S. Hrg. 114–592

FRONTLINE RESPONSE TO TERRORISM IN AMERICA

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

FEBRUARY 2, 2016

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

22–716 PDF WASHINGTON : 2017

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin *Chairman*

JOHN MCCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire
JONI ERNST, Iowa
BEN SASSE, Nebraska

THOMAS R. CARPER, Delaware
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota
CORY A. BOOKER, New Jersey
GARY C. PETERS, Michigan

KEITH B. ASHDOWN, *Staff Director*
BROOKE N. ERICSON, *Deputy Chief Counsel for Homeland Security*
COLLEEN E. BERNY, *Research Assistant*
GABRIELLE A. BATKIN, *Minority Staff Director*
JOHN P. KILVINGTON, *Minority Deputy Staff Director*
BRIAN B. TURBYFILL, *Minority Senior Professional Staff Member*
ROBERT H. BRADLEY II, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
BENJAMIN C. GRAZDA, *Hearing Clerk*

CONTENTS

WITNESS

TUESDAY, FEBRUARY 2, 2016

ALPHABETICAL LIST OF WITNESSES

APPENDIX

FRONTLINE RESPONSE TO TERRORISM IN AMERICA

TUESDAY, FEBRUARY 2, 2016

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

The Committee met, pursuant to notice, at 10:15 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

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

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. This hearing will come to order. I want to welcome all of our witnesses.

The issues that we deal with in this Committee, I think, speak right to our mission statement: to enhance the economic and national security of America. And what we have here today is a hearing that is really going to be talking about what happens at the ground level—the men and women who really spend their lives trying to protect the rest of us, and the very difficult issues that they are grappling with.

We have Chief Wally Sparks from Wisconsin here. I met him at one of our listening sessions as I traveled through Wisconsin talking about national security issues. And the way that this hearing, from my standpoint, is designed is that we want to listen to Chief Sparks, who is trying to prepare for what the rest of you have actually had to deal with, and what he is trying to grapple with. And then, as we move on down the list in terms of the testimony, you can start filling in, at that moment, whether you had an active shooter or whether it was an act of terrorism that you were having to deal with. Tell us what worked, what did not work, and what we have to really improve.

I know that, for Senator Baldwin and I, this hits pretty close to home because on August 5, 2012, there was an active shooter at the Sikh temple in Oak Creek, Wisconsin. And when you look at the webcam from Lieutenant Brian Murphy's patrol car, you see the bravery of the men and women who first respond, who rush into danger.

Now, fortunately, Lieutenant Brian Murphy is alive today, but he was shot 15 times by the perpetrator of that heinous crime. And then Officer Sam Lenda also came on. You can see, again, in the video, the bravery of the men and women.

So I think that it is the responsibility of this Committee to make sure that the men and women who capably and courageously protect our security have the tools and the resources to perform that task. That is really what this hearing is about. What tools and resources are required from a Federal Government standpoint? How do we prioritize that spending?

The Department of Homeland Security (DHS) has about $1.6 billion appropriated for grants and the Department of Justice (DOJ) has appropriated about half a billion dollars. That is about $2 billion that we allocate for grants to help folks like you. It sounds like a lot of money, but in a Federal budget that is starting to approach almost four thousand billion dollars—it is about $3.7 trillion right now—that is about 0.05 percent of our Federal budget.

Now, I think that the defense of this Nation, the defense of our homeland, is a top priority of the Federal Government. I think that we need to prioritize that spending and put that at the top of the list.

So, with that, I will turn this over to Senator Carper, and then we also have Senator Heitkamp and Senator Baldwin who would like to make some brief opening statements as well.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you very much, Mr. Chairman, for holding this hearing. I want to say thank you to Senator Baldwin and Senator Heitkamp for proposing this in the first place and also thank you to all of you who came here to make it real for us. Thank you for what you do with your lives and for your service to your communities and to our country.

Since September 11, 2001 (9/11), the Federal Government has worked hard to ensure that those on the front lines in this country—our police officers, our firefighters, and our emergency medical personnel—are better prepared to help prevent and respond to terrorist attacks and natural disasters. For example, we have helped local officials develop response plans for mass casualty events. We have also helped train thousands of law enforcement officers. And we have helped build a network of fusion centers, as you know, to deliver more timely information to our first responders.

Of course, we have also provided, as the Chairman has alluded to, grant funding for equipment, for personnel, for training, and for other needs. I am pleased that the spending bill that we just passed in December, signed by the President, contains over $1 billion in grant funding to help States and localities prepare for and respond to terrorist attacks and other disasters.

The recent tragedies in Paris, Boston, Chattanooga, and San Bernardino, however, are a stark reminder that we must remain vigilant and ensure as best we can that our first responders are ready for anything that might come their way.

That is why we will be paying close attention next week to the President's Fiscal Year (FY) 2017 budget request. We need to make sure that it provides the selfless men and women who keep us safe with the resources that they need to save lives and stay ahead of the threats that we face as a Nation.

Today's terrorist threats are very different from those that we experienced on 9/11.

Today, we unfortunately know that one or two people with an assault weapon or a homemade bomb can create unimaginable havoc and throw a whole city into chaos and turmoil. Cities like New York, Boston, and Washington, D.C. have been dealing with terrorist threats for quite some time. We know that, with the help of online radicalization, a terrorist attack can happen anytime, anywhere.

I look forward to hearing from all of our witnesses today about how Congress can further help communities, both large and small, to be better prepared for the type of terrorist attacks that we are witnessing today, such as active shooter events.

I also want to hear about what else we could be doing to stop homegrown terrorism and, extremism—something that I know all of our witnesses are familiar with.

Last December, I introduced legislation to strengthen the Department of Homeland Security's efforts to work with community leaders in identifying and preventing homegrown terrorist threats. It is my hope that we can move this legislation soon, so that the Department is better equipped to counter the hateful messages put out by the Islamic State of Iraq and Syria (ISIS) and other terrorist groups.

Again, we thank you all for joining us and a special thank you to Senators Heitkamp and Baldwin. Thank you.

Chairman JOHNSON. Senator Baldwin.

OPENING STATEMENT OF SENATOR BALDWIN

Senator BALDWIN. Thank you, Mr. Chairman. I want to thank you and Ranking Member Carper for so quickly responding to Senator Heitkamp's and my request to hold this important hearing.

Like many of my colleagues, I hear from constituents frequently about their very real fears of being attacked in their own communities—and these concerns are not unwarranted.

Just last week, in my home State of Wisconsin, a terrorist attack was thwarted. A 23-year-old man had a vicious plan to kill, he said, at least 30 people at a Masonic temple in downtown Milwaukee. In my initial conversations with the Federal Bureau of Investigations (FBI), officials indicated that the fusion centers and the FBI databases, such as eGuardian, which allows law enforcement to share intelligence, were very useful in thwarting this planned attack.

In my view, we need to find ways to expand the use of these tools, while certainly also guarding the privacy of our citizens.

We were fortunate in this case, as we have been in others, in preventing the attack. However, there will be undoubtedly more attempts to disrupt our way of life. We have to remain vigilant and ensure that our first responders have what they need to prevent attacks and respond to them if they do occur.

One of the things that we have been taught in recent years is that we must be able to prepare for the unthinkable. If you think about 9/11, up until that point, security for commercial flights was not designed to address the methods that were used by those attackers.

I am working to address a similar blind spot by improving the safety and security of trains that transport hazardous materials. Often more than a mile long, these trains carry volatile crude oil

and other materials past the back yards of my constituents and through our downtowns, which are densely populated urban areas. And while I am proud to have made some headway in including two provisions in our recently passed highway bill to improve first responder access to information in advance about these trains, I feel that there is still a significant safety concern for our citizens.

So, I look forward to hearing from all of our witnesses today about what we can do. I hope that we have some take-homes after this hearing and that we have specific actions that the Federal Government can continue to take to address and assist first responders in their tireless efforts to respond to emergencies and keep Americans safe.

Thank you for all that you do, and thank you for being here.

Chairman JOHNSON. Thank you, Senator Baldwin.

I have had other requests, so let us keep this short, OK? Senator Heitkamp, 2 minutes.

OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. Thank you, Chairman Johnson and Senator Carper for agreeing to hold today's hearing.

As Senator Baldwin has said, once Paris happened, the first response that I had was: What if I were North Dakota's Attorney General (AG) responsible for the Bureau of Criminal Investigation? And how well would we perform, compared to the people in San Bernardino? How well prepared would we be? And you add that on top of these horrific attacks. No part of our country is immune. No part of our country is somehow exempt from this happening. It is not the left coast or the right coast. It can happen right in the heartland, and we found that out when, in 2015, the Islamic State of Iraq and the Levant (ISIL) declared the Minot Air Base, which is responsible for intercontinental ballistic missiles, a terrorist target.

And so, I am curious about where we go from here. Do you get enough information from the Federal Government? Are they sharing information? Are there turf protections? Are we, in fact, training our first responders to, first off, keep themselves safe and not do things that put themselves at unnecessary risk, but also to contain the event? What are the challenges that you have, as people who think about this, immediately after this event? What are you doing today? And how can we help? How can we help change outcomes? How can we be better partners with those men and women who will always be our first responders: the State and local people who are on the front lines?

So thank you for everything that you do. Thank you for appearing today. And I look forward to hearing more, learning more, and helping to build a stronger Federal-State-local partnership to protect all of the citizens of this country.

Chairman JOHNSON. Senator Tester.

OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. Thank you, Mr. Chairman. I appreciate the flexibility. I want to thank you, the Ranking Member, and Senator Baldwin and Heitkamp for this hearing. I want to thank the panel members here today. I appreciate the work that you do. It keeps

this country safe and, quite frankly, we need to defeat ISIS, but we also need to protect our civil liberties. And I think that you guys know that, as we move forward. And we protect civil liberties by employing best practices and making sure that the Federal Government gives you the resources that you need to be successful.

It was about a year ago that we had some in this body who turned funding for DHS into a political football. That is unacceptable. Quite frankly, you need consistency, you need continuity, and you need predictability. As first responders and emergency personnel at the State and local level, you are on the front lines of fighting terrorism in this country.

So, as this hearing is going to demonstrate, we need to be serious about this issue—not play political games with it—and give you guys the resources that you need, so that you can do your jobs and so that we can hold you accountable for those jobs.

Thank you very much, Mr. Chairman.

Chairman JOHNSON. Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Mr. Chairman, I thank you and Senator Carper for holding this hearing. We appreciate you all for being here.

I just was in Ohio meeting with some of our folks who are local law enforcement in central Ohio, the Columbus area, who are part of the fusion center. These are county officials and city law enforcement officials. And my question to them was the same thing that I always ask our local law enforcement: Are these fusion centers working as a two-way communication?

Usually this panel is populated by Federal law enforcement officials, and that is good. And we bring them up, and we talk to them about what they are doing. We have three fusion centers in Ohio—one in Columbus, one in Cleveland, and one in Cincinnati. I also met, by the way, with the FBI last week. Our regional office covers half of Ohio. And my concern is that, from what I am hearing from local law enforcement, it is sometimes a one-way street. In other words, local law enforcement is providing information, which is important, but often they have a difficult time getting that information back.

So what I am interested in hearing today, particularly, Mr. Chairman, is what kind of information flow do you see coming from the Federal Government back to you? That is where I think that we can be the most helpful to you in ensuring that the citizens that we represent are safe.

Thank you.

Chairman JOHNSON. Thank you, Senator Portman.

I ask that my written statement be entered in the record, without objection.[1]

Senator Baldwin mentioned the attack that was thwarted on the Masonic temple in Milwaukee. I just wanted to very briefly read quotes from the foiled perpetrator, Samy Mohamed Hamzeh. These are excerpts of quotes that he gave to an FBI informant.

"I am telling you, if this hit is executed, it will be known all over the world. The people will be scared, and the operations will in-

[1] The prepared statement of Senator Johnson appears in the Appendix on page 39.

crease. This way we will be igniting it. I mean, we are marching at the front of the war, and we will eliminate everyone."

That is what this hearing is about. That is the enemy that we face. That is the mindset of these people who want to slaughter Americans in our own homeland.

So, again, thank you all for your testimony and for your service to your communities, to your States, and to this Nation.

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

Chief SPARKS. I do.

Commissioner BRATTON. I do.

Chief KERR. I do.

Mr. DAVIS. I do.

Mr. GHILARDUCCI. I do.

Chairman JOHNSON. Please be seated.

Our first witness is Chief Wally Sparks. Chief Sparks is the chief of police of the Everest Metro Police Department (PD) in Wausau, Wisconsin. The department serves three communities with a total of 18,000 residents. He has 30 years of experience in law enforcement and currently serves as president of the North Central Chiefs of Police Association. Chief Sparks.

TESTIMONY OF WALLY SPARKS,[1] CHIEF OF POLICE, EVEREST METRO POLICE DEPARTMENT, WESTON, WISCONSIN

Chief SPARKS. Good morning. I would like to thank all of you for this invitation. I am truly honored to be able to speak before this Committee today. When I was advised of who I was testifying with, and especially who I was testifying in front of, I was quite surprised that a local police chief from Wisconsin was included in this group.

But then, as I looked at the subject matter of the hearing and realized how the topic of terrorism in America impacts each and every single law enforcement officer in this country, I finally understood why it was important for me, or somebody like me, to be here.

I am sure that nobody on this Committee has ever heard of the Everest Metro Police Department before, yet when it comes to my distinguished colleagues, just the abbreviation of the New York Police Department (NYPD) is all that is needed, and everyone knows exactly what we are talking about.

But as I began to put that into perspective, I realized that there is only one NYPD—and only one Los Angeles Police Department (LAPD) or Chicago PD, for that matter. They essentially have no peers in this country. Everest Metro PD, on the other hand, probably mirrors similarly-sized departments and communities in each and every State. When I look at the States that each of you serve and represent, I imagine that every one of you has your version of an Everest Metro PD or a Marathon County.

---

[1] The prepared statement of Chief Sparks appears in the Appendix on page 43.

And here are just a few statistics that underscore that point: 84 percent of all sworn officers in the United States belong to local police and sheriff's departments. When it comes to local police departments, 86.2 percent have less than 50 officers and 72.8 percent have less than 25 officers. For sheriff's departments, 77 percent have less than 50 deputies and 58.3 percent have less than 25 deputies. Perhaps the most telling statistic is that 49 percent, or almost half, of all law enforcement agencies employ fewer than 10 full-time officers.

I provide these statistics because I feel that it is important for this Committee to understand that, while the events in larger metropolitan areas tend to dominate the headlines, the majority of policing efforts occur in smaller communities. The size of a law enforcement agency can have a significant impact on the delivery of policing services in a community, particularly when discussing threats like terrorism.

So while I speak for our particular department, I am probably echoing the voices of thousands of other local police chiefs and sheriffs across this Nation who face the same concerns and challenges that I do.

Even though our department is staffed very lean with 25 officers, we are still able to provide a relatively high level of training, which you will find included in my written testimony. This is likely not the case for those 49 percent of departments with less than 10 officers, however.

We also understand that terrorists typically look for soft targets, and they are learning and adjusting to how we, as law enforcement, respond to threats. I think that there has been a false perception in many communities, people think, "It would never happen here." But that reality is changing, with law enforcement leaders across the country now remarking, "It may very well happen here, and if it does, are we prepared?"

So the first emphasis should be on making sure that all of our law enforcement officers are given the proper training and equipment needed to respond to such an event. There is no Federal blueprint on what every law enforcement officer should be trained in nor on the necessary equipment needed for a response.

There should be more of a coordinated effort between the Federal, State, and local agencies to make sure that local agencies are properly trained and equipped. Failure to address this will result in greater loss of life when these incidents occur and will likely spur more attacks on smaller communities as terrorists realize that they offer relatively soft targets.

The other key piece lies in effectively engaging and utilizing all law enforcement officers in the effort to prevent attacks. In the wake of the San Bernardino incident, there has been a significant focus on the "If you see something, say something" campaign. These calls will likely come into local PDs as suspicious activity complaints. If the local law enforcement agencies are not aware of critical information pertaining to subjects in their community who are on the State or FBI's radar, then we are missing a key piece of the preventative puzzle.

In my 30-plus years in law enforcement, dialogue with the Federal agencies has generally been a one-way street. This has im-

proved with increased efforts to expand information sharing through the creation of fusion centers and Joint Terrorism Task Forces (JTTFs). However, the information gap still exists.

We need law enforcement leaders that will break down parochial boundaries and cut through bureaucratic policies and red tape. We must build closer relationships at every level and push critical information down to our frontline officers, if we are going to successfully thwart attacks. Our officers need information in real time so that they can properly assess potential threats and respond accordingly.

I want to thank each of you for your valuable time today, and I look forward to answering any questions that you may have.

Chairman JOHNSON. Thank you, Chief Sparks.

I originally mentioned the dashboard camera from the Oak Creek incident, but with our next witness I also have to mention the iconic pictures of the brave men and women of the NYPD, the New York Fire Department (FDNY), and the Port Authority of New York and New Jersey (PANYNJ), as they walked up the stairs of the World Trade Center (WTC), walking into danger. That is really, again, why we are so appreciative of your efforts.

Our next witness represents those fine men and women. Commissioner William Bratton is the 42nd police commissioner of the city of New York, the second time he has held the post. Mr. Bratton served as the Los Angeles police chief from 2002 to 2009, making him the only person ever to lead the police agencies of the two largest cities. Commissioner Bratton.

TESTIMONY OF THE HONORABLE WILLIAM J. BRATTON,[1] POLICE COMMISSIONER, NEW YORK CITY POLICE DEPARTMENT, NEW YORK, NEW YORK

Commissioner BRATTON. Good morning. My thanks to the Committee for the opportunity to speak with you today.

The issue before us, the frontline response to terrorism in America, is more pressing than at any time since 9/11. We believe that New York City, where I am the police commissioner, remains the top target for terrorists in the United States. Since the first bombing of the World Trade Center in 1993, New York City has been the target or nexus for at least 20 terrorist plots—more than any other American city. There have been four major cases in just the past 2 years.

Since 9/11, the NYPD has spent hundreds of millions of dollars in Federal funding, city and State monies, and private grants to counter that threat. My predecessor as police commissioner, Raymond Kelly, oversaw the creation of a sophisticated intelligence and counterterrorism capability. It was highly capable, but it was limited by significant head count restrictions, even though it was staffed with more than 1,000 personnel. Over the past 2 years, Mayor Bill de Blasio, whom I work with, has addressed that by providing the largest personnel and equipment allocations in the NYPD's history. Because of these allocations, we are evolving in order to face the increasingly diffused and complex threat picture.

[1] The prepared statement of Commissioner Bratton appears in the Appendix on page 52.

