application ensures that these threats and incidents are investigated, tracked, and stored during the threat mitigation period until a disposition is determined. The Deputy Director's guidance made clear that Task Force Officers (TFOs) have the same access to Guardian as FBI Special Agents, that TFOs are not restricted to using Guardian only for their assigned cases, and that they are encouraged to leverage their positions on JTTFs to stay abreast of any threats in their jurisdictions. The Deputy Director also clarified that the portion of the JTTF Memorandum of Understanding that requires Supervisory Special Agent approval for the dissemination of information is not meant to prohibit TFOs from sharing information with their home agencies.

---

*These responses are current as of 4/11/14*

The FBI is currently implementing a requirement that the managers of each JTTF meet at least monthly with the JTTF's TFOs to review counterterrorism assessments and investigations opened or closed since the last meeting. This requirement will help ensure the FBI shares all threat information proactively and uniformly with federal, state, local, and tribal partners, and will ensure our partners have a clear understanding of the potential threats in their areas of responsibility.

**2. For the Boston marathon bombings, has your agency conducted an "After Action" review or prepared any sort of "Lessons Learned" document? If you have, will you provide those to our committee? If not, can you explain why this has not been done?**

Response:

On December 31, 2013, the FBI completed an After Action Review of the response to the Boston Marathon bombing. Numerous FBI elements participated in the review, including the FBI's Boston Field Office, Counterterrorism Division, Critical Incident Response Group, Laboratory Division, Operational Technology Division, Office for Victim Assistance, and Finance Division. The review concluded with the production of a "Law Enforcement Sensitive" report that analyzed the FBI's response to the bombing. Beyond the lessons we learned from this review, which have application beyond the FBI and have, for that reason, been shared with our law enforcement and Intelligence Community partners, the report contains a great deal of detail regarding internal FBI operations. Because of the sensitivity of the operational content, it is not appropriate to disseminate the report outside the FBI. However, we would be pleased to allow Committee staff to visit FBI space at a convenient time to review the report and other materials that document the FBI's response to the Boston Marathon bombing. In addition, the FBI is reviewing the recently issued report of Inspectors General on the handling and sharing of information prior to the bombings and has taken steps to implement the report's recommendations.

**3. Can you explain what the threshold is to create a record in the TECS database about an individual? Will you provide a copy of CBP's policy on TECS record creation to the committee?**

Response:

The FBI suggests that the Committee contact the Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) for a response to this inquiry.

**4. How can agencies accurately determine what material should be classified and ensure they are not over-classifying materials? Are we? If so, why? How much of the extensive**

**increase to documents considered classified is linked to government service contracts that contain excessive proprietary information?**

Response:

In accordance with Executive Order (EO) 13526, *Classified National Security Information*, the FBI has established policies and procedures to ensure that information is appropriately classified. When an Original Classification Authority (OCA) with relevant subject matter expertise identifies information that poses a risk to national security, the OCA designates the information as classified at the appropriate level. That classification decision is then recorded, along with previous classification decisions, in a Security Classification Guide. Once this decision has been recorded, the classified content can be paraphrased, extracted, or summarized. Classification of the resulting content, which is derived from the OCA's classification, can be applied uniformly by "derivative classifiers" making future decisions involving similar circumstances and fact patterns.

EO 13526 and its implementing regulations (Title 32, Code of Federal Regulations, Part 2001) require that both OCAs and derivative classifiers receive training to ensure that their classification decisions comply with both the EO and regulations. In a September 2013 report (Audit Report 13-40), the Department of Justice (DOJ) Office of the Inspector General noted several ways the FBI classification program reduces instances of misclassification and mishandling of national security information. These included well developed and implemented classification guides and robust classification training/ awareness programs.

The Information Security Oversight Office (ISOO) monitors the U.S. government system of classification and oversees compliance with established mandates and policies. As required by ISOO, the FBI annually reports the number of derivative classification decisions made by its personnel, using a sampling method similar to that used by other Intelligence Community agencies. ISOO then publishes a report that provides analysis of the system of classification and declassification based on ISOO's review of agency programs, including agency self-reporting. ISSO does not provide for or request that agencies track classified documents in a way that would allow us to identify those linked to government service contacts that contain proprietary information. Therefore, we cannot speculate on the volume of classified documents that is entirely attributable to classified contracts.