That picture now includes ISIS and lone-wolf actors—threats that barely existed 2 years ago and certainly did not exist on 9/11. These entities—ISIL and others—attempt to attract recruits through promises of valor, belonging, and empowerment. While we are always on guard for the spectacular al-Qaeda-style attack, with ISIS, we have seen a shift toward low-tech, low-cost, and high-impact attacks, oftentimes inspired and not directed by ISIS. November's Paris attacks left 130 people dead. In San Bernardino, 14 were killed. In New York City, this past spring, we saw three separate plots—all influenced by ISIS—to either behead people, bomb public events, or attack police, specifically.

But we cannot address these threats without partners. Two years ago, I directed John Miller, my deputy commissioner for intelligence and counterterrorism, to execute a "collaborative reset" with our closest allies: the FBI, the Secret Service, DHS, FDNY, and PANYNJ. Today we believe that we have seamless relationships with all of these agencies. By way of example, the FBI sits in on the NYPD's intelligence case meetings, and we sit in on their meetings. We have also worked to improve the NYPD's intelligence capabilities.

For more than a decade, with the help of the New York City Police Foundation, we have placed NYPD liaison officers overseas, where they work with and learn from local law enforcement agencies. We currently have 11 stations and have recently added one in Australia, as well as seconding an officer to Europol. By getting real-time, on-the-ground insight into overseas terrorist attacks—in Tunisia, France, Australia, and Canada—the liaison program has helped us redesign our tactical posture in New York City.

Given the nature of the threat, however, intelligence must be accompanied by improved response and prevention capabilities. Our primary asset in this regard has been our Emergency Service Unit (ESU), the best trained police officers in the world. But ESU is small, fewer than 600 officers, and needs to be mobile. So for years, critical sites in New York were instead guarded by patrol officers who were borrowed each day from routine precinct assignments. These officers were neither trained nor equipped to counter the type of threats that they were deployed against. With the help of Mayor de Blasio and the New York City Council, we created the Critical Response Command (CRC). This new unit, CRC, is a dedicated team of over 500 specially-trained officers with special weapons and enhanced body armor and vehicles. They are briefed on the latest intelligence, deployed daily to potential terrorist targets, and prepared to mobilize for active shooter or terrorist events.

We have also revamped our citywide task force, the 800-member Strategic Response Command, which is primarily used for crime response and disorder control. They, too, have been trained and equipped for the new threat picture—all of them are equipped with long guns, for example.

Today, we have 1,800 officers who are capable of being deployed with special weapons across the city. That capability is unmatched by any other city.

Despite this, it remains likely that the first officers on the scene of any event will be patrol officers. Accordingly, we have already trained over 3,500 of our officers in active shooter tactics in a 2-

day training. We will eventually be training all 35,000 officers. In the training, officers learn how to form small "contact teams" and move toward the threat, with the aim of reducing the gunmen's "time on target" and saving lives. We will continue the training until all of our patrol officers have been trained.

And through our 16,000-member Shield Program, a public-private partnership, we have already trained 20,000 civilians in what to do—run, hide, or fight—if they find themselves in such a situation. But, again, these threats cannot truly be addressed without partners. For example, we have worked with the New York City Fire Department to develop ways to get to the victims of a Paris-style or Mumbai-style attack as quickly as possible. The Rescue Task Force uses the new tactical teams that we have developed to provide force protection for paramedics in "warm zones" where shooting has ended, while other teams—primarily ESU officers—go after the terrorists or gunmen simultaneously in "hot zones."

Our efforts go far beyond these particulars, but being mindful of time, my descriptions of a small number of others will be very brief.

We have expanded the number of our bomb detection K–9 dogs, known as "vapor wake dogs." We have added almost $160 million of technology, including the issuance and development of smartphones to all 36,000 officers. The apps on these devices have been paid for, in many instances, by Department of Homeland Security grants. It is technology unrivaled by any police organization in the world.

We also conduct many multi-agency tabletop exercises, which we have had the good fortune to have the Secretary of Homeland Security recently attend in New York.

And under the leadership of FBI Assistant Director Diego Rodriguez, the 35-year partnership in our Joint Terrorism Task Force—the first one in America—continues. One hundred of my detectives are assigned to that unit.

New York City faces threats like no other and has invested like no other, in terms of dollars, personnel, and partnerships.

I, along with my colleagues, would be happy to answer your questions relative to this testimony and any other issues that you might have interest in. Thank you.

Chairman JOHNSON. Thank you, Commissioner Bratton.

Our next witness is Rhoda Mae Kerr. Ms. Kerr is a fourth generation firefighter and currently serves as the fire chief of the Austin Fire Department. She is also president of the International Association of Fire Chiefs (IAFC) and the vice president of the Metropolitan Fire Chiefs Association. Ms. Kerr.

TESTIMONY OF RHODA MAE KERR,[1] PRESIDENT AND CHAIR OF THE BOARD, INTERNATIONAL ASSOCIATION OF FIRE CHIEFS, AUSTIN, TEXAS

Chief KERR. Thank you. Good morning, Chairman Johnson, Senator Carper, and Members of the Committee. I thank you for allowing me to testify here today. I am honored that I get to be the lone representative of the fire service in this great country.

[1] The prepared statement of Chief Kerr appears in the Appendix on page 55.

The International Association of Fire Chiefs represents more than 11,000 members and leaders of the Nation's fire, rescue, and emergency medical services (EMS). It is important to recognize that the terrorist threat is evolving. The attacks on 9/11 were carried out by a foreign terrorist group using a coordinated strategy. The attacks were designed to generate media attention and public fear.

As you mentioned, over the past years, we are seeing a different terrorist threat. The incidents in Boston, Paris, Garland, Chattanooga, and San Bernardino used a variety of tactics. They were carried out by lone wolves or smaller groups of individuals. They used tactics like gunfire and explosives. In some cases, they may have communicated with overseas actors. But in all cases, the planning for these attacks was hard to detect.

The Nation's fire and emergency service is adapting to respond to both large-scale and localized threats. For example, we worked with our law enforcement partners and other stakeholders to remove silos that were common prior to 9/11. Also, the IAFC and other organizations are educating our members and developing resources to help prepare for the wide variety of threats. We look forward to partnering with Federal, State, tribal, and local agencies, as well as other stakeholders, to protect our communities.

In order to prepare for this new threat environment, local fire departments require accurate information about threats to our jurisdictions. Federal agencies like DHS and FBI can educate us about the new tactics, techniques, and procedures that terrorists use. Because many fire chiefs do not have security clearances, this information should be transmitted at the For Official Use Only (FOUO) or unclassified level. We need to be aware of what the terrorists' plans are, not the sources or the methods used to obtain them.

Like many major fire departments across the country, I have firefighters stationed at my local fusion center. However, there still needs to be greater fire and EMS involvement in fusion centers. Also, the IAFC recommends that fire chiefs reach out to local FBI Joint Terrorism Task Force offices and local law enforcement agencies to stay informed.

We also support the National Counterterrorism Center's (NCTC's), Joint Counterterrorism Assessment Team, which invites first responders to work with Federal intelligence analysts.

Fire departments can be partners in the information-sharing system. The IAFC encourages fire departments to take part in the Nationwide Suspicious Activity Reporting Initiative. Much like evidence of domestic abuse, firefighters can report evidence of suspicious activity, such as caches of explosives or civilians asking for details about emergency response procedures.

Fire and EMS departments also can educate law enforcement agencies about evidence of the use of fire or hazardous materials as weapons. Local fire and EMS departments also need to plan and exercise for the response to a major terrorist attack. They must develop capabilities to provide rapid on-scene care, triage, and transport to patients. They must also plan an exercise with local law enforcement officers, emergency management personnel, and public health officials for these events.

Command and coordination are important aspects of an effective response. The IAFC supports the implementation of the National Incident Management System (NIMS). NIMS implementation requires constant use and preparedness exercises to ensure its adoption by all emergency and support functions.

Many fire and EMS departments also have mutual aid agreements with surrounding jurisdictions. These agreements support localized and regionalized planning and interoperability. For example, specialized response capabilities, like a Hazardous Materials (Hazmat) Team, can be shared in a region.

An interoperable communications system is also a vital component of an effective response, and we thank Congress for its leadership in allocating that 20 megahertz (MHz) in the 700 MHz band and for its $7 billion to help build a nationwide broadband network. The First Responder Network (FirstNet) is expected to focus on data communication first, and then, to develop voice communications capability in the future.

In the meantime, local jurisdictions must rely upon the land mobile radios, and there are several large cities, Boston included, that still rely upon the T-band for interoperable communications. We encourage you to look at the statutory requirements that are going to require them to sell that T-band network.

I am aware of the time here, so I am going to try to wrap up my remarks very quickly.

In order to respond to the wide variety of terrorist threats, the Federal Government provides grants like the Urban Areas Security Initiative (UASI) and the State Homeland Security Grant Program for specialized equipment, training, and exercises. Local fire and EMS departments use this funding to build and sustain mass casualty and hazmat response capabilities. In addition, these funds are used to staff fusion centers, and the grants also provide a vital incentive for stakeholders to collaborate on terrorism response planning.

Again, as mentioned, it is important to note that the public can play a vital role in terror response. The Stop the Bleed campaign is working to educate the public about how to provide hemorrhage control with the use of tourniquets during a terrorist attack or an active shooter event. Local fire and EMS departments can build upon public education programs like Austin's "Do Your Part" program to provide the training.

I would like to thank Congress for its focus on homeland security preparedness for first responders, and I am going to thank you all. I am going to close out because I am over my time. I am going to thank the Committee for the ability to represent the fire and emergency service today. The terrorist threat has evolved, and the Nation's fire and EMS systems and departments are adapting to meet this threat. In order to be prepared, it will require a partnership of Federal, State, and local agencies, along with the private sector and the American public. And I look forward to working with you all on these efforts.

Thank you.

Chairman JOHNSON. Thank you, Chief Kerr.

Our next witness is Ed Davis. Mr. Davis is the president and Chief Executive Officer (CEO) of Edward Davis, LLC, a security

and business strategy firm. Mr. Davis served as the police commissioner of the city of Boston from December 2006 until October 2013 and he led the local response to the 2013 Boston Marathon bombing. Mr. Davis.

TESTIMONY OF EDWARD F. DAVIS III,[1] CHIEF EXECUTIVE OFFICER, EDWARD DAVIS, LLC, AND FORMER COMMISSIONER OF THE BOSTON POLICE DEPARTMENT, BOSTON, MASSACHUSETTS

Mr. DAVIS. Good morning, Chairman Johnson, Ranking Member Carper, and distinguished Members of the Committee. Thank you for inviting me to participate in the "Frontline Response to Terrorism in America" hearing. This is a critically important topic that touches each and every one of us and is in the forefront of the daily news across the country and throughout the world. It may be the active shooter incident in a conference room that devastated a community in San Bernardino or improvised explosive devices (IEDs) at the Boston Marathon finish line that destroyed the lives of many of my fellow Bostonians. The terrorists who commit these heinous acts are radicalized here and abroad, but the theme and the intent is the same: chaos and the destruction of civilian populations, offering no quarter to women or children. We must stop it, and we must do so in an urgent and coordinated fashion.

Today, Commissioner Evans and Mayor Walsh admirably protect the city of Boston and do a great job in dealing with terrorism. But in 2014, I testified before this Committee on what worked and what did not work during the Boston Marathon bombing response. At that time, I recognized the deceased. Again today, I shall do the same: 8-year-old Martin Richard, Krystle Campbell, Lingzi Lu, and Massachusetts Institute of Technology (MIT) Police Officer Sean Collier. I also recognize every other victim in the United States, and those abroad, whose lives have been senselessly taken by terrorists. We can never forget them.

Progress has been made since we dealt with the Boston tragedy. We are seeing improvements in the quality of intelligence, coordination of agencies, sharing of information, training, and equipment. Game-changing technologies have been developed at a rapid rate, and first responders, including the medical community and fire departments, are receiving life-saving training and equipment, like the tourniquets issued to all Boston police officers after the incident.

Recent terrorist attacks in San Bernardino, Chattanooga, and Garland, Texas demand a coordinated, common-sense response.

Community policing plays a very important role in the prevention of these incidents. My former colleagues have long recognized the effectiveness of community policing and are laser focused on building community relationships, transparency, and accountability. This becomes most effective when reaching out to community members that are sometimes in the shadows, those that do not attend community meetings or religious services, and those activist groups that never sit down with law enforcement officials. We need to move beyond our comfort zone if we really want change and the

[1] The prepared statement of Mr. Davis appears in the Appendix on page 62.

important information needed to prevent these attacks. Community policing efforts need to be continuously and properly funded and trained up. They should also be audited.

Intelligence gathering and sharing is another critical prevention tool utilized by Federal, State, and local agencies to fight terrorism. Fusion centers across the country provide crucial information every day, in real time, to multiple agencies as well as forward redacted information to the private sector. Their value for prevention and crisis response management has been proven time and time again. Fusion centers should continue to meet annually to discuss issues, needs, concerns, and trends—what is working and what is not. Funding needs to be increased in order to attract talented analysts and grow properly managed and effective fusion centers that coordinate intelligence from all levels of government.

Since 2013, intelligence sharing among agencies continues to improve. Impediments have been removed. Federal, State, and local law enforcement need to continue working together as equal members of Joint Terrorism Task Forces across the country and in fusion centers, with unrestricted access to information that could identify terrorists in their early stages and prevent catastrophic events. However, separate systems are ripe for dysfunction. Any deterrent to this seamless coordination needs to be extinguished.

Intelligence gathering occurs in this country, domestically, every day. For 35 years, I have been a police officer working on drug cases and organized crime cases. We collect intelligence. We cannot be afraid to recognize that fact and to manage it properly with the proper Federal oversight. We need to look at what is happening, pay attention to it, and make sure, as Senator Tester said, that it is done constitutionally—but it does happen and it needs to be coordinated at the top level of government.

I am a member of and work closely with the Business Executives for National Security (BENS) organization. I have included their recommendations, which I think are very well thought out and on point, as to what can work to streamline our intelligence-gathering services here in the United States.

In addition to that, there are other things that worked really well during the Boston Marathon. Police officers respond the way that they are trained. DHS provided us money through the Urban Area Security Initiative (UASI) system to do that training, and we responded the way that we prepared. That made all of the difference in the world. And if you do not train, you do not respond properly.

Social media is extremely important in "establishing a dialogue with people. You cannot establish a relationship in a crisis. But social media allows police agencies, fire agencies, and other public service entities in a city to connect with people, to communicate with them, and to establish a dialogue.

And, finally, equipment is extremely important. The ability to be able to respond, as Commissioner Bratton said, with specialized equipment—not to be on display when it is not needed, but to be immediately available when the balloon goes up, as they say, is extremely important.

Finally, in closing, what I learned, in my role during the terrorist attack in Boston, is that there is no panacea. The reality is that

such a challenge requires informed and trusting community members who are not afraid to speak out, coordinated intelligence gathering and sharing among all equal partners who strive to prevent attacks, highly trained and well-equipped law enforcement, fire, and EMS departments that respond in unison, and, finally, all of you to continue to legislatively and financially support these important efforts.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Mr. Davis.

Our final witness is Mr. Mark Ghilarducci. I think that I got that right. Mr. Ghilarducci serves as the director of the California Governor's Office of Emergency Services and previously served as the Secretary of the California Emergency Management Agency. He also serves as the Governor's homeland security advisor (HSA), where he oversees Statewide public safety, emergency management, emergency communications, counterterrorism efforts, and the State Threat Assessment System (STAS). Mr. Ghilarducci.

Senator CARPER. First thing, would you just pronounce your name for us?

Mr. GHILARDUCCI. Ghilarducci.

Senator CARPER. Thank you.

Chairman JOHNSON. I was pretty close.

Senator CARPER. That was great.

Mr. GHILARDUCCI. Pretty close, yes.

Senator CARPER. I am sure that we have butchered it in worse ways than that.

Mr. GHILARDUCCI. No. Very good. Thanks.

TESTIMONY OF MARK S. GHILARDUCCI,[1] DIRECTOR, CALIFORNIA OFFICE OF EMERGENCY SERVICES, AND THE GOVERNOR'S HOMELAND SECURITY ADVISOR, MATHER, CALIFORNIA

Mr. GHILARDUCCI. Well, good morning everyone, and, particularly, Chairman Johnson, Ranking Member Carper, and ladies and gentlemen of the Committee. Thank you so much for the invitation to address you on this important topic. It is really an honor to represent California and the National Governors Association (NGA) today to and to discuss the work that we are engaged in from both a homeland security and an emergency management perspective.

As California's director of the Governor's Office of Emergency Services and homeland security advisor to Governor Brown, my portfolio and responsibilities straddle both homeland security and emergency management. As a result, I bring a unique and nuanced perspective to bear today as my "aperture," so to speak, for viewing and working on many diverse and complex disasters and emergencies—whether man-made or the result of natural circumstances—is wide open.

The State's and the Governor's homeland security advisor plays a critical role in ensuring that objectives, priorities, and collaborative operational actions remain coordinated within States and with local governments. The chief executive of a State is ultimately responsibile for public safety and must be kept informed and en-

[1] The prepared statement of Mr. Ghilarducci appears in the Appendix on page 98.

gaged. The homeland security advisor, who is the Governor's point person on statewide security, must be a focal point for Federal-State-local coordination and collaboration to ensure a coordinated and proactive posture in support of local government and the State infrastructure. Anything other than this undermines the larger unity of effort and the common operating platform necessary to detect, deter, prevent, protect, respond to, and recover from a potential act of terrorism.

As seen with the San Bernardino case, we continue to experience challenges in obtaining pieces of intelligence, in our ability to connect the dots, and in the lead-up to a possible act of terrorism. There were a number of signs associated with the suspects' actions and the related engagement with co-conspirators that we, as an enterprise, were unable to acquire.

Some of this is due to the use of encryption technology by the bad guys. Some is due to legal provisions in place for gaining access to or initiating the tracking of suspected homegrown violent extremists (HVE). But some aspects of this challenge can be still attributed to gaps in information sharing and communication across all levels.

In recent years, homegrown violent extremism and cybersecurity threats have evolved in fundamental ways and, in many ways, we are still reactive rather than proactive in terms of countering these evolving threats. This needs to change. Built into our homeland security enterprise must be nimbleness and proactiveness, so that we can get out and remain out in front of these threats. This needs to have its foundation in empowerment at the local and State levels, and it should start with information sharing.

Currently, there exist many organizations engaged in this intelligence arena, including the FBI, Department of Homeland Security, the Department of State (DOS), State law enforcement, local law enforcement, the fusion centers, and the international intelligence community.

There remain information and intelligence stovepipes and organizational protocols protecting designated proprietary information that needs to be shared. Plots and terrorist actions are carried out in communities at the local level and within States. The impacts of such events, of course, are felt nationally and internationally. This effort must be approached as one team, fighting one fight, so that we can, together, remain coordinated and lean forward as legally as possible, leveraging all levels of government capabilities so that we can all be on the same page in the effort to detect, deter, and protect lives and property.

Currently, we as a Nation—local, State, and Federal—are not optimally suited, in my humble opinion, to proactively prevent evolving HVE-style threats. DHS remains a good partner, but needs continual evaluation in order to be consistent with current threat streams. Its coordination and communications could be improved. Funding, training, and information sharing can be inconsistent and there needs to be more robust coordination with the homeland security advisors, Governors, and State top-level homeland security officials when engaging with locals and/or private entities within States.

With respect to fusion centers, there are 6 centers in California, with some 72 across the country, and they are all essentially front-line components to our Nation's homeland security. Over the last several years, we have been forced to evolve into all-hazard, all-crime centers in order to justify existence. This has spread these centers thin at times, with regard to their mission focus, and forced them to become distracted at times from their core mission of counterterrorism.

In California, our fusion centers are closely coordinated by our STAS and oversight is provided by the homeland security advisor. These centers, facilitated by local governance boards, have incredibly strong public-private partnerships that are leveraged to facilitate intelligence and information sharing as well as to prepare for and respond to emergencies. This is all coordinated at the regional and State levels. Building on these best practices and looking at what works in a State the size of California is important.

What worked best in San Bernardino was this exact system. The response was very well executed in the overall context, where the local authority led the immediate response and was supported in a unified command through mutual aid coordinated by the region and the State. This included personnel, specialized equipment, intelligence and information, situational awareness, authorities and clearances of regulations, victim services, and recovery assistance.

Outside of the FBI, which is the lead Federal agency supported by components of DHS, there were a few other Federal agencies that provided direct services, incident funding, or mutual aid assistance in a coordinated way, as did California's mutual aid and standardized emergency management system. This should be highlighted as a best practice and used as a performance metric in modeling a strong unity of effort. The team in San Bernardino was a unified team of local, State, and Federal agencies working together with wrap-around and integrated incident objectives. The incident required the combined efforts of multiple organizations beyond law enforcement, to include fire and EMS, public health, emergency management, telecommunications, and faith-based non-governmental organizations, just to name a few.

I am proud to say that the relationship between local, State, and Federal agencies in California is very strong, and this was evidenced by the actions of city, county, State, and Federal responders who came together in San Bernardino with the common objectives of saving lives, protecting further loss of life, and neutralizing a moving threat. This very dynamic and dangerous situation demanded close coordination and communications, and its success can be attributed to excellent relationships, good training, appropriate equipment and supplies, and robust coordination at all levels.

Nevertheless, San Bernardino did present lessons to be learned, with gaps and challenges, particularly, with information and intelligence sharing at all levels still being a challenge and not at the level or quality that needs to be in place to fully safeguard this country.

As an HSA, I require timely and regular intelligence updates during an event of San Bernardino's magnitude to keep the Governor informed, to engage with my local and Federal counterparts,

and to coordinate the statewide homeland security and mutual aid mission that I spoke of previously.

When an event like San Bernardino occurs, we must be careful not to revert back to not wanting to share "proprietary" information. The FBI in the San Bernardino case received strong support from the Joint Regional Intelligence Center (JRIC), located in Norwalk, California. But along the way, it became a one-way information-sharing relationship between the FBI and that fusion center. This impacted the fusion center's communications responsibilities to the State. This presented challenges and resulted in gaps in relevant information getting to senior leaders and decisionmakers, who needed to be kept informed, particularly, when the news was reporting the "proprietary" information through open-source media. This required the development of a time consuming work-around to obtain necessary information at a number of critical junctions at the information-sharing stage.

This must be one team, fighting one fight. With all of the money and infrastructure established since 9/11 to safeguard this country, we need to move past "proprietary" if we are truly going to function in a manner that allows us to protect the American people and maximize our total unity of effort.

In closing, let me reinforce that it is critical that we, as an enterprise, understand that the threat landscape continues to shift toward a more diffuse, amorphous threat that focuses on homegrown radicalization and lone-wolf actors, who are inspired by foreign terrorist organization's propaganda and extreme ideologies, and are leveraged to act in any way possible in all of our communities—large and small. This is a new norm, just as deadly and much harder to counter. We must remain vigilant, but also nimble and proactive enough to address this evolving threat.

Enhanced training, adequate funding, the maintenance of equipment and resources, and that collective unity of effort are all absolutely necessary in order to meet these requirements.

Thank you for the opportunity to testify. I would be happy to answer your questions.

Chairman JOHNSON. Thank you, Mr. Ghilarducci.

I really appreciate the attendance of my colleagues here. There are two choices: either limit the questions to 5 minutes or limit them to 7 minutes, but I am going to use the gavel. So we will keep it at 7, but I do not want answers going beyond 7 either. So let us discipline ourselves to be respectful of everybody's time.

Chief Sparks, I want to start with you. I get a feeling Senator Portman is going to be talking about information coming down the chain. I really want to talk about the grant programs that actually work, the coordination—we have heard that term a number of times—with other departments, both big and small. Can you just speak to which grant programs are essential, which ones work, and hopefully which ones could be improved upon?

Chief SPARKS. Well, the problem is, especially for smaller agencies, it is really difficult to get some of those grant funds down to the local level so that we can utilize them for some of the training and equipment that we need. We particularly like the Community Oriented Policing Services (COPS) grant. We applied for a COPS grant, and typically what we saw was that, in Wisconsin, they

went to the large cities. They went to Milwaukee and Madison, and very little filtered down to the local level.

But, as you heard from some of the other people on the panel, it is critical—that training is critical. Like Mr. Bratton said, in New York they have special teams that are specifically trained with the equipment that they need. But, in rural communities and in smaller departments, that response is going to be from frontline patrol officers. So, whatever equipment they have in their squads is going to be used to respond. And, in smaller communities, you may have only one or two officers, so you are going to have people coming from multiple departments trying to go in there. So, we need to be able to have grants that can be designed, not only for the smaller communities, but presented in a fashion that encourages the communities to work together and to train together.

In the county that I work in, we have nine law enforcement agencies, excluding State and Federal. And only three of those have probably the frontline training that they need to respond to active shooters and provide emergency medical treatment through Tactical Emergency Medical Specialists (TEMS) and provided equipment—and each of our officers carry that equipment.

The other six agencies really have no level of training, and if we have an incident, we are going to be working with them. So it is important that you can funnel funds through your grant programs that are designed to—maybe on the "train-the-trainer" programs through the local municipalities, start funneling grant funds through a technical college system, where you can put them out regionally through the State and encourage—or maybe even tie into that funding—the idea that, at the county level, you will train the trainers, but the caveat is that you have to reach out to the other municipalities that provide that training.

Chairman JOHNSON. So, it takes just a lot of time and resources to write a grant, correct?

Chief SPARKS. Exactly.

Chairman JOHNSON. So, I think that potentially one of the solutions, from an overall Federal standpoint, is determining how we can help the smaller communities, so that you can spend the time training rather than grant writing. And I think that we are all mindful of that. Let us face it. The thwarted plot was in Milwaukee, but no community is safe. So I think that we really need to be mindful of that.

Commissioner Davis, you talked about the need for intelligence-gathering capability explained and how we are gathering it, but then we always hear about stovepipes. Can you speak to the problems that we are still running into and what needs to be done to continue to lower those stovepipes, so that we actually do have what I consider to be the first line of defense against these terrorist acts, an effective intelligence-gathering capability, while being mindful of our civil liberties?

Mr. DAVIS. Certainly, Senator. So, in being mindful of civil liberties and in understanding that intelligence gathering does occur, coordination of the various agencies is really important. And one of the problems that I see is that, if you pick one agency to be in charge of it all, then the same kind of problem occurs with some focus on that particular agency.

If this goes up to the level of the Director of National Intelligence (DNI) Office, then the control is happening—or the oversight, the auditing, and the sort of direction of best practices is occurring at the highest levels of government, and it is not vested in the one agency or the two agencies that are picked out among equal players. And I really think that that is important. Anytime that you have silos, you have the possibility of missing something. And it has happened over and over again, and based upon my colleague's testimony in the San Bernardino case, it seems to have happened again there. And I think that it will continue to happen until there is a coach, somebody that is in charge of the whole thing that says that you have to play together properly. It is like a sports team.

Chairman JOHNSON. Talking about playing together, kind of going back to Chief Sparks' problem in a smaller community, again, being mindful of the fact that in New York or in Boston—maybe talk to Mr. Ghilarducci here—how do we get those funds allocated in an efficient way? How do we provide the training, so that, not only are we covered in the large cities—where, let us face it, those are very severe threats. But how do we get the training, the dollars, and the grant money down to the smaller communities in an efficient manner? I will start with you, Commissioner Bratton. And do you feel some kind of responsibility to help that process? Because, obviously, I know that you are fighting for the funds, but what can we do to help?

Commissioner BRATTON. I am coming at it from a different perspective than some of my colleagues, having been in charge of Los Angeles (L.A.) and New York, the two largest cities in the country. The issue of how to get it down to the smaller agencies is not one that I have had to grapple with, but how to get funds is certainly one that we have grappled with. Early on in the DHS process, as it was being created, the issue of control was centered at State government levels, where the money would come down through the State and the State would take a certain percentage as their fee, if you will. We have had great problems with that, both in L.A., and, in some respects, even now in New York.

So I do not have a solution for you on that issue, other than to reinforce the importance of those grants—and in no city have they been more important than in New York, where we have received, since 9/11, about $1.4 billion from the Federal Government through various grants, all of which have been part of the wide range of activities that we engage in in New York. This is similarly the case in Los Angeles, which received hundreds of millions of dollars during this time.

One of the great strengths of democracy, is the way that we operate in this country, with all of these thousands of communities—18,000 police departments—but it is also one of our greatest weaknesses: trying to get them coordinated and trying to get them collaborative. And that still remains a very significant weakness. How do we get all of these silos, at some point in time, to come together?

Chairman JOHNSON. I will be respectful of my time as well. That will probably be a question for the record—any suggestions on what we can do, Mr. Ghilarducci, in terms of California. Again, I do not want to take more time because I am out it, but I would really like to see your recommendations for how we can effectively

and efficiently allocate those resources, even to the smaller communities as well.

Senator Carper.

Senator CARPER. Thank you. Thank you very much, everyone.

Chief Kerr, just give us one really good example of how the Federal Government can better support fire and emergency service providers. Just give us one good example.

Chief KERR. I think that the way that we can help support our first responders and the fire and emergency medical service is through continued grant funding and the sharing—and this is the key, critical thing that we have heard here today—of intelligence and information. The fire service does not have State or Federal backup or reinforcements. The local fire service is it when it comes to responding to terrorist events.

So it is really important that every entity, whether they are in a small, local community or in a large, major urban city, has access to the intelligence and the information, so that they know what they are going into.

So I think that it is really important that we can somehow fund or prepare people to be part of the Joint Terrorism Task Force offices. I am very fortunate in Austin. I have a firefighter in the Austin Regional Intelligence Center. I have a firefighter that sits on—or is part of—the FBI Joint Terrorism Task Force. And I have another firefighter that is destined to the National Counterterrorism Center in that regard as well. But that is not the case for firefighters around the country, and that is something that we definitely have to improve.

Senator CARPER. Great. Thank you so much.

Commissioner Bratton, I think that you may have mentioned in your testimony—did you hold up a smartphone? I think that you indicated that these smartphones were being provided for, I think that you said, 36,000 police officers. Here is my question, and I will make you a guided missile. Here we go. I remember when we wired every public school classroom in Delaware with access to the Internet. We provided a lot of computers in the school classrooms and I went, as Governor, to visit the schools to see how the teachers were using them—and they were using all of the technology for their emails. And I said, "I do not think that is what we had in mind." And we had to train them. We had to train them. It was a combination of using our technical community college to train them and, frankly, using younger teachers to teach the older teachers how to use the technology.

What advice would you have for other police departments—or fire departments, for that matter—across the country that are using this kind of technology, buying the phones and all of these apps, to make sure that they actually get their money's worth?

Commissioner BRATTON. It is a new field, in the sense of how police agencies—and I will speak to my agency—are using these devices. I think that I would be correct if I were to indicate that what we are doing in New York is probably unparalleled anywhere else in the country at the moment. We have been fortunate, through Federal grant funds as well as asset-forfeiture funds, to have been given hundreds of millions of dollars so that we have been able to develop technology that we will be seeking to share with my col-

leagues across law enforcement and the fire services—lessons learned, as you will, as we move forward with this technology.

But it is essential that we get this technology into the hands of our police officers, so that if I am looking for a terrorist on a terrorist alert, I can send out his information, his photo, to 36,000 officers instantly. If I am looking for a lost child with autism, I can send out that photo. My officers instantly, through their various apps, can access just about everything that we have, in the way of intelligence, on an issue.

So it is 21st Century technology that has come, fortunately very early in the 21st Century, and it is going to be essential going forward.

Senator CARPER. All right. Thank you. My question was about the training. We are not going to pursue this any——

Commissioner BRATTON. Training is absolutely essential in the job, but where we are with the training is that we are learning every day. The creativity of our officers and how they use these devices, we are keeping a running journal on how they are using the devices to creatively use the information, solve crime, and connect with the community. The connection with the community is one of the principal benefits. So the training that we give initially is, we are training them——

Senator CARPER. That is good.

Commissioner BRATTON. We are learning from them also.

Senator CARPER. That is good. You mentioned connections to the community—and I only have a limited amount of time, so I apologize for interrupting you. Secretary Johnson just hosted for breakfast the leadership of the homeland security authorizers in the House and the Senate, as well as the appropriators. One of the things that we talked a bit about was the Department's interest—they are very much interested—in our passing legislation that authorizes something called "Community Partnerships and Countering Violent Extremism (CVE)." And the idea there is to go to the root causes. And it is all well and good that we degrade and destroy ISIS—I think that that is critically important. It is important that we do a very good job of vetting the people that are trying to come here, either as refugees, through the Visa Waiver Program (VWP), or through any other kind of program. But it is also important that we figure out how to reach out into the community. It could be to faith-based groups, it could be to nonprofit organizations, or it could be to others. And what the Department is trying to do—and we have given them some money to create the entity, have the leadership, and get the grants—to have $50 million for grants.

Would you just respond to this approach? Is this a valuable approach for us to pursue. Mark, do you want to go first? That way I do not have to say your last name. Ghilarducci?

Mr. GHILARDUCCI. You guys will get it.

Senator CARPER. It is coming to me. Go ahead. Just be very brief.

Mr. GHILARDUCCI. Yes. Let me just say that there is nothing linear about any of these homeland security and counterterrorism efforts. It has to be a whole-of-community approach. If we are really going to counter this, it has to involve all of these entities—nongovernmental all the way down to school kids.

This dynamic is changing our country and we need to be informing and empowering people to, not only recognize what is happening, but to be a part of the solution.

Now, that can be done while protecting civil liberties and our constitutional rights. But, much like we have seen in history in the past, there are certain things—certain threats—whether they are natural or man-made, where we want to empower folks to be able to make themselves a part of the solution.

So this effort that the Secretary is talking about is a good one because it does actually begin that process of countering and——

Senator CARPER. I am going to ask you to hold it right there. Thank you very much.

Raise your hand if you think that what the Department of Homeland Security is pursuing is a smart idea.

Let the record show that four to one say that it is a smart idea. Commissioner Bratton, we will talk with you about it later. Thank you.

Chairman JOHNSON. Senator Baldwin.

Senator BALDWIN. Thank you. I appreciate all of your testimony. I want to start where the conversation is right now. We are talking about communication. We have been talking about communication at the local, State, and national level, talking about communication among peer agencies—and how we can do a better job if we have a "coach" rather than silos, and talking about public and private conversations as well as conversations within governmental agencies.

Chief Kerr, you talked a little bit about interoperability in your testimony, especially regarding real-time response to an emergency—whether that emergency is man-made or naturally occurring. I want to just use a quick example. Mr. Chairman, I have some testimony from Chief Gregg A. Cleveland, the fire chief from La Crosse, which I would like to ask unanimous consent to enter into the record.[1]

Chairman JOHNSON. Without objection.

Senator BALDWIN. Great.

The reason that I raise this relates back to some of the concerns that I expressed about the movement of hazardous materials—obviously subject to an accident if it is by train or even if it is by truck, but also subject to nefarious terrorist activity.

In La Crosse, Wisconsin, where Chief Cleveland works, they have invested huge amounts of money into upgrading their communications equipment to respond to a real-time emergency. La Crosse is on the Mississippi River. La Crosse has a rail line running through it along the Mississippi. On the other side—the Minnesota side—there is also a rail. Both transport hazardous materials on a daily basis. Their upgraded communication system could not operate with the Minnesota side—even though they had just invested a very significant amount of local resources with that upgrade.

What is your sense of the status right now, in terms of interoperability? And I would certainly be interested in all of you—hearing your perspective briefly on where we are right now with those investments as well as how you would be able to communicate in real

[1] The statement from Chief Cleveland appears in the Appendix on page 110.

time during an emergency—natural or man-made—with the agencies that you need to coordinate with. Let us start with you, Chief Kerr.

Chief KERR. Thank you, Senator Baldwin. The FirstNet, which I mentioned, is the federally designated network and it is an independent entity within the U.S. Department of Commerce. They are the ones that have been charged with completing and working out the 20 megahertz band that was designated for interoperability.

The first part of that is going to be for sharing data only and then the voice transmission will come second. So the land-to-mobile radio system, which Chief Cleveland was talking about, has its limitations when it is built out only to communicate within its own entity. That is a critical part of being able to communicate and share information "across the river", so to speak, which you are not able to do.

The answer eventually will be FirstNet, but it is not going to come in the next year or two.

Senator BALDWIN. Let us go down the panel. Chief Sparks, can you talk about your reality on the ground in Everest?

Chief SPARKS. Actually, countywide in a scenario, we do have interoperability. So, police, fire, and EMS, we are going to be coordinated, as far as our communication goes.

Commissioner BRATTON. Where we are is certainly not where we need to be. We are making progress all of the time. Recently, Congress—yourselves—voted to increase the spectrum available to us—dedicated spectrum—which is critical to interoperability. But every community is still wrestling with it. In my city, by the end of this year, finally, my subway cops—the cops who work below ground and then the others who work above ground—will be able to use radios below or above ground without having to go through a whole series of connections to try and talk with each other. And, similarly, we are continually improving our relationship communications with our fire colleagues.

But we still have a long way to go in this country. It is going to cost a great deal of money to do it. It can be done, but the devil is in the details—and the devil is in the budget.

Senator BALDWIN. Is that your most significant gap, the one you pointed out with the subway police?

Commissioner BRATTON. It is a significant concern, certainly in an active-shooter issue and in a disaster issue. The interoperability capabilities that we have seen time and again in every one of these instances is the inability to communicate in real time.

Senator BALDWIN. Mr. Davis.

Mr. DAVIS. We have cobbled together a system of interoperability in Boston that works effectively. It is not pretty, but it gets the job done. But that interoperability is based upon the T-band that the chief mentioned earlier. And the FirstNet legislation removes that T-band from us at a particular point in time. And with the slow progress of FirstNet, we need to address that issue because if we lose the T-band, then we lose our interoperability in Boston.