**5. While we don't want to track people permanently, we need to strike the appropriate balance. Currently how long should a person remain on a watch-list in TECS after being the subject of an FBI investigation?**

Response:

Pursuant to Homeland Security Presidential Directive 6, the Terrorist Screening Center (TSC) maintains the U.S. Government's consolidated watchlist of Known or Suspected Terrorists (KSTs). The TSC manages the watchlisting of KSTs for the U.S. Government and through the consolidated Terrorist Screening Database (TSDB) and disseminates appropriate information to certain U.S. Government (USG) international partners. Records of KSTs meeting the minimum watchlisting criteria are continually added to the TSDB, modified to be more accurate, and removed for a variety of reasons.

The TSC exports data to DHS through a single, transactional conduit called the DHS Watchlist Service (WLS). WLS makes TSDB data available in near real-time to appropriate DHS systems, including TECS. The TECS system is maintained by DHS' CBP and is the principal system used by officers at the border to assist with screening and other determinations regarding the admissibility of arriving persons. KSTs exported to the TECS system by the TSC are maintained in the TSC's TSDB for as long as those individuals meet the minimum watchlisting criteria.

Following their review of the Boston Marathon bombings, the DOJ and DHS Inspectors General recommended "that the FBI and DHS clarify the circumstances under which JTTF personnel may change the display status of a TECS record, particularly in closed cases." The FBI concurs with this recommendation and is working with its partners at CBP to implement it.

**6. Last year, multiple news reports were published that claimed to be based on classified information that, among other things, described alleged U.S. involvement in Stuxnet, the expansion of a classified drone campaign in Yemen, and the use of a double-agent who helped thwart an AQAP bomb plot targeting Americans. Director of National Intelligence Clapper said last June that unauthorized disclosures have "profound implications for current and future intelligence capabilities and our nation's security." He went on to say that polygraph questions for personnel would be modified and that the Inspectors General of the Intelligence Community would have more authority to send a strong message that intelligence personnel will be held to the highest standards. Does al-Qaeda have a history of exploiting this kind of leaked information referred to by the DNI? How might al-Qaeda or another organization use information from these leaks to hone its tactics?**

Response:

The FBI believes al-Qa'ida in the Arabian Peninsula (AQAP) uses lessons learned from the media coverage of its activities and of U.S. operations targeting it to adjust its attack tactics. For example, in AQAP's third edition of the English-language magazine *Inspire*, AQAP indicated that, after details of the failed 2009 Christmas Day attack by the

"underwear bomber" were published in the media, it researched airport security systems to design devices that would pass through current airport security equipment.

**7. This Committee released a report on the Fort Hood shooting in 2009, which called for a "comprehensive approach" to address "Counter Violent Extremism" and homegrown terrorism, and that means someone should be in charge of coordinating the implementation of the national strategy. Which agency is ultimately responsible for coordinating our efforts to combat homegrown terrorism?**

Response:

The White House released the *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States* (SIP) in December 2011. The SIP articulates three primary goals: (1) enhancing federal engagement with, and support to, local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise; and (3) countering violent extremist propaganda. The SIP calls for a whole-of-government approach, and directs the Department of Justice, Federal Bureau of Investigation, Department of Homeland Security, and National Counterterrorism Center to collaborate and coordinate implementation, rather than appoint a lead agency.

In January 2012 the FBI established the Countering Violent Extremism Office (CVEO), which aligned the FBI with the approach outlined in the SIP. The FBI's CVEO collaborates with Federal counterparts to empower local law enforcement and community partners to help prevent violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the United States to commit acts of violence. The CVEO works to ensure that all of the FBI's CVE efforts are effectively coordinated, particularly community outreach efforts. Taken together, the FBI's execution of its individual mission along with its collaboration with other agencies contribute to the "whole-of-government" approach to countering violent extremism that is articulated in the National Strategy and the SIP.

**8. In 2011, then-Chairman of the Joint Chiefs of Staff Navy Admiral Mike Mullen stated: "I've said many times that I believe the single, biggest threat to our national security is our debt." In the current fiscal environment, Congress is going to have to make some extremely difficult decisions regarding the funding of military, intelligence community and counterterrorism. In your testimony, you described some of the programmatic choices that the Bureau is making in light of the current budget climate. Would you benefit from greater flexibility to manage your budget and prioritize how resources are allocated? Do you recommend that Congress provide any additional flexibility?**

Response:

The FBI uses a strategy management system to ensure resources are aligned to the highest priorities, addressing the greatest risks. The FBI's past, current, and planned budgets have accounted for efficiencies and program offsets to address the constrained budget environment, ensuring that our resources are directed only to programs of high priority and significant importance. The FBI's budget is appropriated into four Decision Units. This provides adequate flexibility while still permitting appropriate oversight.