Senator BALDWIN. Mr. Ghilarducci.

Mr. GHILARDUCCI. I would just say that there is no silver bullet with interoperable communications. And I think that initially after 9/11, when we were talking about interoperable communications,

there was the thought that you could lay down an overarching system nationwide—and I think that this is the concept behind FirstNet, which we have been engaged with.

But in the absence of that—and leading up to that—we have dealt with a lot of regional interoperable capabilities. California, specifically, has a very robust mutual-aid system. We move resources up and down the State for disasters all of the time, and so that precipitates the need to have multiple agencies talking to each other in different jurisdictions. A lot of that is done via mobile interoperable communications capabilities, which have to be put in place. It is backed up through a redundant system to the Statewide Microwave Network that can support that. And we have had some regional projects, like the L.A. Regional Interoperable Committee (LA–RICS) and the Bay Area Regional Interoperable Communications Systems Authority (BayRICS). There has been a lot of engagement by the private sector into that, which has complicated the matter a little bit. I am sure that you do know, in the Bay Area, that really was a large factor that actually caused that BayRICS project to end.

So I would say again, like the other panelists have said, we have further to go on the interoperability. But, there are pockets of development that have been put in place in California that have worked pretty well.

Senator BALDWIN. Thank you.

Chairman JOHNSON. Thank you, Senator Baldwin.

Again, I want everybody to be mindful of the clock and of wrapping things up so that we stay on time. Senator Heitkamp.

Senator HEITKAMP. Thank you, Mr. Chairman.

I want to discuss making sure that we are all taking a "one team, one fight" approach and sharing information, because if there is one thing that I hear over and over again when talking with my first responders, it is that, once an incident happens, we are all in it—and then, there is that immediate response of collaboration and cooperation—but that starts eroding, in terms of what we know, what we can find out, who is talking to who, and where we can go from here. And I think, Director, you spent a lot of time in your written testimony on this issue. We had certainly hoped that after 9/11, when we talked about these communication gaps, we would be further along in making sure that there was a fair amount of Federal to State and local respect for the need for data, for information, and for intel.

You raised a lot of these concerns in your testimony. You did not offer us a whole lot in the way of solutions—other than a "let us do better" kind of systemic structure that we could be looking at which could be helpful as we deal with your Federal partners. So could you offer some concrete examples of how we could do better in terms of information sharing?

Mr. GHILARDUCCI. Well, let me just start out by saying that the overarching information sharing structure and our collaborative efforts have improved exponentially since 9/11, to use that as a baseline. That does not mean that we do not need to do more, and as we have these events that occur, like Boston, San Bernardino, or Chattanooga, we learn little bits each time about what has worked and what still needs to be improved.

I think that generally there is a sense in the organizational cultures that exist to want to keep information sort of inside their organization. This is not just at the Federal level. It is also at the local level and at the State level. And so, we need to build into our training programs right from the beginning—in our academies and in any of the training programs that we are doing on terrorism—curriculum expressing the importance of sharing information. Really one of the cornerstones of being able to counter terrorism is sharing critical information amongst all of the players. It does not matter that I am wearing a State patch and he is wearing a Federal patch and she is wearing a local patch. When it comes to this—that is the concept of "one team, one fight"—and we should be able—we all have clearances. We should be able to all get that information appropriately.

Senator HEITKAMP. I understand what you are saying, Director, but what you are talking about is changing the culture—not systemic changes. And I am interested in any other comments from any of the other panelists in terms of how we institutionalize cultural changes, not just say, "Let us do better, let us work together better". So maybe, Mr. Bratton, you can help me here.

Commissioner BRATTON. I think that at this particular time, I could point to my city as a model of what you are trying to get to. For many years in New York, the collaboration was not all that it could have been. We were dealing with a combination of personalities, skill sets, and intelligence handlers not trained to the same level. The BENS Report that both Commissioner Davis and I would recommend to the Committee speaks to a lot of these issues: the importance of leadership, the importance of the collaboration of that leadership, which pushes down into the organization, but also the creation of systems that ensure the sustainability that you are talking about, and also the training of personnel. A major gap in our situation is our intelligence handlers. Many of them come into the organization and within a couple of years they leave because there is no upward mobility—and the quality of training is not consistent across the agencies.

Senator HEITKAMP. One of our roles here is to hold Federal agencies accountable, is to have that oversight—that kind of accountability. In order to do that, we need something more concrete than "You need to change your culture" or "You need to be more communicative." We need to have benchmarks or measurements that can, in fact, be enforced and will, in fact, build a better culture because there will be a known list of expectations.

I am curious about—and I will look at—the BENS Report and take a look at those secondary sources. But you are all here right now—and we have training needs and we have equipment needs—I recognize all of that. We are working hard to make sure that we are using everything as efficiently as we can. But I think that it is more elucidating to get to this problem of information sharing, which I think is critical for the protection of the citizens of this country. And so, where are the benchmarks so that we can say, "Look, this is what our expectation is. How are you communicating beyond the fusion centers? Are these fusion centers simply box-checking or are they actually doing what we expect them to do?"

Mr. Sparks, you and I come from the same small-town universe—actually, you are from a very large town in my universe. And it needs to filter down, not only to the major cities and not only to the major States, but we also need to have that trust level with States like North Dakota and Wisconsin. So what would you offer in terms of our ability to look at holding Federal agencies more accountable?

Chief SPARKS. Well, let me give you a classic example. I talked to one of the chiefs in our area. He retired just a couple of years ago as a Federal Supervisory Police Officer. He did not want me to state the specific organization. But he said that he was frustrated because he had a lot of information that would come to him—terrorist-related information—and he would have specific information, but he had local contacts who he was not allowed to share anything with.

Now, I understand the need for secrecy on an active investigation, but some of this was general information: "This person is going to your community. He is meeting up with this person." And he said that he was frustrated because he could not share that information with local law enforcement. And, as he moved up the chain of command and asked why, he said that it was because those local law enforcement officers did not have security clearances.

So, to touch on some of the other comments here, you have to be able to eliminate some of that. And, even if you cannot trust local law enforcement with information, we are shooting ourselves in the foot. We are not going to be able to prevent a lot of this stuff. You are missing 80 percent of law enforcement agencies across this country. You have to break down some of the policies that are inhibiting that.

Senator HEITKAMP. I think that there are a lot of us here who go into the secret, hidden room and hear things, only to walk out and see them on the front page of the New York Times. We share your pain in terms of overclassification and the overprotection of data. And that is something that we need to be talking about, because you cannot get the expertise of the men and women who are the eyes and ears—who are on the street every day and could say, "Oh, that is what they are talking about. We have seen that." In fact, doing so builds on that intelligence. We have to get through this issue.

And so, thank you, we look forward to any additional suggestions that you have going forward. My time is up.

Chairman JOHNSON. Thank you, Senator Heitkamp. That might be a good subject for a hearing, the overclassification of material, because I think that it is certainly within our Committee's jurisdiction on oversight, but it potentially even falls under legislative jurisdiction. Senator Booker.

OPENING STATEMENT OF SENATOR BOOKER

Senator BOOKER. First of all, I just want to thank the panel. Your leadership is extraordinary. Having been a mayor and having had to deal with the challenges of an urban police department, I am aware that every single day we have officers out there who are doing heroic things that never make the papers or never make the

news, but ultimately that are saving American lives and securing property. So I am grateful for your service and your commitment is just something that is worthy of respect.

I would like to first talk really quickly about the idea of dual usage. It has come up a few times. The reality is that we do all of this work to prepare for counterterrorism, but our first responders, when gunshots go off, they are responding to a situation.

Now, there have been at least 80 mass shootings, as defined by four fatalities or more, since the Columbine massacre of 1999. Nine of those mass shootings were at schools. Less than 10 of these incidents have been described as a product of homegrown extremism. And when I am talking about that, I am talking about mass shootings, not bomb threats or other plots.

Many capabilities which support terrorism preparedness simultaneously—obviously—support preparedness for these other hazards, which are becoming incredibly frequent in our Nation.

And so, what I would like to understand is, as we are funding a lot of these things—really two sides of this—one is: Can you discuss sort of the dual use, why this is helpful in that effort? But then also, Mr. Ghilarducci——

Mr. GHILARDUCCI. You guys are going to be perfect at pronouncing it when we are all done. [Laughter.]

Senator BOOKER. Thank you very much. "Booker" is a hard one, too, so I feel your pain. But you talked about how it might be straining some of these resources because there are multiple usages for them. So I would just like to understand—and perhaps starting with Commissioner Bratton, who I owe a lot of gratitude. We share a metropolitan region. The work that you and your department do benefits everybody in the New York City region. I like to think of it as the Newark region. But I want to thank you for your leadership. I would love to get your thoughts about this.

Commissioner BRATTON. Actually, you raise a great point, because one of the good things, if you will, about the issues of terrorism—and particularly the form of terrorism that we are most concerned with in this country at this time: the lone wolf—is in many respects—other than motivation—not different than what we are dealing with with the active shooters, with all of their various motivations. The response is very similar. We learned after Columbine that we have to get in there and get the shooter. We learned through the various terrorist acts committed around the world that we have to get in there and get the shooter. And we are constantly learning about how to deal with the shooter, while at the same time preparing to deal with the victims who are in the same location while we go in.

So the duality is a strength that we can build on because we can train our officers to deal with the current terrorist threat—and the most significant one currently is an ISIS-inspired or ISIS-directed assailant—and at the same time, in a country that has as many guns as we do, where mass killings have become a very commonplace circumstance and one that our officers—all 800,000—and our firefighters increasingly are drawn into, we can prepare them for all active shooters. So training for one is effectively training for the other.

Senator BOOKER. Yes, please, Chief.

Chief KERR. I would just like to comment on the dual threat and the dual use. I am proud to say that in Austin we have worked extensively with our law enforcement partners and have a developed, strategic operating plan that we use and have drilled and exercised on. And I think that the importance here—how you all can help—is first of all by providing those opportunities and, second, by providing the funding that will allow us to continue to hold those large-scale exercises and drills so that we are practicing what we need to do and sharing standard operating procedures. This way, we are skilled at getting into the "warm zone," applying those tourniquets, and pulling people out that are savable and then allowing law enforcement to protect us and go after the shooter. Let the fire service or the EMS service get in there, get the people out, and get them into the cool zone where they then can be transported for treatment.

Senator BOOKER. Great. Would somebody else like to comment?

Mr. DAVIS. Thank you, Senator. The issue of dual use is extremely important in the city of Boston. We leverage the funding that we have been using for the fusion center to work on crime analysis across the board. The intelligence streams are all the same. We are looking at different crimes that are occurring and deriving an incredible benefit, reducing common crime and violent crime in the city by centralizing those functions into one group. They are specially trained. They become very good at the numbers—at predicting where crime is going to occur—so that our deployments are much more effective. It works very well for us in Boston.

Senator BOOKER. Thank you. Mr. "G"?

Mr. GHILARDUCCI. Actually, I think that what you saw in San Bernardino was the execution of how dual-use training and policies and procedures came together. Those officers, those firefighters, and the Special Weapons and Tactics (SWAT) medic program were all trained. In fact, at the time of the San Bernardino shooting—that exact time—we had a multiagency active shooter training going on. I do not know if you knew this or not, but, in fact, many of the people in the class thought that the actual event at the health center was part of the exercise—until they realized that it was not.

One of the things that I have been able to do in my role as HSA is drive funding—and put requirements on that funding—so that fire service, law enforcement, and EMS, which are going to develop a training program in these kinds of things, have to come together around the table and development common sense operational constructs and build that into everything across the board, from school safety to hospital safety. And that really has been a benefit to all of——

Senator BOOKER. Thank you, Mr. Ghilarducci.

A last question in 30 seconds, Commissioner. So you have heard a lot here. If you were a U.S. Senator—we are having issues with interoperability, with critical investments being made so that we can do the training. There have been some concerns about funding programs. You are obviously a big-city leader, but you see States like mine that have lots of small towns—not necessarily the experience that you have—working together. Could you give like three

things that you would do and that you would focus on if you were a U.S. Senator?

Commissioner BRATTON. Funding is absolutely critical. The development of standards, as the Senator spoke to, is also critical. And, third, in this day and age, the issue of communications is absolutely critical across the line, up and down—and that also requires funding. So I would suggest your role in the U.S. Senate—as well as your colleagues' role in the House—is to ensure that funding is available for hometown security, because hometown security is what homeland security is all about.

Senator BOOKER. Thank you.

Chairman JOHNSON. Senator Ayotte.

OPENING STATEMENT OF SENATOR AYOTTE

Senator AYOTTE. Thank you, Chairman. I want to thank all of you for being here today.

Commissioner Davis, I wanted to follow up regarding the Boston bombing terrorist attack—I really appreciate your leadership on that.

Mr. DAVIS. Thank you, Senator.

Senator AYOTTE. You came before this Committee, and you and I talked about issues with the JTTF. I raised these issues with Director Comey of the FBI, and as I look at the background we received on this hearing today and what happened in Garland, Texas—in that situation you also had the FBI tracking one of the individuals involved. The FBI sent a memo to the Garland police and to the North Texas JTTF hours before the attack, but that information never got to the actual patrol officers who were there. As we talked about what happened post-Boston and the things that needed to be communicated at the local level—something that Chief Sparks raised as well—the question is: is how do we stop that? The reality is that it is a patrol officer who is likely to come upon one of these situations. The FBI is not out roaming the streets in the way that the patrol officers are. Where are we now with the JTTFs in terms of disseminating that critical information to the officers? And have we improved that? How do we get at this fundamental issue?

I was very interested that you brought up the concept of a "coach". Who should that "coach" be? Because you talked about DNI. Right now, as I look at this system, it seems like the FBI is the "coach", but we still have instances where—whether it is a security issue or , whether it is a need-to-know issue—the information is not getting to the front lines. We would love to get your impression, Commissioner Davis, on that. And we would love to get your impression as well, Commissioner Bratton, Chief, and anyone else who wants to jump in.

Mr. DAVIS. Thank you, Senator. I appreciate that, and I had a great team in Boston. It was a real team effort there.

Prior to the Boston incident, we had two special agents in charge in Boston, Warren Bamford and Rick DesLauriers. Both of those men were incredible partners and opened up the place to us. We worked very closely with them. Director Comey and I have spoken since I stepped down. I believe that the FBI wants to do the right thing.

However, there are silos and bureaucracies involved, and when that happens, things start to break down. And despite the best intentions of everyone involved, it really is important that someone is auditing the functions. Every year, the FBI comes into the Boston Police Department and audits our motor vehicle checks to make sure that they are all legitimate. But who is auditing for larger issues? Who is looking at the transfer of information——

Senator AYOTTE. Is anyone doing that right now within the Federal Government?

Mr. DAVIS. No, absolutely not. And so, that really needs to happen. And I mentioned the DNI. I just think that if all partners are equal, then the "coach" cannot be one of the partners. I think that it needs to be somebody——

Senator AYOTTE. Agreed. It has to be someone who is not directly in the line of command—that is what you are saying.

Mr. DAVIS. Right, because then you have the same problem of being protective of your information and it goes back to the old issue of police wanting to make the busts themselves. Everybody wants their own information, because if you give it to somebody else, then you might lose the arrest.

But the other issue that you brought up, the technology side of things, is extremely important, Senator. Going back to the NYPD, when those two officers were killed, Baltimore had information that was faxed—pictures were faxed from the Baltimore police to the NYPD. The state of communication among police agencies is really reprehensible in this day and age and the use of these devices that Commissioner Bratton has shown will help with that. But it needs to be a nationwide initiative. It cannot just be department by department, because when you set up individual protocols, you have other communication problems.

So there are two levels that you talked about which are extremely important, Senator.

Senator AYOTTE. Commissioner Bratton, I wanted to get your impression.

Commissioner BRATTON. Prior to your arrival, I had displayed a smartphone device that the department has customized and will, by March, be in the hands of every one of the 36,000 New York City police officers. It is a model and a device that can be shared with American law enforcement—and it was developed very specifically after the murder of our two officers—because the messaging—the traditional messaging—the length of time that it took to get information out to the field was too long. And in any event, even as the information arrived in New York, it would have been too late to save the lives of those two officers.

With this instant messaging now, I can instantly send out an alert to 36,000 officers. I can override everything else that they are doing and indicate that this is a terrorist alert or that there is a "threat on your life" alert, and the capability can effectively be expanded nationwide with the coordination and collaboration of capabilities. So we are moving in this direction thanks to technology.

On the issues of collaboration and leadership, we are very fortunate with the leadership of Director Comey, who Commissioner Davis and I have had extensive involvement with. He is going to be around for about 8 years, and that is essential, because in our

world, people come and go very quickly. He is committed to this. He is trusted by us. He is committed to the idea of information sharing, and the relationship that we have in New York City with our FBI is a direct result of his leadership, indicating that the FBI will get along with the NYPD. And the commitment on my end is that the NYPD will get along with the FBI. And this is essential.

So the benefit that we have at this time is that the technology is becoming available—and I think that I would argue that the leadership's support of collaborative relationships is also available and will be around for a while.

Senator AYOTTE. Thank you. And, I think that as you think about resources, this would be worthy of a national investment.

Commissioner BRATTON. I think so.

Senator AYOTTE If you think about both the terrorism and law enforcement contexts, this would be a huge protection measure for the country.

I wanted to follow up. You mentioned forfeiture briefly, Commissioner Bratton. Recently, in the end-of-the-year budget deal, one of the things that was grabbed was over $1 billion in forfeiture money.

Commissioner BRATTON. Which is a major mistake and something that we resent tremendously.

Senator AYOTTE. Yes, so that is why I am asking you about it. As I look at what my police officers are doing and what my law enforcement in New Hampshire is doing with the forfeiture money, it is obvious that we did some really important things—increasing funding for first responders and funding to combat the heroin epidemic facing my State. On the other hand, I think that people around here are not understanding the value of forfeiture resources and the consequences of taking the forfeiture resources that help address the problems for our first responders.

So I just wanted to put that on the record and make sure that people understand here. We have to turn this around. We should not do this again. These resources are critical to first responders.

Commissioner BRATTON. These smartphone devices could not have been bought without $160 million of forfeiture money from my local district attorney's asset forfeiture fund. It did not come from the Federal Government, fortunately, because it is no longer there.

Chairman JOHNSON. Thank you, Senator Ayotte.

Two points. I do not think that anybody has asked to have the BENS Report entered into the record.[1] I will do so, without objection.

I actually circled your comment about auditing, and I would really like to work with you, Commissioner Davis, to develop a way to audit so that it is a positive thing as opposed to being viewed negatively. But I would encourage any colleague to work with me on that. I turned around to my staff and said that that is a piece of legislation that we should work on as a result of this hearing. Senator McCaskill.

[1] The BENS Report referenced by Senator Johnson appears in the Appendix on page 64.

OPENING STATEMENT OF SENATOR MCCASKILL

Senator MCCASKILL. Thank you. It is an honor to be here in front of all of you. I am still in uniform withdrawal from my days as a prosecutor. So it is terrific to be with all of you, and one of my specializations, Ms. Kerr, was arson prosecution. So I spent a lot of time with fire chiefs also.

A few months ago, I introduced a bill—and I want to emphasize this—that would not end any Federal programs for local law enforcement and would not cut any funding for local law enforcement. One of the things that Mr. Davis touched on in his testimony which is profoundly important is that a discussion over whether law enforcement is too militarized or does not have enough resources is really irrelevant if you do not have the trust of your community. I do not need to lecture you guys on how important it is, in terms of the rule of law in this country, that people have trust that law enforcement is, in fact, going to be fair, trained, and competent.

So, one of the things that we did in carefully drafting this bill was to make sure that we did not cut it—we did not eliminate programs—but we talked a lot to the National Tactical Officers National Association (NTOA) and worked with them on the language of the bill. Then, basically, the bill requires States to establish certain minimum training requirements for any officer with decision-making authority on the deployment of SWAT—necessitating that SWAT members attend some kind of training.

I believe that most States are already in compliance with this. Most States do require some kind of SWAT training. But I would ask you all to comment on whether you think—in light of the $1 billion in Federal resources that are going to State and local law enforcement—that requiring some kind of minimal training, through language that was helped to be drafted by the National Tactical Officers Association, is a reasonable thing for the Federal Government to do. Mr. Bratton?

Commissioner BRATTON. I can speak to that and speak strongly in support of it. Training is absolutely essential for SWAT entities or for any police officer function. And the trust that you are talking about, let us face it, we have a crisis of confidence in the American criminal justice system at the moment. It is not just police any longer. That has been the focus for most of the last 30 years. It now goes to grand juries, it now goes to prosecutors, and it now goes to judges. Every element of the criminal justice system is now under attack because there has been a diminution of trust. We can get it back, but it is going to require standards and it is going to require training. Training is the heart and soul of it all—for SWAT teams in particular. It cannot be just an odd assortment of people coming together equipped with heavy weaponry. They need to constantly train together and they need to basically adhere to standards. The organization that you referred to has very significant standards for what they would want their members to be capable of achieving.

Senator MCCASKILL. Does anybody have a problem with the Federal Government establishing some kind of minimal standards of training for the deployment of SWAT resources that have been given to State and local governments by the Federal Government? OK.

Commissioner BRATTON. I think that you are talking about two different issues. One issue is the equipment that has been given to them relative to the standards set for them—because the equipment issue is one that is the subject of great debate at the moment, as you know—the type of equipment given, how it is being utilized, and the lack of standards as to how it should be utilized. So there are several different issues.

Senator MCCASKILL. That is what this bill would do. This bill would say that, if you are going to get this type of equipment from the Federal Government, you would be required——

Commissioner BRATTON. As to how it should be utilized, how it should be——

Senator MCCASKILL [continuing]. To have a program in place that would require training. The notion is that we would no longer—because what we discovered—we discovered a number of things after Ferguson in a hearing that we had in this Committee. One was that of the three programs—the DHS program, the Byrne grant program, and the 1033 program of the Department of Defense (DOD)—the leaders of those three programs sat in your chairs and they had never met each other before. They had never met each other before that day, which was jaw-dropping to me. We also learned that there was a proportionality issue, where we had little-bitty, tiny departments getting Mine Resistant Ambush Protected Vehicles (MRAPs) that had been in a shed for years. We had little-bitty, tiny departments getting way more military weapons than there were even sworn officers in their departments. There did not seem to be any rhyme or rationale regarding need and whether or not those communities were equipped to handle that equipment. Yes, Mr. Sparks?

Chief SPARKS. I guess that I want to touch on this in two respects. Being a smaller community, we have a couple of members of our department that are on a countywide SWAT team. But our officers—we do not have the luxury that some of the larger cities have. We do not have regional SWAT teams. So if we respond to an active shooter incident, it is going to be patrol officers responding. And when you are talking about the equipment needed, they need at least long guns—they need tactical rifles. They need, obviously, their ballistic vests. But it would be nice to have ballistic shields and helmets—not that they are worn, but that they are in those squad cars, because, by the time a SWAT team arrives, that incident is over. And, the quicker that we can get the appropriate equipment to our patrol officers, the better—because they will be the ones there. It is not going to be a SWAT team. And it is going to be a significant amount of time before we actually get people who are SWAT trained or people who have the tactical equipment there to respond. So, if we are not equipping our frontline officers—all of our officers on SWAT team are trained. In fact, we have seven officers in our department that are SWAT trained. And we also do a lot of additional training as far as active shooter incidents. But they are not all SWAT team members. And across America, the majority are going to be patrol officers who need that equipment.

Senator MCCASKILL. Right. Well, that is why I want to make sure—I mean, I think that one of the reasons we wanted to do this

is to make sure that your department gets that equipment that you need and not five Ballistic Engineered Armored Response Counter Attack Trucks (BearCats) or five MRAPs that were not even ever designed to run on city streets in the first place. I guess that that is the argument that I am making, getting your department, Mr. Sparks, what you need in light of who your personnel are and what your demands are. None of that was going on with these Federal programs. There was nobody checking, there was no reporting back, and there was no—they could not even tell me if the equipment was being used in the various communities that were getting it—especially the DOD. Once it was out the door, they were done.

I have been a little disappointed that there has not been more robust support for the bill because I think that law enforcement is in a little bit of a defensive crouch, and there was a sense that well, if you open this up, then maybe somebody will take the programs away. I am not going to let anybody—I do not want anybody to take the programs away. I have seen how they work. I know that they are important. I do think that a little bit of tweaking in terms of proportionality and training is probably the order of the day—and I would certainly appreciate you all taking a look at the legislation and seeing your way through to let us know if there are any problems that you see with it that we need to fix, which we are willing to do. On the other hand, it would be helpful if we could get more folks—I think that people are just afraid of doing anything and worried that it is going to take something away. I would like to see us get beyond that, if possible.

Thank you all very much.

Chairman JOHNSON. Thank you, Senator McCaskill.

We really could go on and on. There are so many questions. But what I would like to do is give everybody an opportunity to just make a final comment—please keep it somewhat brief—before we close out the hearing. We will go in reverse order. Mr. Ghilarducci.

Mr. GHILARDUCCI. All right. Well, great. Again, thank you very much for the opportunity to speak with you.

This has been a fascinating discussion, and I think that it just presented the challenges that we continue to face. The threat continues to change. Your support, the support of the Federal Government to State and local governments, is absolutely critical. And you started off, Senator, saying the percentage of funding that is really made available is minuscule compared to what the need is. California, since 2008, has lost $150 million in homeland security funds. We need to reverse that trend and we need to put resources into our communities to get us to where we need to be.

Thank you.

Chairman JOHNSON. We need to prioritize spending. Commissioner Davis.

Mr. DAVIS. Well, thank you for your attention to this issue, Senator. I just truly believe that this threat has created a theater of war, domestically—and we need to address it like that—the geographic distribution of these pieces of equipment, not to each individual small town, but geographically, so that they can be called in, if necessary.

But the bottom line is—and it goes to the last question that was asked—that the balance between the militarization of policing and

the community policing that we all want in our communities requires strong leadership on the part of Chief Sparks, Commissioner Bratton, and other people who are in those positions across the Nation. They have to keep pushing not to allow that military mentality to take over, remembering that we are there to keep the peace—not just to arrest people.

Thank you, Senator.

Chairman JOHNSON. Chief Kerr.

Chief KERR. Thank you, and I appreciate the invitation. I just want to remind all of you that the title of this hearing is "Frontline Response to Terrorism in America." I encourage you not to forget about the part and the role that is played by the fire service and EMS. We realize that there is funding needed to help our law enforcement partners, but I encourage you all to make sure that we do not forget and ignore the fire service and EMS.

Just one comment on what Commissioner Bratton talked about regarding his device right here that he keeps holding up and the information that they can get from that. Imagine the information that can go to every first responder in America through a smartphone or a smart device—and that really is part of what FirstNet is about—transmitting data to make sure that a first responder who goes into a house to help somebody that has a seizure where the man sits up and shoots the first responder in the chest, that if that first responder had information, that this person had behavioral issues prior to going into that house, then the first responder may still be alive today.

So, it is important that we are really taking care of our first responders who are taking care of our community—whether they are law enforcement, fire, or EMS.

Thank you.

Chairman JOHNSON. Commissioner Bratton.

Commissioner BRATTON. Thank you. Well, the issue of concern here is terrorism on the front lines, and I will go to Senator Booker's comment about duality. It is quite clear that we are losing more lives through traditional crime in this country, and at the same time, we are very concerned about the potential for losing more lives to terrorism.

The benefit that we have is the duality, the idea that while combating one, we can combat the other. So, the technology that we have referenced and the collaboration that we have referenced, that means that you—who have to make the funding decisions as it relates to this issue, terrorism and crime—can get double the bang for the buck. That smartphone that I held up works for terrorism notifications, as well as fire coordination notifications, as well as for crime prevention.

Similarly, so much of what we have talked about, in terms of interoperability, the device that works for conveying data for terrorism works for conveying data about a fire or a life-saving emergency. So we do benefit, at this particular time, that there is the duality of concern about crime, which takes more lives, and the growing potential of more lives being taken by terrorism. Actually by solving one, we can solve the other.

Chairman JOHNSON. Chief Sparks.

Chief SPARKS. I just want to touch on—when it comes to priority and the funding, we need to make sure that all of the departments out there at least have the basic level of training for active shooter response. It is critical. There are a lot of small communities that still do not have that. So, if we can funnel that through on criteria that gets it out to those local agencies, then that would be great.

And then, we can encourage the cooperation among these small agencies, because they are not going to be responding on their own, so that means getting people within counties to actually work together and train together.

And then, regarding the information sharing, we have to break down some of those silos—and some of the policies are inhibiting that free flow of information.

And the last point that I really want to talk about—and you talked about law enforcement in general as taking a hit—in my community, since a lot of these incidents have occurred, it is just the opposite. The outpouring of support has been phenomenal and the community trusts the department. And I think that it is important for you to recognize that these high-profile incidents do not define who law enforcement is. We have people on the front line that are willing to put their lives on the line—and do not lose sight of that, because it is that local police officer, in whatever community it is, who is going to be the one charging in there when an incident occurs—and they deserve a little more respect.

Senator CARPER. Can I say something?

Chairman JOHNSON. Sure.

Senator CARPER. Before we close, I just want to thank Senator Heitkamp and Senator Baldwin, again, not just for suggesting this as a topic for a hearing, but also for you and your staffs, and for our staffs, who collaborated in inviting all of you to come. And you were a terrific panel—and I said this to the Chairman. And we generally have very good panels—but you guys are terrific, and we are grateful, not only for your service, but also for what you have done here in conveying this information in very helpful ways.

Thank you.

Chairman JOHNSON. Senator Carper, I mentioned this earlier. Go to the YouTube page and look at the dashcam video from those first responders responding to the Sikh temple shooting. Take a look at the pictures of those first responders walking up the stairs of the World Trade Center. We see the service and the sacrifice.

I want to thank all of you for your time, for putting together this very thoughtful testimony, for your answers to our questions, but really thank you for your service to your communities, to your States, and to this Nation. Truly, I think everybody on this panel would certainly agree with that and approve that message. Correct?

Senator CARPER. I am Tom Carper, and I approve this message. [Laughter.]

Chairman JOHNSON. So, with that, the hearing record will remain open for 15 days—and, by the way, I think that you can probably expect some questions for the record, and we would appreciate your responses to those.

The record will be held open until February 17th at 5 p.m. for the submission of statements and questions for the record.

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

APPENDIX

Chairman Johnson Opening Statement
"Front-Line Response to Terrorism in America"

Tuesday, February 2, 2016

As submitted for the record:

Good morning and welcome.

Just last week, federal, state and local authorities worked together successfully to thwart an apparent terrorist attack on a Masonic center in Milwaukee, Wisconsin. It was a reminder of the serious threats we face in the United States in 2016.

Over the past year, terrorist attacks have occurred in communities across America—including in Boston, Massachusetts; Garland, Texas; Chattanooga, Tennessee; and San Bernardino, California. A number of other attacks poised to cause mass casualties were thwarted by federal, state and local authorities. U.S. authorities reported a high number of terrorism-related arrests last year — in fact, the most since 2001.

The threat is real. It is growing. And it can happen anywhere.

As chairman, my main focus is to help ensure that the federal government is fulfilling its first responsibility: to keep our nation safe and protect the American people.

It will require hard and effective work by federal, state and local authorities to identify extremists and disrupt terrorism plots before they occur, as they did in Milwaukee last week.

The American people will need to do their part too. This includes staying alert and reporting suspicious behavior to law enforcement authorities.

Unfortunately, we are learning the very difficult and tragic lesson that we will not be able to prevent every terrorist plot in the United States. And when terrorist attacks and other horrific crimes do occur, local first responders are the first to arrive at the scene and coordinate to secure the area, clear the building, and eliminate the threat. These heroes put their lives on the line each day to protect the American public.

We are fortunate to have a diverse panel of state and local witnesses with us today who can speak to the local response during recent attacks. We will also hear what police, fire and emergency service personnel in communities across America are doing to prepare for the next attack. Earlier this year, I traveled across Wisconsin on a national security listening tour to hear directly from local first responders and citizens. I would like to extend a special welcome to Chief Sparks, who attended one of those sessions and is bringing that message to Washington today.

It is my hope that this discussion will help us draw lessons learned about what first responders in communities across the country can do to save lives after terrorist attacks.

I also want to draw on the experience of our witnesses to help us understand how we can work together better to prevent terrorism:

For example, how can we improve our information sharing programs and operations? Our front lines of defense — state and local authorities — need to have all the information available to stop terrorist attacks.

How can we ensure better cooperation and collaboration between law enforcement agencies on terrorism investigations to prevent attacks? We can't afford silos. We can't afford not to work together.

We have made progress in these areas since 2001. But to address the serious and growing threat of violent extremism in the months and years ahead, we will need to do better.

I thank each of you for being willing to testify today. And, more importantly, thank you for your service on behalf of the American people.

Statement of Ranking Member Tom Carper
"Frontline Response to Terrorism in America"

Tuesday, February 2, 2016

As prepared for delivery:

I would like to thank the Chairman for holding today's hearing. I would also like to thank our witnesses for being with us today to share their experiences responding to terrorist attacks and other emergencies. I would especially like to recognize Senators Baldwin and Heitkamp for proposing this important and timely hearing and also for their leadership on first responder issues.

Since 9/11, the federal government has worked hard to ensure that those on the frontlines – our police officers, firefighters, and emergency medical personnel – are better prepared to help prevent and respond to terrorist attacks and natural disasters. For example, we have helped local officials develop response plans for mass casualty events. We have also helped train thousands of law enforcement officers. And we have helped build a network of fusion centers to deliver more timely information to our first responders.

Of course, we have also provided grant funding for equipment, personnel, training, and other needs. I am pleased that the spending bill that we just passed in December contains over one billion dollars in grant funding to help states and localities prepare for and respond to terrorist attacks and other disasters.

The recent tragedies in Paris, Boston, Chattanooga and San Bernardino, however, are a stark reminder that we must continue to remain vigilant and ensure as best we can that our first responders are ready for anything that might come their way.

That is why we will be paying close attention next week to the President's fiscal year 2017 budget request. We need to make sure that it provides the selfless men and women who keep us safe with the resources they need to save lives and stay ahead of the threats we face as a country.

Today's terrorist threats are very different from those we experienced on 9/11.

Today, we unfortunately know that one or two people with an assault rifle or homemade bomb can create unimaginable havoc and can throw a whole city into turmoil. Cities like New York, Boston, and Washington D.C. have been dealing with terrorist threats for quite some time. But we know that with the help of online radicalization, a terrorist attack can happen anywhere, anytime.

I look forward to hearing from all of our witnesses today about how Congress can further help communities both large and small be better prepared for the type of terrorist attacks we are witnessing today, such as active shooter events.

I would also like to hear about what else we could be doing to stop homegrown extremism, something that I know all of our witnesses are familiar with.

Last December, I introduced legislation to strengthen the Department of Homeland Security's efforts to work with community leaders in identifying and preventing potential homegrown terrorist threats. It is my hope that we can move this legislation soon so that the Department is better equipped to counter the hateful messages put out by ISIS and other terrorist groups.

Again, I would like to thank all of our witnesses for being with us today and for their willingness to share lessons learned on how we can make our country a safer place for us all.

EVEREST METROPOLITAN POLICE DEPARTMENT

Serving the Communities of Schofield and Weston

Chief: Wally Sparks
Captain: Clayton Schulz
Captain: Mark Hull

Testimony of Mr. Wallace L. Sparks
Chief of Police for the Everest Metro Police Department, Weston, WI
In front of the United States Senate Homeland Security and Governmental Affairs Committee
Hearing on "Frontline Response to Terrorism in America"
February 5, 2016

Chairman Johnson, Ranking Member Carper, and Members of this Committee, thank you for the invitation to speak to you today on this very important subject.

On behalf of the Everest Metro Police Department and all of the countless smaller local police agencies across the country, I would like to thank you for the opportunity to discuss the challenges faced by local law enforcement in today's threat environment. I will discuss some of the efforts undertaken to prepare our officers for these potential threats and how we coordinate our efforts with our neighboring law enforcement agencies as well as our colleagues at the state and federal levels.

I think one of the most important aspects to understand is that the vast majority of this country is served by smaller local police agencies. According to the recent census compiled by the U.S. Department of Justice - Bureau of Justice Statistics (2008), you will find that the local police and sheriff's departments account for 84% of all sworn personnel in the U.S. The following statistics will also reveal that the majority of these sworn officers come from small agencies, which face some distinct challenges when compared to large cities and heavily populated metropolitan areas.

- *Local police departments were the largest employer of sworn police personnel, accounting for 60% of the total. Sheriff's offices were next, accounting for 24%.*
- *86.2% of local police agencies have less than 50 sworn officers*
- *72.8% of local police agencies have less than 25 sworn officers*
- *77% of Sheriff's departments have less than 50 sworn deputies*
- *58.3% of Sheriff's departments have less than 25 sworn deputies*
- *49% of all law enforcement agencies employ fewer than 10 full-time officers*

5303 Mosker Street, Schofield, WI 54476 • Phone: (715) 359-4202 • Fax: (715) 359-4204
www.everestmetropolice.org

I provide these stats, because I feel it is important for this committee to understand that while events in the larger, metropolitan areas tend to dominate the headlines, the majority of policing efforts occur in smaller communities. The size of a law enforcement agency can have a significant impact on the delivery of policing services in a community, particularly when discussing threats like terrorism.