**9. What lessons were learned from the April Boston bombing and the mass shooting at the Navy Yard in September in how can we better counter the threat of homegrown violent extremism?**

Response:

The April 2013 Boston Marathon bombings and September 2013 Navy Yard shooting highlight the challenges in detecting individuals intent on carrying out attacks using easily acquired weapons and simple explosives. Although the Navy Yard shooting was a criminal act with no nexus to terrorism, the tactics employed there and in the Boston attack could be replicated by homegrown violent extremists (HVEs). The Navy Yard shooting was carried out using legally acquired firearms, and the Tsarnaevs were able to construct multiple explosive devices using readily available components, including pressure cookers, fireworks, nails, and radio-controlled cars. Instructions for explosives similar to those used by the Tsarnaevs are available in AQAP's *Inspire* Magazine, which is commonly read by HVEs.

**10. What accounts for the significant rise in acts of terrorism perpetrated on U.S. soil by homegrown violent extremists?**

Response:

Al-Qa'ida-inspired U.S.-based extremists have successfully carried out three attacks in the U.S. since 2009. During that same period there has been an increase in the number of disrupted HVE plots in the United States. This increase demonstrates the FBI's focus on identifying HVEs with the intent to carry out attacks in the U.S. before they commit these acts.

The FBI is unable to identify any specific causation for year-to-year fluctuations in the number of HVE attacks or plots. We have, though, identified several factors that likely play a role in HVE mobilization to violence, including: the increased prominence of English-speaking ideologues from the West whose writings and videos are readily available on the Internet; HVEs' evolving use of the Internet and related technology; and

continued perceptions among these extremists of imbalanced U.S. government foreign policy.

**11. What is the extent of the threat from U.S. citizens who train for and actively participate in acts of terrorism and return to the United States?**

Response:

U.S. citizens who train overseas to conduct acts of terrorism pose a significant national security threat. These individuals may receive training, battlefield experience, and exposure to radical teachings while overseas and may use this upon their return to the United States to commit acts of terrorism or to influence others to participate in extremist activity. They may also associate with extremist elements overseas and maintain communication with these extremists once they return to the United States, increasing the likelihood that they may become involved in an attack on the U.S. directed by the extremist.

**12. Understanding the constitutional rights of American citizens, does the FBI have strategies in place to monitor potential threats associated with people who travel to countries known to recruit, train, and actively participate in terrorist activities?**

Response:

The FBI uses countless sources of information to identify and address potential threats to the United States, including human sources, signals intelligence, and the sharing of information with our law enforcement and intelligence partners both inside the U.S. and overseas. We pursue investigative measures against every identified threat.

**13. Can you describe how you view the work of the Joint Terrorism Task Forces? Do you think that the JTTFs and the Fusion Centers serve different roles? Are they duplicative?**

Response:

The JTTFs, which focus exclusively on terrorism, are responsible for investigations of, and operations to address, domestic terrorist threats and terrorist acts, including related domestic intelligence collection activities. The 104 JTTFs throughout the country comprise task force members from more than 440 state and local agencies and more than 50 federal agencies. The JTTFs are responsible for coordinating and sharing terrorism threat information underlying their operations with relevant state and local entities.

The role of the fusion centers is different but complementary. The fusion centers were designed to serve as analytical hubs and focal points for their respective state and local

jurisdictions for the receipt, analysis, and sharing of threat-related information among federal, state, local, tribal, and territorial partners. While fusion centers can produce actionable intelligence for dissemination, which may aid law enforcement organizations in their investigative operations, they focus on locally generated intelligence and do not conduct terrorism operations. The FBI works closely with fusion center partners, embedding FBI employees in almost 80 percent of all fusion centers.

**14. Recent media reports accuse CBP of investigating people who purchased books related to how to beat a polygraph. The story describes how CBP apparently collected a list of approximately 4,900 people who were suspected of acquiring information related to beating polygraphs. According to the media report, some of these people were simply private citizens. How does the FBI treat investigations of people involved in First Amendment protected activities (such as purchasing books or information)? Do you believe such an investigation is constitutional?**

Response:

The FBI is committed to ensuring that all investigations, including investigations designed to protect the national security, are operationally effective and respectful of privacy and civil liberties. To that end, the Attorney General has issued investigative guidelines that govern the activities of the FBI. Those guidelines provide:

> All activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General Guidelines. These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. These Guidelines also do not authorize any conduct prohibited by the Guidance Regarding the Use of Race by Federal Law Enforcement Agencies.