To provide greater context, I will share some background on the Everest Metro Police Department, which I have been fortunate enough to lead since 2009. This is a multi-jurisdictional department created in 1993 when two municipal police departments serving the Town of Weston and the City of Schofield merged to create the Everest Metro Police Department. Our department provides police services to the City of Schofield, the Village of Weston and the Town of Weston with a combined population of around 18,000. The department has 29 employees, 25 of which are sworn officers with four civilian support staff. We are located adjacent to the City of Wausau (population 39,000) and located in Marathon County (population 135,000) which is the largest geographic county in Wisconsin covering 1,576 square miles.

We have nine law enforcement agencies in Marathon County, only three of which have 25 or more sworn officers/deputies. The remaining six law enforcement agencies all have 10 or fewer officers. The three largest agencies are Wausau PD with 70 sworn officers, the Marathon County Sheriff's Department with 66 sworn deputies and Everest Metro PD with 25 sworn officers. Our three departments are all located in close proximity in the Wausau/Metro area. The greater Wausau/Metro area is located in North Central Wisconsin and sits at the intersection of two major highway systems, halfway between Milwaukee, WI and Minneapolis/St. Paul, MN. This area is also a drug distribution hub to the northern third of Wisconsin and is considered a major area of drug trafficking from both Chicago/Milwaukee and Minneapolis/St. Paul.

Within the Everest Metro jurisdiction, we have the DC Everest School System and two private parochial schools with eight school campus locations and a total enrollment of 5,924 students. We also have a number of large international businesses, some of which have military contracts, as well as a large power plant located just a mile outside of our jurisdiction. We have a large hospital complex, a number of churches, including two large churches with 3,000 to 4,000 members each. Needless to say, these all represent potential terrorism targets, and are usually served by only three patrol officers on duty with a patrol area covering approximately 44 square miles.

Why is it important for you to know this? Because this is closer to the norm for the law enforcement agencies across this nation, most of which face the same challenges as we do. Large cities like New York, Los Angeles, Chicago, Boston and many others have very different structures and policing models that provide for greater levels of specialization than local police departments, which as articulated by the statistics, represent over 80% of all sworn officers in this country. When you look at the response capabilities from past terrorist events in New York, Boston and San Bernardino, the amount of personnel and the level of specialized equipment that responded to these scenes within minutes is remarkable. Unfortunately, if a similar attack occurred in a community similar to ours, the amount of personnel able to respond, the promptness of that response and the level of tactical equipment available will be drastically lower.

We understand that terrorists typically look for soft targets and that they are learning and adjusting to how we respond to threats. Just this week the FBI arrested an individual in Milwaukee for plotting to kill at least 30 people at a Masonic Temple. A couple of our local churches have up to 1,000 people attending a single church service, one of which is 15 seconds from an on/off ramp for a major highway. A shooter could kill hundreds and be back on the highway by the time officers were even dispatched. These are the thoughts that run across my mind and probably trouble thousands of other police chiefs and sheriffs across this country as they consider what threats and challenges they face in their own communities.

So, what has our department done to prepare for such an attack? It starts with training and like the rest of law enforcement across the country; we have provided active shooter training to all our officers since the Columbine school shooting caused law enforcement to adapt their response protocols to active shooter events. Since I have been here in 2009, we have upgraded our tactical rifles, and progressively expanded our training which is summarized in the timetable below:

- 2010 - We acquired Tactical Response Threat Vests to include extra rifle and pistol magazines and other tactical accessories for officers to carry in the event of a critical incident. These vests included drag straps so officers could be pulled from incident scenes if they were shot or wounded at scenes.
- 2011 - We conducted Active Shooter Response training at one of our elementary schools with the Sheriff's department and three other local police departments so all our officers could train together to help with coordinated responses.
- 2011 – We worked with the Sheriff's Department, and Wausau PD to train officers/deputies from our three departments as MACTAC Instructors. MACTAC stands for Multiple Assault Counter Terrorism Action Capabilities.

- 2012 - The MACTAC instructors trained all Everest Metro officers on MACTAC and had both live fire exercises at the range as well as scenario exercises at a local elementary school.
- 2012 – One of our instructors, who also served on the Marathon County SWAT team attended TEMS Training and served as the TEMS operator for the SWAT team. TEMS stands for Tactical Emergency Medical Specialists and was derived from the military experience with Tactical Combat Casualty Care. This allows officers to provide immediate life saving measures to wounded officers and civilians in the field, which is critical in preventing loss of life.
- 2012 - The Marathon County SWAT team was licensed as the first TEMS team in Marathon County
- 2013 - All Everest Metro officers were trained in TEMS and the department purchased TEMS equipment kits for all officers to be placed on their Tactical Vests and deployed in every squad.
- 2013 – All SWAT team members were trained in TEMS as basic operators.
- 2013 - Everest Metro PD conducted an Active Shooter Joint Training Exercise with our local Hospital.
- 2013 - Everest Metro PD SWAT officers worked with the Marathon County Sheriff's Department to develop presentations to local groups and organizations regarding Active Shooter Responses.
- 2014 – Everest Metro conducted scenario training at a local Jr. High School to include all the disciplines of Active Shooter, MACTAC and TEMS.
- 2014 – An Everest Metro Detective and SWAT team member co-authored the Wisconsin Department of Justice Training Guide for Tactical Emergency Casualty Care for the Law Enforcement Manual that was approved by the Law Enforcement Standards Board and is now included in the Law Enforcement Academy Training Curriculum for 2016.
- 2015 – Our department purchased a .308 AR-10 Designated Marksman Rifle to be placed in one of the patrol supervisor's squads to upgrade our threat response to a terrorist style attack. The department plans to purchase another in 2016 when more budget funds are available.
- 2015 – Our department sent four officers through CIT (Crisis Intervention Training) conducted by NAMI (National Alliance on Mental Illness) and we are working with Marathon County Sheriff's Department and North Central Technical College to host CIT trainings locally in 2016 to get the remainder of our officers trained in CIT.
- 2015 – Worked with our local Hospital to conduct and debrief another Active Shooter exercise and debriefing.
- 2015 – Reached out to all the local churches to offer presentations and advice regarding active shooter threats. A presentation was made to one of the large churches in 2016.

This timeline illustrates the steps we have taken as a department, but it also reveals how much coordination we have with the other agencies in our community. I cannot underscore just how important those relationships are in smaller communities. In Marathon County, we have departments that work extremely well together. Both Everest Metro PD and Wausau PD have members on the County SWAT team and the Special Investigations Unit (drug unit). We have a Countywide Dispatch Center and a shared records system that allows information to be shared and flow freely through all the law enforcement agencies. Having spent 23 years in law enforcement in another community and in speaking with fellow police chiefs throughout Wisconsin and other states, I can tell you that this is far from the norm.

Our relationships with the fire department and EMS first responders has also been outstanding with seven members from both the Wausau Fire Department and the Safer Fire District (which serve the majority of the metro area) serving as TEMS operators for the SWAT team. As President of the Wisconsin North Central Chiefs of Police Association (NCCPA) which I had the privilege of leading for the past 18 months, we have also developed great relations with our neighboring counties and the law enforcement leaders from local, county, state and federal agencies. We have regular meeting attendance and representation from the Wisconsin Division of Criminal Investigation, the local FBI field office in Wausau as well as Tribal police and even Canadian Railroad Police. These relationships and information sharing at our meetings has resulted in formal mutual aid and assistance agreements with our respective departments to assist each other in the event of a major critical incident in any of our communities.

I believe these are the key successes our department and community have achieved and are the foundation of our preparation for responding to an attack in our community. With this foundation laid as the starting point, there are still challenges we face and areas that we need to improve upon. One major challenge is budgetary and trying to prioritize expenditures for things like tactical equipment. I am in the process of drafting a proposal to purchase ballistic shields and helmets for our patrol squads so that they will have the appropriate equipment if they have to respond to an active shooter. This equipment is not worn and is only used in the event of a critical shooting incident. I will be asking to use some non-designated fund balance proceeds to purchase this equipment if approved.

Along those same lines, is staffing levels. While training is, and always will be, a priority for our department, it is difficult to send staff away for some of these specialized trainings and maintaining sufficient staffing levels to staff the road. With 25 sworn officers, we are able to juggle our schedule enough to accommodate most of the training needs, but that is not true for many of the other departments, most of which have only one or two officers working at any given time. That is why only the three largest departments in Marathon County have staff

trained in such critical areas like TEMS, MACTAC, SWAT and other specialty disciplines. We also have one combined SWAT team that, based upon the average duration of the active shooting events that have occurred this country, would arrive well after the "active" threats have been eliminated or fled the area. This means that our patrol officers and deputies will be engaging these threats with only the tools available to them in their patrol squads.

As an example, if we had an active shooter incident on the west end of Marathon County, there would be one or two officers / deputies arriving while waiting a significant amount of time for back-up officers and probably close to an hour before any highly trained officers or SWAT members or the lone tactical vehicle from Marathon County Sheriff's Department SWAT team could arrive. While there will be countless resources coming from both State and Federal agencies, the response times would be well after the attack and resulting carnage. These resources would still be needed to handle the lengthy aftermath of an event, but would not help prevent or limit the amount of casualties.

This reflects the need for additional training and equipment for rural police officers and deputies. We know from previous incidents that those precious minutes at the onset of any incident are critical. All officers should have basic training in Active Shooter Scenarios, MACTAC and TEMS and have TEMS kits and ballistic shields and helmets to give our officers a fighting chance of survival. Next, we need to be engaged with our local EMS providers, who should also have TEMS training and the necessary TEMS equipment. Our current EMS provider has trained their staff in TEMS and conducted some warm zone training with the SWAT team, but they have no equipment to wear (ballistic vests and helmets) that would be necessary to respond as a Rescue Task Force (RTF). Our department is including SAFER Fire District in our Active Shooter Response training in 2016, but they don't have funding for the equipment needed to fully implement the program right now.

To this point, my testimony has been focused on our training and capabilities when <u>responding to</u> events, but perhaps the biggest area for improvement lies in how to <u>prevent</u> events. I have talked about local cooperative efforts, information sharing and how critical those are to the success of the average smaller community. One key preventative measure is in hardening our targets. As a community, taking those steps outlined above through proper training, the acquisition of equipment needed to respond to events and reaching out to community leaders and organizations and teaching them how to prepare are vital.

On the wake of the San Bernardino incident, there has been a significant focus on the *"If you see something, say something"* campaign. This is obviously an extension of the basic neighborhood watch model that law enforcement has been successfully using for years. And,

like the neighborhood watch program, those "say something" comments are most likely going to be delivered to their local police agencies. Suspicious activity calls are one of the most common calls received from law enforcement agencies. Some are related to possible drug activity, some just nosy neighbors and some are just nuisance activities. Many of these calls are unsubstantiated, some result in arrests and drug investigations, while many others are just normal everyday activities.

So how do local police agencies vet these calls to determine if there is any merit? One is obviously looking through our previous contacts in our police records systems, checking address histories and making contact if the fact situation warrants it. The problem is that rather innocuous behaviors for someone with no known history or problems may find this information being closed out by a patrol officer with nothing to act upon. But, what if local law enforcement knew that this person was on a FBI watch list? Those innocuous behaviors may lead to a very different conclusion and warrant contact with our local FBI office or the closest Joint Terrorism Task Force.

In my 30 years in law enforcement, I had numerous interactions with local FBI agents on some higher profile cases or interstate cases where federal involvement was warranted. Not to disparage anyone or the agency as I have a good relationship with our local agents, but the historical dialogue has been primarily a one way street. There have been efforts to improve this and I have seen some progress, but if we as a country are going to be effective in proactively trying to disrupt and prevent these attacks, vital information must be passed down to the local police and sheriff's departments. The FBI has its hands full just trying to monitor those they already know about and if we are not effectively engaging local law enforcement and providing such information as known potential offenders that have been designated as suspicious or placed on a watch list, we are missing a key piece of the preventative puzzle.

I understand the need for secrecy on active investigations or current surveillance measures, but absent that, I would want to know if I have someone living or working in my community that is on the FBI radar. I have spoken with fellow law enforcement executives and I can assure you that they feel the same way. Unfortunately, we do not having the staffing level to have a member of our department assigned to the JTTF and the closest location is in Milwaukee, which is three hours away. We do receive some intelligence bulletins, which are helpful, but we generally do not receive targeted intelligence that has direct bearing on our community. I am not familiar with the policies governing information sharing at the federal level, but if they are inhibiting the free flow of such information with local law enforcement, this is something that needs to be changed.

In speaking with my colleagues from the North Central Chief of Police Association, most do not have anyone assigned as a Threat Liaison Officer or Fusion Liaison Officer. While these are great programs, very few small departments have the staffing, time or training dollars to send staff to participate in these programs. If it were not for our local North Central Chiefs of Police Association, most of our local chiefs would probably not even know who their area FBI agents are. I credit our local agents for attending these meetings and being able to establish a rapport with local law enforcement leaders. As law enforcement executives, we are barraged with emails and correspondence from multiple organizations, training bulletins and networks. For the larger state and federal agencies to be effective with information sharing outlets, those personal connections and relationships are absolutely critical.

Summary and Recommendations

The landscape of law enforcement has been forever changed with the increasing occurrences of terrorism in our country. The thought of small communities feeling that "it would never happen here" is changing. Local law enforcement leaders throughout the country should be realizing that "it may very well happen here" and if it does, are we prepared?

Training:

- Develop and provide at least partial funding or grants for training programs in the area of Active Shooter, MACTAC, TEMS, Rescue Task Force, and Crisis Intervention Training that can be delivered regionally throughout each state so local public safety responders can receive this vital response training. Grant funding should be prioritized for communities and agencies providing joint and shared services to encourage training and working together in these vital disciplines. Most grant funds, including the current COPS program goes to large metropolitan agencies who have full time staff with significant grant writing experience.

Information Sharing:

- Review current policies and protocols as it relates to information sharing among federal, state and local law enforcement agencies. We need law enforcement leaders who will break down parochial and bureaucratic boundaries and work together for the greater good and provide for the safety of all our citizens. Information must be pushed down to the operational levels of organizations. As a police department, we are only effective if our front line officers have the information they need to properly assess potential threats and respond accordingly.

Narrative and Optics:

- The profession of policing has been placed under intense scrutiny and while accountability should be one of the top priorities for any police chief or sheriff, disparaging the profession as a whole through the acts of a few has caused considerable damage. We ask our brave men and women to place their lives on the line to protect the communities we serve. Highlighting the actions of a few bad apples while ignoring the dedicated and unselfish actions of the majority is causing severe damage to a profession that is desperately needed with these increasingly dangerous threats.
- The militarization of the police has been unfairly represented. These weapons and equipment are needed when we face these extreme threats. We need to the tools to counter the threats we face and our officers deserve to have equipment that will hopefully allow them to survive an encounter and return home to their families.

I would like to thank you for the opportunity to share this information with this esteemed Committee and will be happy to answer any questions you may have.

Respectfully Submitted,

Chief Wallace L. Sparks

NYPD
New York City Police Department

TESTIMONY OF POLICE COMMISSIONER WILLIAM J. BRATTON
NEW YORK CITY POLICE DEPARTMENT

BEFORE THE UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
"Frontline Response to Terrorism in America"

FEBRUARY 2, 2016

My thanks to the committee for the opportunity to speak with you today.

The issue before us—the frontline response to terrorism in America—is more pressing than at any time since 9/11. New York City, where I am the police commissioner, remains the top target for terrorists in the United States. Since the first bombing of the World Trade Center in 1993, New York City has been the target or nexus for twenty terrorist plots, more than any other American City. There have been four major cases in just the past two years.

Since 9/11, the NYPD has spent hundreds of millions of dollars—in federal funding, city and state monies, and private grants—to counter that threat. My predecessor as police commissioner, Raymond Kelly, oversaw the creation of a sophisticated intelligence and counterterrorism capability. It was highly capable, but was limited by headcount restrictions. Over the past two years, Mayor Bill de Blasio has addressed that with the largest personnel and equipment allocations in the NYPD's history. Because of these, we are evolving in order to face the increasingly complex threat picture.

That picture now includes ISIL, and lone wolf actors—threats that barely existed two years ago. While we are always on guard for the spectacular Al Qaeda-style attack, with ISIL we have seen a shift towards low tech, low cost, high impact attacks. November's Paris attacks left 130 people dead. In San Bernardino, 14 were killed. In New York City, this Spring, we saw three separate plots—all influenced by ISIL—to either behead people, bomb public events, or attack police.

We cannot address these threats without partners. Two years ago, I directed John Miller, my Deputy Commissioner for Intelligence and Counterterrorism, to execute a "collaborative reset" with our closest allies: the FBI, Secret Service, DHS, Fire Department, and the Port Authority. By way of example, the FBI sits in on the NYPD's intelligence case meetings, and we sit in on the FBI's. We have also worked to improve the NYPD's intelligence capabilities.

For more than a decade, with the help of the New York City Police Foundation, we have placed NYPD liaison officers overseas where they work with and learn from local law enforcement. We currently have 11 stations, and are adding one in Australia, as well as seconding an officer to Europol. By getting real-time, on-the-ground insight into overseas terrorist attacks—in Tunisia, France, Australia, and Canada—the liaison program has helped us redesign our tactical posture in New York City.

Given the nature of the threat, however, intelligence must be accompanied by a response capability. Our primary asset in this regard is our Emergency Service Unit, or ESU—the best trained police officers in the world. But ESU is small, and needs to be mobile. So for years, critical sites were instead guarded by patrol officers borrowed each day from routine precinct assignments. These officers were neither trained nor equipped to counter the type of threat they were deployed against. With the help of Mayor de Blasio and the New York City Council, we created the Critical Response Command. CRC is a dedicated team of over 500 specially trained officers with special weapons and enhanced body armor. They're briefed on the latest intelligence, deployed daily to potential terror targets, and prepared to mobilize for active-shooter or terrorist events such as those in Paris or Mumbai.

We have also revamped our citywide task force, the 800-member Strategic Response Command, which is primarily used for crime response and disorder control. It, too, has been trained and equipped to address the new threat picture.

Today, we have 1,800 officers capable of being deployed with special weapons, spread across the city. That capability is unmatched by any other city.

Despite this, it remains likely that the first officers on the scene of any event will be patrol officers. Accordingly, we have already trained 3,500 NYPD officers in active-shooter tactics. They learn how to form small "contact teams" and move toward the threat, with the aim of reducing the gunmen's "time on target" and saving lives. We will continue the training until all our patrol officers have it.

And through our Shield Program, a public-private partnership, we have already trained 20,000 civilians in what to do—run, hide, fight—if they find themselves caught in such a situation. But

again, these threats cannot truly be addressed without partners. For example, we have worked with the New York City Fire Department to develop ways to get to the victims of a Paris- or Mumbai-style attack as quickly as possible. The Rescue Task Force uses the new tactical teams we have developed—CRC and SRG—to provide force protection to guide paramedics and EMTs into "warm zones" where shooting has ended, while other teams—primarily ESU—go after the terrorists or gunmen in "hot zones."