The Attorney General's Guidelines for Domestic FBI Operations at 13 (September 29, 2008).

The FBI has in turn issued its Domestic Investigations and Operations Guide, which states clearly that no investigative activity can be based solely on the exercise of First Amendment rights or on the race, ethnicity, national origin, or religion of the subject, or on a combination of only those factors.

Before electronic surveillance can be used during an investigation of unlawful material support to terrorism, the government must demonstrate to the Foreign Intelligence

Surveillance Court (FISC) or to a federal district court that the requisites for such surveillance have been met. In order to authorize electronic surveillance pursuant to Title III of the Wiretap Act, a federal judge must find that the government has demonstrated probable cause to believe that a certain offense, such as violation of the material support statute, has been, is being, or is about to be committed. 18 U.S.C. §§ 2516(1)(q), 2518(3)(a). Similarly, the FISC (which is composed of Article III judges) must find that the government has demonstrated, among other things, probable cause to believe the target is an agent of a foreign power. As to that determination, no United States person "may be considered . . . an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. § 1805(a)(2)(A).

In addition to those specific safeguards that Congress has created for electronic surveillance, both the FBI and DOJ conduct internal and external oversight to ensure that investigations – whether of material support for terrorism or otherwise – comply with the law. The National Security Division of DOJ and the National Security Law Branch of the FBI's Office of the General Counsel (OGC) conduct regular reviews of national security investigations to ensure compliance with the law and with internal guidelines. DOJ's Inspector General conducts reviews of various aspects of the FBI's national security program, and Congress conducts oversight through the Intelligence and Judiciary Committees in both the House of Representatives and the Senate. Finally, EO 13462 requires the FBI to report to the President's Intelligence Oversight Board, with copies to the Director of National Intelligence and DOJ, activities that may have been unlawful or contrary to executive order or Presidential directive.

**15. The FBI conducts cyber hacking against targets and has released documents that describe how it can use certain methods to obtain the identity of computers on the internet which may be masked. Additionally, court documents and news articles suggest the FBI can access a person's computer through the internet to obtain data from that computer – files, emails, web browser histories – and even activate cameras or microphones on the computer. Do you have a good understanding of the FBI's cyber investigative capabilities and techniques?**

Response:

The FBI Director has a comprehensive understanding of the FBI's cyber investigative capabilities and techniques and of the authorities governing these activities. Depending on the operational tempo within the program, the Director receives frequent, sometimes daily, briefings on computer intrusion investigations across the FBI.

The FBI lawfully conducts physical searches and electronic surveillance in predicated investigations into potential violations of federal law, operating in compliance with the federal authorities governing these activities. These authorities include the Fourth

Amendment to the United States Constitution, electronic surveillance statutes such as the Wiretap Act (18 U.S.C. §§ 2510-2522), and Rule 41 of the Federal Rules of Criminal Procedure, which provides the procedures for obtaining a search warrant.

**16. Does the FBI use the term, "network investigative techniques"? What does it mean? When operating on targets within the United States, what kinds of thresholds does the FBI apply to determine when it uses its hacking, or offensive cyber capabilities? Are they different from those of any other investigative techniques? Under what legal processes does the FBI use the capability to hack into a target's computer or network? When does it require a warrant?**

Response:

FBI investigations are governed by the United States Constitution, applicable laws and regulations, the Attorney General's Guidelines, the FBI's Domestic Investigations and Operations Guide, and other internal policies that clarify the framework of law and policy under which all investigations must be conducted. The FBI OGC and field-assigned Chief Division Counsel provide significant training and guidance on the use of our investigative authorities. The FBI's cyber activities are subject to the same legal constraints as our other investigative techniques. The FBI conducts electronic surveillance and physical searches only in predicated investigations, and we rely on appropriate judicial process and case law when we do so. In accordance with these authorities, when required by law the FBI obtains a warrant for a search or seizure when the subject has a reasonable expectation of privacy or a court order when the content of an electronic communication is collected in real time.

There are numerous different methods of gathering information from a networked computer. The FBI uses the term "Network Investigative Technique" (NIT) to refer to one such technique used to identify the location of a computer based on its Internet Protocol address. We do not know what the Committee means by "hacking" and we are, consequently, unable to answer that portion of the question.

**17. What other kinds of judicial oversight exist for these lawful hacking operations, and does it differ depending on the nature of the target? The nature of the information sought? The crimes suspected or alleged? What internal Department of Justice oversight exists regarding these cyber capabilities? Are you aware of any instances in which the FBI is believed to have improperly used these hacking capabilities? Has the FBI used its hacking capabilities against journalists, for any reason, including the investigation of leaked sensitive information?**

Response:

As discussed in response to Question 16, we do not know what the Committee means by "hacking" and we are, consequently, unable to answer that portion of the question. The FBI's cyber activities are subject to the same legal constraints as our other investigative techniques – when required by law the FBI obtains a warrant for a search or seizure when the subject has a reasonable expectation of privacy or a court order when the content of an electronic communication is collected in real time. The FBI obtains such orders with the assistance of the appropriate DOJ attorneys (often from a United States Attorney's Office). DOJ attorneys are responsible for coordinating with the DOJ sections that have relevant specialized expertise.

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Matthew Olsen**
**From Senator Tom Coburn**

**"Threats to the Homeland"**
**November 14, 2013**

**The responses to these questions are classified and can be reviewed at the Office of Senate Security (OSS-2014-0189).**

1. Can you please tell us what, if any, policies or changes you have made to improve our systems moving forward so that we are better equipped to prevent attacks like what occurred in Boston?

2. How can agencies accurately determine what material should be classified and ensure they are not over-classifying materials? Are we? If so, why? How much of the extensive increase to documents considered classified is linked to government service contracts that contain excessive proprietary information?

3. Has the National Counter Terrorism Center conducted an "After Action" review or prepared any sort of "Lessons Learned" document? If you have, will you provide those to our committee? If not, can you explain why this has not been done? Can you explain what the threshold is to create a record in the TECS database about an individual? Will you provide a copy of CBP's policy on TECS record creation to the committee?

4. One of the keys to addressing cyber security threats is better information sharing. Given NCTC's experience as the lead of inter-agency information sharing for counterterrorism, what steps are you taking to improve how we share cyber security information?

5. Last year, multiple news reports were published that claimed to be based on classified information that, among other things, described alleged U.S. involvement in Stuxnet, the expansion of a classified drone campaign in Yemen, and the use of a double-agent who helped thwart an AQAP bomb plot targeting Americans. Director of National Intelligence Clapper said last June that unauthorized disclosures have "profound implications for current and future intelligence capabilities and our nation's security." He went on to say that polygraph questions for personnel would be modified and that the Inspectors General of the Intelligence Community would have more authority to send a strong message that intelligence personnel will be held to the highest standards. Can you update the Committee on the status of any investigation into these national security leaks?

6. This Committee released a report on the Fort Hood shooting in 2009, which called for a "comprehensive approach" to address "Counter Violent Extremism" and homegrown terrorism, and that means someone should be in charge of coordinating the implementation of the national strategy. Which agency is ultimately responsible for coordinating our efforts to combat homegrown terrorism?

7. Is the growing instability in countries where violent transnational terrorism organizations control significant territory, or are allowed to operate freely because of a country's inability to control its sovereign territory, creating the necessary conditions for terrorist groups to plan and execute attacks on U.S. soil?

8. What accounts for the significant rise in acts of terrorism perpetrated on U.S. soil by homegrown violent extremists?

9. What is the extent of the threat from U.S. citizens who train for and actively participate in acts of terrorism and return to the United States?

10. Is al-Shabaab's recent attack in Nairobi, Kenya and Boko Haram's terrorist attack against an agricultural college in northeastern Nigeria, evidence that these groups are acquiring the capabilities necessary to attack the homeland?

11. Does Iran Qods Force's attempted use of what they believed to be a member of a narcotics-trafficking cartel to carry out a plot to assassinate the Saudi Arabian Ambassador to the United States represent a new terrorist tactic and a threat to U.S. security?

12. Does al-Qa'ida in the Arabian Peninsula (AQAP) still represent a growing threat after its repeated attempts to infiltrate and weaponize aviation?

13. The Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism or (SIP) has three major objectives; (1) enhancing federal community engagement efforts related to CVE, (2) developing greater government and law enforcement expertise for preventing violent extremism, and (3) countering violent extremist propaganda. NCTC has developed a training briefing for local communities, held summits, and actively supported CVE efforts at embassies, what results have come from these efforts?

14. Can you explain what the new terrorist watchlist designation "label-plus" is and how it is utilized? Are individuals considered "label-plus" believed or suspected of posing a threat to the United States? How has this new designation assisted your efforts to make the nation safer from terrorism?