Our efforts go far beyond these particulars, but mindful of time, my descriptions of a small number of others will be brief.

We have expanded our pack of bomb-detection K-9s known as "vapor wake dogs," which can pick up the scent of explosives on the move — for example, being carried by a suicide bomber through a subway station or a public event.

Thanks to $160 million from Mayor de Blasio and District Attorney Cy Vance, we have given smartphones to every officer—with alerts, tools, and apps that turn all 35,000 of my cops into counterterror assets.

We conduct multi-agency tabletop exercises and field drills that mirror the tactics we see in the latest terror attacks overseas. Secretary Johnson recently attended one, focused on our subways, and gave it high marks. The drill tested the new Rescue Task Force and a larger, full-scale exercise is planned for May of this year. I am pleased to say that the NYPD-DHS relationship has never been stronger.

Finally, I cannot say enough about the work of the FBI-NYPD Joint Terrorist Task Force. Under the leadership of FBI Assistant Director Diego Rodriguez, this 35-year partnership—the first JTTF in the country—is a seamless coalition of federal, state, and local law-enforcement agencies. One hundred NYPD detectives are assigned there, and the four plots interdicted in the last two years were JTTF cases undertaken in concert with our Intelligence Bureau.

No other city faces the threat faced by New York City, and no other city has invested so much—in dollars, personnel, or partnership—to counter that threat.

I would be happy to answer any questions.

Frontline Response to Terrorism in America

Statement of
Fire Chief Rhoda Mae Kerr
President and Chair of the Board

presented to the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

United State Senate

February 2, 2016

INTERNATIONAL ASSOCIATION OF FIRE CHIEFS
4025 FAIR RIDGE DRIVE • FAIRFAX, VA 22033-2868

Good Morning, Chairman Johnson, Ranking Member Carper and members of the committee. I am Rhoda Mae Kerr, fire chief of the Austin Fire Department, and President and Chair of the International Association of Fire Chiefs' (IAFC) Board of Directors. The IAFC represents more than 11,000 leaders of the nation's fire, rescue and emergency medical services. Thank you for the opportunity to discuss frontline response to terrorism in America.

The fire and emergency service is a key component to the response to a terrorist incident. The revised National Preparedness Goal includes "Fire Management and Suppression" as a core capability. The local fire and emergency medical service (EMS) department will be on-scene early in the incident to provide fire suppression capability; emergency medical response, including victim triage; search and rescue capability; and, in some cases, bomb squad response. The local fire and EMS department expects to be the first on-scene and provide critical emergency response and lifesaving care for up to 72 hours before receiving any federal assistance.

The Evolving Terrorist Response

This year marks the 15th anniversary of Al-Qaeda's September 11 attacks. After 9/11, the nation took great steps to improve its preparedness for future terrorist attacks. Our main focus was another attack similar to 9/11, which involved a complicated large-scale effort planned from overseas using airlines, bombs, chemical or biological weapons. The concern was that the terrorists would use a large-scale attack and the resulting media phenomenon to raise the profile of the sponsoring organization and spread fear and insecurity in the nation, as Al-Qaeda had done using the airplane attacks of 9/11.

Over the past years, this threat has evolved. Overseas, in last November's Paris terrorist incidents and the incidents in Mumbai in 2008, the terrorists implemented coordinated attacks using small groups in multiple areas of a city using a variety of tactics including gunfire and small explosives. The 2013 Boston Marathon bombing involved two brothers using primary and secondary explosive devices. Last May's incident at the Curtis Culwell Center in Garland, Texas, involved two individuals inspired by communications with the Islamic State of Iraq and al-Sham (ISIS). The July incident in Chattanooga involved an active shooter at a U.S. Naval Reserve Center and a military recruitment center. The December incident in San Bernardino involved a husband and wife using active shooter tactics with potential pipe bombs.

These examples demonstrate that terrorists' tactics and techniques have evolved. The actors involved in recent domestic incidents have been small groups or lone wolves. They may be inspired by communications with overseas actors and may be composed of tightly-knit groups (like family members) which are harder to detect.

For the fire and emergency service, we have to prepare for not only large-scale incidents, such as those of 9/11. We also must prepare for active shooter incidents such as occurred in Garland, Chattanooga, and San Bernardino. Meanwhile, we also must be prepared for a coordinated attack using multiple actors and various tactics as occurred in Paris and Mumbai. In addition, the potential remains for a major attack using biological or chemical agents. These incidents may

occur in a major city, a suburb, or even rural America at any time. In addition, there is no federal fire and EMS response capability to provide immediate assistance to a local fire department. The National Guard or U.S. Northern Command may not be able to supply resources until 24 to 72 hours after a terrorist attack occurs.

The local fire and emergency service has actively advocated and engaged in initiatives to prepare for the evolving terrorist threat. Most importantly, we worked with our law enforcement partners and other stakeholders to remove silos that were common prior to 9/11. In addition, the IAFC and other organizations are fully engaged in helping our members prepare for the variety of threats that they face. For example, we have sponsored educational opportunities for our members to learn about the terrorism threat. We also have developed checklists and guides to help fire and EMS departments obtain information about threats to their communities and work with their communities to prepare for them.

Fire and EMS Preparedness

In order to meet this evolving terrorist threat, local fire and EMS departments must take a number of steps to be prepared for potential terrorist attacks in their communities. No fire department has the capability or resources to develop information-sharing, command and coordination, planning and exercise, communications, and specialized response training and equipment capabilities on their own. Local fire and EMS departments must work collaboratively with a variety of stakeholders, including law enforcement, public health, public works, emergency management, state and local elected officials, the private sector and other local stakeholders, as well as other fire and EMS departments in the state and region, and the general public. In addition, the federal government has an important role in supporting local fire and EMS preparedness.

One of the key success elements that local fire and EMS departments need is timely and relevant information about threats to their communities. Because local fire chiefs must balance competing priorities with tightened budgets, they need to have credible information about the tactics, techniques, and procedures that the terrorists are starting to use. The federal government is an important partner in educating local fire chiefs about the threats to their areas. This information should be classified at the For Official Use Only level or even unclassified, if possible. Local fire chiefs do not need to know the sources and methods of how information is obtained; they must however know what tactics the terrorists are planning to use and how to respond to them. Such information is critical not only for the public's safety, but for the safety of the responding fire/EMS personnel as well. Lower levels of classification are important, because many fire chiefs still do not have security clearances and it is difficult to pass on classified information to other stakeholders that do not have clearances.

The IAFC supports state and regional fusion centers, which can serve as a clearinghouse of information between federal, state, and local partners. It is important that these fusion centers have local fire service representation, not only to contribute subject matter expertise beyond typical law enforcement expertise but also so that information can be made actionable for the local fire and EMS departments. For example, I have firefighters assigned to my local fusion center. In addition, the IAFC recommends that fire chiefs develop working relationships with

their local FBI Joint Terrorism Task Force and law enforcement agencies to stay aware of threats to their jurisdictions. The IAFC also has posted a generic set of fire and EMS intelligence requirements that fire chiefs can use when working with fusion centers to explain their needs.

A local fire department also can provide intelligence to the local fusion center and federal, state, and local counter-terrorist efforts. Much as some states require local fire departments to report evidence of domestic abuse, the IAFC urges fire and EMS departments to report suspicious activity, such as if the firefighters witness a heavy presence of chemicals or explosives at a fire scene or civilians asking curiously detailed questions about emergency response operations. The Nationwide Suspicious Activity Reporting Initiative provides training and procedures to local first responders to ensure that they are appropriately trained for suspicious activity reporting. The IAFC also supports efforts like the National Counterterrorism Center's Joint Counterterrorism Assessment Team, which embeds local first responders with federal intelligence analysts to develop specific products aimed at a broader local first responder audience. Fire departments can be of particular value in identifying ways to detect, prepare and mitigate attempts to use fire and hazardous materials as a weapon in a terrorist incident.

One key area of preparedness is the need for local fire and EMS departments to develop mass casualty response capabilities. Local fire and EMS departments must work with local law enforcement, emergency management, and public health agencies to be prepared to respond to an incident involving mass casualties. They must develop capabilities to provide rapid on-scene care; triage patients; and transport patients to the most appropriate hospitals. It also is important for a jurisdiction to develop a patient tracking system, so that authorities can let concerned families and friends know where injured patients have been transported. Federal grants can provide funding for planning and exercises to help communities prepare for mass casualty events.

The events of 9/11 demonstrated the need for a unified command system during the response to a terrorist incident. The IAFC supports the development of the National Incident Management System (NIMS), which is based on the fire service's incident command system. It is important for multiple agencies to plan and exercise together before an incident, so that they can function effectively during the early moments of the incident response. The need for effective NIMS implementation increases if there is a coordinated attack like the one in Paris which took place in multiple locations. Overall, NIMS implementation has been effective, due to the requirement that federal grantees certify that they are NIMS-compliant. However, we have witnessed cases, exemplified by the response to the Ebola outbreak in 2014, where some emergency support functions still were trying to adopt to the NIMS requirements.

It is important to realize that local fire and EMS departments probably will require assistance in responding to a large-scale terrorist incident, especially if the attack occurs outside of a major metropolitan area. Local fire and EMS departments rely on mutual aid agreements with surrounding jurisdictions to provide assistance during large-scale incidents. Mutual aid agreements provide automatic aid during times of need. They also help local fire and EMS departments to plan together ahead of time. Because they may be activated with regularity, mutual aid agreements also ensure that local fire and EMS departments are used to working together during a major terrorist incident. State and local mutual aid agreements also support

regionalization and regional response: not every fire department needs specialized hazardous materials or search and rescue response units if they have an agreement to use its neighbor's capabilities. The Emergency Management Assistance Compact provides a nationwide mutual aid agreement among the states to supply resources during a national emergency.

As the terrorist threat evolves, there also is a need for local first responders to engage in regional planning and exercises. As I discussed, a community can face a wide variety of threats and the local fire, EMS, and law enforcement community must be prepared to respond to major terrorist attacks and ISIS-inspired active shooter incidents. Each type of incident requires a different degree of response. Scenario-based planning and training, along with tabletop and full-scale exercises, help fire, EMS, and law enforcement to become familiar with the tactics needed to respond to the various types of incidents. For example, a mass casualty exercise in Paris on the morning of the November terrorist attack helped to expedite the response later that evening. Federal grant programs, such as the Urban Areas Security Initiative (UASI) and the State Homeland Security Grant Program (SHSGP), provide an important incentive for state and local stakeholders to plan, train, and conduct threat-based exercises together. As fire chief in Austin, I have found large-scale drills to be an effective use of federal funding.

One important area for improvement is communicating to the public about what can be done during a terrorist attack. Terrorists obviously are attempting to create fear and confusion. However, as the incident at the Boston Marathon proved, skilled bystanders are willing to assist during a major terrorist attack. Organizations, such as the Stop the Bleed campaign, support efforts to educate the public about how to provide vital first aid, such as hemorrhage control with the use of tourniquets, during a terrorist attack or active shooter event. Local fire and EMS departments can provide this training in their communities just as they provide CPR training. For example, we have a "Do Your Part" public education program in Austin that we can expand upon to promote public preparedness.

It is important to provide clear guidance on evacuation routes and whether or not to shelter in place during a terrorist incident. Clear and concise information from a trusted source, like the local fire chief, can prevent confusion. As local fire, EMS, law enforcement, and emergency management agencies are planning and conducting terrorism response exercises, they should develop pre-scripted directions and messages for the public.

An interoperable communications system is another vital component for an effective response to a terrorist incident. The Final Report of the National Commission on Terrorist Attacks Upon the United States identified the need for improved interoperable communications between first responders. This problem also was identified in the after-action reports of the Hurricane Katrina response and other incidents. Congress and the Administration have worked over the years to address this need.

The Middle Class Tax Relief and Job Creation Act of 2012 (P.L. 112-96) provided the necessary 20 MHz of spectrum in the 700 MHz band and $7 billion to build a nationwide broadband network dedicated to the mission requirements of public safety. This legislation also created the First Responder Network Authority (FirstNet), an independent authority within the National Telecommunications and Information Administration. FirstNet will develop and operate the new

broadband network, which is to be based on a single nationwide network architecture, thus enabling first responders to communicate with one another within and across jurisdictions. The FirstNet network will allow multiple agencies to be interoperable on-scene at an incident. It also should be more resilient than commercial networks and prevent the network being jammed by users during an emergency. In January, FirstNet achieved a major milestone by releasing a request for proposals to select a commercial nationwide partner to help it build and manage the network.

Currently, FirstNet is focused on building a network for data communications, such as streaming video of the incident to the incident commander. Public safety agencies still must depend on land mobile radio (LMR) in the short term. One of the provisions of P.L. 112-96 will create problems for public safety voice communications at the beginning of the next decade. The law requires first responder agencies to vacate their LMR systems in the T Band (470-512 MHz) by early 2023 with the Federal Communications Commission directed to auction this spectrum in 2021. Eleven major urban areas currently use this T Band spectrum, including Boston which used T Band systems for its interoperable communications during the response to the Boston Marathon bombing. It may cost $5.9 billion to migrate these jurisdictions' communications systems to another band, and at least five jurisdictions do not have excess spectrum to which to migrate. The IAFC urges Congress to address this issue before the end of the decade.

It is important that local fire and EMS departments have the training and specialized equipment they need to respond to the variety of terrorist threats facing their communities. Programs such as the SHSGP and UASI play an important role in helping communities pay for assets to be used in mass casualty or mass decontamination response. These grant programs also can be used to purchase advanced chemical detectors and equipment needed to respond to a bioterrorism attack. In many cases, state and local grantees have used the approximately $40 billion in federal grants to purchase the capabilities that they need, and these funds are now being used to sustain these capabilities. Federal grant funds also are used to staff and maintain local fusion centers. It also is important to recognize that federal funding acts as an important incentive in regional planning, training and exercises by bringing together all of the federal, state and local stakeholders together. The IAFC supports the concept of developing a database of state and local projects funded by SHSGP and UASI grants, so that other jurisdictions can learn how federal funds have been used. This database could allow for the better use of taxpayer funds by preventing grantees from "re-inventing the wheel" when developing capabilities.

The IAFC also supports current efforts in Congress to improve the preparedness for potential acts of bioterrorism. In December, this committee marked up the First Responder Anthrax Preparedness Act (S. 1915), which would set up a voluntary anthrax vaccine program at the Department of Homeland Security. On February 2, 2015, the House passed the Medical Preparedness Allowable Use Act, which would allow grantees to use SHSGP and UASI funding to establish programs that place kits of medical countermeasures with first responders and their families. The IAFC supports both of these bills as necessary to improving local first responder preparedness for bioterrorism attacks. We urge the Senate to pass this legislation this year.

Conclusion

I thank the committee for the opportunity to represent the fire and emergency service at today's hearing. The terrorist threat has evolved since 9/11 and local first responders now must be prepared for a variety of incidents. It will take a whole community effort to be prepared for these threats, which requires the active participation of all federal, state, local, and private sector stakeholders, including the American public. The federal government provides a number of opportunities for local first responders to receive the information, training, communications, planning, equipment and coordination that are required for an effective emergency response. It is important to recognize the essential role that this committee has played in improving our nation's preparedness. I look forward to working with you to ensure that local fire and EMS departments are ready to protect their communities.

Testimony of Edward F. Davis, III CEO of Edward Davis, LLC and Former Boston Police Commissioner before the United States Senate Committee on Homeland Security and Governmental Affairs

February 2, 2016

Chairman Johnson, Ranking Member Carper, distinguished members of the Committee, thank you for inviting me to participate in the "Frontline Response to Terrorism in America" hearing. This is a critically important topic that touches every one of us and is in the forefront of the daily news across the country and throughout the world. It may be an active shooter incident in a conference room that devastated a community in San Bernardino or IEDs at the Boston Marathon finish line that destroyed the lives of many of my fellow Bostonians. The terrorists who commit these heinous crimes are radicalized here and abroad, but their theme and their intent is the same – chaos and destruction of civilian populations, offering no quarter to women or children. We must stop it and we must do so in an urgent and coordinated fashion.

In 2014 I testified before this Committee on what worked and what did not work during the Boston Marathon bombing response. At that time I recognized the deceased. Again today, I shall do the same: 8 year old Martin Richard, Krystle Campbell, Lingzi Lu and MIT Police Officer Sean Collier. I also recognize every other victim in the US and those abroad whose lives have been senselessly taken by terrorists. We can never forget them.

Progress has been made since we dealt with the Boston tragedy. We are seeing improvements in quality of intelligence, coordination of agencies, sharing of information, training and equipment. Game-changing technologies are being developed at a rapid rate and first responders (including the medical community) are receiving life-saving training and equipment, like the tourniquets issued to all Boston Police.

Recent terrorist attacks in San Bernardino, Chattanooga and Garland demand a common sense and coordinated response.

Community Policing plays a very important role in the prevention of these incidents. My former colleagues have long recognized the effectiveness of community policing and are laser focused on building community relationships, transparency and accountability. The community in every city and town across the US has the capacity to play a central role in preventing terrorist attacks. If this is going to happen, they need to trust the police. Information also needs to be shared with the community. Citizens can, if properly informed, provide early information on radicalization in their midst. Citizens need to understand what to look for and call the police when they see something that doesn't look right. This becomes most effective when reaching out to community members that are sometimes in the shadows: those that don't attend community meetings, or religious services and those activist groups that never sit down with law enforcement officials. We all need to move beyond our comfort zone if we really want change. Community Policing efforts need to be continuously and properly funded, trained up and they should be audited.

Intelligence gathering and sharing is another critical prevention tool utilized by federal, state and local agencies to fight terrorism. Fusion centers across the country provide crucial information every day in real time to multiple agencies and forward redacted information to the private

sector. Their value for prevention and crisis response management has been proven time and time again. Fusion centers should continue to meet annually to discuss issues, needs, concerns, and trends: what is working and what is not. Funding needs to be increased in order to attract talented analysts and grow properly managed and effective fusion centers that coordinate intelligence from all levels of government.

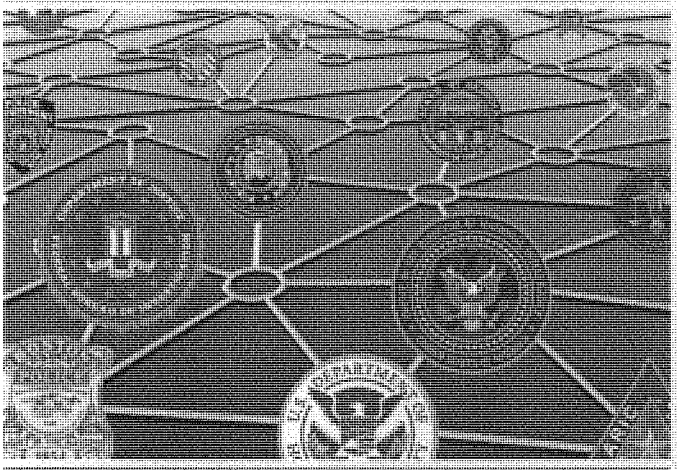
Since 2013, intelligence sharing among agencies continues to improve. Impediments have been removed. Federal, state and local law enforcement need to continue working together as equal members of Joint Terrorism task forces across the country and in Fusion Centers, with unrestricted access to information that could identify terrorists in their early stages and prevent catastrophic events. Separate systems are ripe for dysfunction. Any deterrent to this seamless coordination needs to be extinguished.

Social media is a proven, effective tool to communicate with and provide information to residents, business owners and visitors during a major emergency. The regular use of Twitter, Facebook and other social media outlets should be utilized by any agency that would benefit from community contact and used for notifications and information. But social media does more than notify, it begins a dialogue that helps understanding on all sides. This was proven during the Boston Marathon bombings when photographs, video and other tips were received via crowd sourcing; and information such as road closings, transportation status and correcting misinformation were all done via social media.

Community policing, intelligence gathering and sharing alone cannot prevent terrorism. Training is an essential component for prevention and response. Prior to the Marathon bombings the US Department of Justice, and the Department of Homeland Security through UASI and other funding programs provided opportunities for law enforcement to receive terrorism prevention and response training. This funding allowed cities and towns to train with other law enforcement partners and in the case of Boston, with the Boston medical community during a Mumbai style scenario and table top exercise. The building of these relationships and practicing emergency response together identified some gaps, solidified practices and saved countless lives at the Marathon. The provision of active shooter response technical assistance and other terrorist prevention assistance through DHS legislation is an important step in furthering prevention and saving lives during an actual incident. I strongly encourage this funding to continue.

Consistent funding for high quality equipment is necessary for responders during a major incident. This could range from armored vehicles to the critical need for tourniquets in every responding vehicle. Law enforcement needs the tools to safely take immediate action, contain the situation and assist those in need.

In closing, what I learned in my role during the terrorist attack in Boston is that there is no panacea. The reality is that such a challenge requires informed and trusting community members who are not afraid to speak, coordinated intelligence gathering and sharing among all equal partners who strive to prevent, highly trained and well equipped law enforcement fire and EMS to respond in unison and all of you, to continue to legislatively and financially support these efforts.



Domestic Security:

Confronting a Changing Threat to Ensure Public Safety and Civil Liberties

Executives
National Security

BENS Practitioners Panel

Michael Allen
Former Majority Staff Director House Permanent Select Committee on Intelligence United States House of Representatives

Alfred Berkeley
Vice Chair National Infrastructure Advisory Council
Former President NASDAQ Stock Market, Inc.

Michael Chertoff (Vice Chair)
Former Secretary of Homeland Security

Commissioner Edward Davis
Former Commissioner, Boston Police Department

Robert Graham (Vice Chair)
Former Governor of Florida
Former Chairman Senate Select Committee on Intelligence United States Senate

David Hall
Director Missouri Information and Analysis Center

Lee Hamilton
Former United States Representative (IN)
Vice Chair The National Commission on Terrorist Attacks Upon the United States

Michael Hayden
Former Director CIA
Former Director NSA

Brian Michael Jenkins
Senior Advisor to the President RAND Corporation

Loch K. Johnson
Regents Professor of Political Science University of Georgia

Thomas Kean
Chair, The National Commission on Terrorist Attacks Upon the United States
Former Governor of New Jersey

Michael Leiter
Former Director of the National Counterterrorism Center

Joseph Lieberman
Former United States Senator (CT)
Former Chairman Homeland Security and Government Affairs Committee United States Senate

James Locher
Former Assistant Secretary of Defense for Special Operations and Low Intensity Conflict

Steven McCraw (Vice Chair)
Director, Texas Department of Public Safety
Homeland Security Advisor to the Governor of Texas

Norton Schwartz (Chair)
President & CEO Business Executives for National Security

Maurice Sonnenberg
Former Member President's Intelligence Advisory Board
Vice Chair Report of the National Commission on Terrorism

Frances Townsend
Former Assistant to the President for Homeland Security and Counterterrorism

Juan Zarate
Former Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism

BENS Member Task Force

Stephen Shapiro
Task Force Chair
Managing Partner of BSR Investments

Thomas Barron
Task Force Member
Chief Operating Officer (Ret.) The Episcopal Church Pension Group

Jonathan Lewis
Task Force Member
Managing Principal
Chief Investment Officer
Samson Capital Advisors LLC

Alan Silberstein
Task Force Member
Former CEO Western Union

Business Executives for National Security (BENS) is a non-profit, non-partisan organization that for over 30 years has served as the primary channel through which senior executives can help build a more secure America. Leveraging the collective expertise of its national membership, BENS applies best business practices to public sector challenges in order to help strengthen the nation's security and improve the performance of government agencies.

Contents

EXECUTIVE SUMMARY

Domestic Security: Confronting a Changing Threat to Ensure Public Safety and Civil Liberties

The terrorist threat to the United States has not abated. Instead, it is fundamentally different than it was on September 11, 2001: greater numbers; more sophisticated communications strategies, including through the use of technology; decentralized leadership and geographic dispersal; homegrown radicalization; and returning foreign fighters.

As the terrorist threat to the United States continues to evolve and adapt, so too must our domestic counterterrorism efforts. An effective domestic counterterrorism strategy that can enhance public safety requires a stronger linkage with state and local law enforcement and clear federal leadership. The efforts conducted pursuant to this strategy cannot violate our society's expectations for personal privacy and must be conducted within constitutional standards, complementing and reinforcing our civil liberties.

The changing nature of the terrorist threat puts ever-greater emphasis on the need for the domestic counterterrorism posture to be as agile and as effective as possible. It places heightened importance on the ability of federal, state, and local governments to acquire, process, and share high-value information rapidly and securely, using common standards and procedures. Although it is unrealistic to expect that every attack can be prevented, it is vital to improve the preparedness of our domestic counterterrorism enterprise, including the private sector, to better ensure domestic security and resiliency in the face of these evolving and persistent terrorist threats.

Business Executives for National Security (BENS) undertook a project to assess whether the many reforms enacted after the September 11, 2001 terror attacks are still effective at confronting a changing terrorist threat. This report considers the extent to which information sharing between federal, state, and local agencies is efficient and responsive; organizational missions are clearly defined; federal leadership is effective at articulating national domestic counterterrorism priorities and supporting state and local efforts; and workforce initiatives at the federal, state, and local levels are effective at maintaining a cadre of skilled intelligence analysts. While this report primarily examines U.S. domestic counterterrorism systems and processes, it does explore broader issues associated with domestic intelligence efforts in connection with other domestic national security threats.

To address these objectives, a Member Task Force composed of four New York based BENS members conducted a dedicated primary research effort. Over a period of three years, the Task Force met with over 100 senior and knowledgeable people in the intelligence community, its overseers, managers, and consumers, including visits to fusion centers in six states and meeting with a number of state and local law enforcement agencies. Among the federal agencies, the Task Force met with senior leaders in the Office of the Director of National Intelligence (ODNI), the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the National Counterterrorism Center (NCTC), the National Security Council staff, and the profes-

sional staff of the Intelligence and Homeland Security oversight committees in both houses of Congress. This effort was complemented by a review of the relevant literature, including the after action reviews of the 2009 Fort Hood and 2013 Boston Marathon attacks.

From this effort, the Task Force discovered broad agreement that improvements in the domestic security structures and processes are needed. Drawing upon its knowledge and understanding, the Task Force produced an initial summary of its findings and potential recommendations. BENS then convened a 20-person Practitioners Panel which reviewed the Task Force's findings and recommendations and identified the most salient and immediately-actionable recommendations. The Panel was comprised of current and former high-level officials from the state, local, and federal levels, as well as noted subject matter experts. BENS next reviewed those identified recommendations with major stakeholders to solicit their input and ideas, including with relevant Congressional Committee staffs, and senior leaders at DHS, FBI, and ODNI. The recommendations in this report are the result of those reviews.

We offer one caveat: none of the involved agencies are maintaining the status quo. Change and progress has occurred since our research and the report's preparation concluded. While the details may have changed, however, the central themes of our recommendations remain valid.

What BENS Found Overall:

There is widespread agreement that our domestic security apparatus must be improved. Our law enforcement and intelligence agencies are operating without an enterprise-wide concept at the federal level. This shortcoming impedes the federal government's ability to optimally conduct domestic intelligence activities in support of counterterrorism and related missions and to provide effective oversight of these activities. It also hinders its ability to fully support and use the 800,000 law enforcement officers at the state and local levels in the national effort.

What BENS Recommends:

The ensuing recommendations represent those actions that the Practitioners Panel believed offer the most immediate path for substantive improvement to the United States' domestic counterterrorism posture, while also enhancing civil liberties protections. They include:

- **Establishing integrated fusion centers** located in the highest-threat areas by enhancing analytic capability and collocating selected federal intelligence components – such as from the FBI Joint Terrorism Task Forces (JTTFs), Field Intelligence Groups (FIGs), National Mission Cells, and other relevant federal national security intelligence entities – with state and local law enforcement.
- **Increasing the mutual awareness of state and local law enforcement** and FBI Joint Terrorism Task Forces by creating mechanisms to ensure that information about current counterterrorism investigations is shared with state and local partners in real-time, and that closed case information is likewise provided to state, local, tribal, and territorial (SLTT) assets so that they can determine whether to pursue independent investigations;
- **Enhancing intelligence analyst capabilities and interoperability** through the development and application of high-quality, standardized training for intelligence personnel at all levels of government and the application of Goldwater-Nichols style

joint duty and joint training protocols;

- **Encouraging the service and retention of high-quality analysts** through career path enhancement and incentives;
- **Bringing greater federal focus on domestic intelligence structures and processes** by assigning a Deputy-level officer at the Office of the Director of National Intelligence to manage the programmatic aspects of the federal domestic intelligence effort, and enhancing the use of the Domestic DNI Representatives to bring strategic coordination to the myriad federal agencies operating in the field;
- **Establishing a domestic threat framework** through an annual, interagency process to assess and prioritize domestic threats and intelligence needs;
- **Enabling better coordination and management of federal intelligence efforts** by including within the definition of the Intelligence Community (IC) those federal entities that undertake domestic intelligence activities but are not now included as members of the IC; thereby enhancing strategic planning and budgeting, and affording intelligence-based oversight of their activities;
- **Strengthening the intelligence culture at the FBI** by (i) creating a reporting relationship, as determined by the FBI Director, for the Executive Assistant Director (EAD) of the Intelligence Branch to the Office of the Director of National Intelligence with respect to intelligence priorities and community management (while preserving its direct reporting relationship to the FBI Director for operational matters); and (ii) enhancing internal recruitment, training and talent management programs for its intelligence analysts;
- **Enhancing the capabilities of DHS' Office of Intelligence & Analysis** by focusing its attention on those missions unique to it, such as critical infrastructure protection; border and transportation security; aggregation of intelligence information from DHS subcomponent agencies (such as Customs and Border Patrol); and providing leadership and assistance to the integrated fusion centers and the remainder of the fusion center network, especially programs for countering violent extremism; and
- **Improving Congress' ability to provide oversight of domestic intelligence activities** by having all domestic intelligence activities authorized and overseen by the Intelligence Committees, and by creating an Intelligence Appropriations Subcommittee in each chamber to appropriate funds to support those activities.

These recommendations do not represent an endpoint for change nor are they a finite solution to confronting the terrorist threats to the homeland. Change must be a constant effort. As the terrorist threats continue to change and adapt, so too must our domestic counterterrorism structures. Failure to adapt will leave the United States vulnerable to terrorist threats that are increasingly difficult for our current structures and processes to manage. If enacted however, the recommendations will move the needle toward increasing the operational efficiency of our domestic counterterrorism enterprise, with proper attention to constitutional protections, at a time when federal, state, and local public safety officials are increasingly aware of the evolving threat and a new Congress provides an opportunity to legislate accordingly.

The Case for Change

Why Now

In In the nearly fourteen years since al-Qaida attacked the United States on September 11, 2001, it has been degraded, its senior leadership scattered, and its capacity to orchestrate another major attack on the homeland reduced. Yet, the terrorist threat to the United States has not abated. Rather, it has evolved, becoming more diffuse and decentralized but no less determined to attack the American homeland or our interests.

Moreover, the United States faces a growing threat from homegrown violent extremists and self-inspired radicals as technology makes it easier for al-Qaida and other extremist groups to spread their virulent ideology. The 2009 Ft. Hood shooting and 2013 Boston Marathon bombing illustrate the threat from self-inspired radicals. The Islamic State's (IS) adroit use of social media to inspire and recruit Western European and American sympathizers illustrates the challenge for the United States, as do the 18,000 fighters trained and battle-hardened in the Syrian and IS conflicts,[1] 3,000 of whom are estimated to hold Western passports and are now returning to their home countries.

The fragmented threat environment created by individuals and organizations with transient affiliations poses a unique challenge to American domestic counterterrorism efforts. Indeed, in 2014 Director of National Intelligence James Clapper identified the "diversification of terrorism ... loosely connected and globally dispersed ... as exemplified by the Boston Marathon bombing and by the sectarian war in Syria," as a potential threat to the homeland.[2]

Of particular concern to law enforcement and intelligence officials are homegrown violent extremists (HVEs) and self-inspired radicals with little or no organizational support. In 2013 former National Counterterrorism Center (NCTC) Director Matthew Olsen stated that "Homegrown Violent Extremists... remain the most likely global jihadist threat to the Homeland."[3] Director Olsen characterized the scale of this threat as "a handful of uncoordinated and unsophisticated plots."[4] Similarly, FBI Director James Comey has asserted that "These individuals present unique challenges because they do not share the profile of an identifiable group. Their experience and motives are often distinct, but they are increasingly savvy and willing to act alone."[5]

The 2009 Fort Hood shooting and 2013 Boston Marathon bombing, however, demonstrated that smaller scale terrorist attacks can still disrupt our daily lives. The 2014 shooting in Ottawa, Canada, and recent 2015 attack in Paris, France by individuals purported to harbor extremist sympathies are further evidence that threat from the homegrown or small-scale terror attacks is persistent. Although smaller in scale the potential threat vectors of these challenges are proliferating as jihadist propaganda continues to implore individual action, and as Western passport holders' flock to the Syrian front. While it is unrealistic to ask our law enforcement and intelligence officials to interdict every potential attack, it is clear these smaller scale threats must be more efficiently and effectively managed.

As these threats continue to adapt so too must our Nation's domestic counterterrorism efforts. Specifically, our ability to manage a durable and dynamic terrorist threat must be improved, as must our capacity to identify emerging threat patterns and prepare actions against them. Terrorism is a long-term challenge, and it requires a long-term commitment to address it.

The changing nature of the terrorist threat now puts ever-greater emphasis on the need for the domestic counterterrorism posture to be as organized, as nimble and as effective as possible, with continued attention to the protection of civil liberties. Further, it places heightened importance on the ability of federal, state, and local governments to acquire, process, and share high-value information rapidly and securely, using common standards and procedures.

Although the post-9/11 reforms to our intelligence and homeland security structures were significant, and many improvements have ensued, the United States still lacks a cohesive domestic counterterrorism strategy with the capacity for coordinated execution at all levels of government. With no clear federal leader orchestrating U.S. domestic intelligence efforts, state and local law enforcement entities remain underemployed assets and federal efforts remain disparate. These deficiencies reduce our national capacity to effectively identify and manage terrorist threats.

U.S. domestic counterterrorism efforts must be part of a broader domestic intelligence capability that can confront a full spectrum of domestic threats within transparent legal boundaries and with proper respect to civil liberties. Protecting civil liberties is an essential component of our national value system, and ensuring such protections is essential to maintaining public support for the Nation's domestic security efforts. As such, although this report primarily examines domestic counterterrorism structures and processes, it does discuss broader issues associated with national domestic intelligence efforts in connection with other threats, including those that cut across neat bureaucratic definitions. None of the recommendations presented are threat-specific, and if implemented they will all increase our national ability to remain agile in confronting the diverse array of domestic threats.

A Business Perspective on Counterterrorism

Applying common-sense, business-style analysis to complex problems of national security is what Business Executives for National Security (BENS) does. BENS undertook this study to assess whether the myriad reforms made to the U.S. intelligence and homeland security structures after the September 11, 2001 terror attacks are still effective at confronting a changing terrorist threat. Adopting a business perspective and applying private sector best practices, BENS sought to identify ways to improve the operational efficiency of U.S. domestic security structures and processes and make the operation coherent in all of its dimensions.

The private sector clearly has a stake in these issues. For example, 85% of U.S. critical infrastructure is privately owned.[6] These and other privately owned assets are often the primary targets of terrorist attacks. The private sector also plays an active role in keeping the United States secure and resilient. After the 2013 Boston Marathon bombing, video footage provided by local business owners was key in helping authorities identify the suspects.

This report considers the extent to which information sharing between federal, state, and local agencies is efficient, responsive, and preserving of individual liberties; organizational missions are clearly defined; federal leadership is effective at articulating domestic security priorities and supporting state and local efforts; and workforce initiatives at the federal, state, and local levels are effective at maintaining a cadre of skilled intelligence analysts. In undertaking this study BENS examined both U.S. domestic counterterrorism structures and processes as well as broader issues associated with domestic intelligence efforts.

BENS would like to thank all of those individuals who met with our Member Task Force, offered their insight and counsel throughout the course of this project, and helped to edit and enhance this report. This product and our study could not have been completed without numerous individuals in government, the private sector, and nonprofit organizations who dedicated their time and leadership to reviewing, informing, and enriching our project. This includes individuals from the Department of Homeland Security, Federal Bureau of Investigation, Department of Justice, the White House, Office of the Director of National Intelligence, and numerous state and local law enforcement and public safety officials. All of these individuals were extremely forward thinking, gracious with their time, and demonstrated the utmost leadership and dedication to keeping our nation safe. To all of you, we say: Thank You.

What BENS Recommends

Supporting State and Local Efforts: Creating Best Practice Integrated Fusion Centers through Scale, Collocation and Enhanced Information Sharing

What BENS Found

State and local law enforcement officers—numbering nearly 800,000 nationwide—are integral to U.S. domestic security efforts, including counterterrorism (CT). Much of these officials' domestic security functions are carried out through a network of 78 state and urban area fusion centers, which "serve as local points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners."[7] As the National Network of Fusion Centers has observed, "No one in government knows more than state and local officials know about what is normal or abnormal in their cities and towns."[8]

BENS' research, however, found that state and local law enforcement officers are an underused asset in national CT efforts. Through extensive on-the-ground research, BENS noted that the relative analytic performance of fusion centers varies greatly throughout the national network, owing, in part, to a lack of governance standards for domestic security efforts, an absence of sufficient skilled analysts and unfocused and inconsistent federal efforts and funding. Further, very few centers are collocated with federal entities, such as FBI Joint Terrorism Task Forces (JTTFs), FBI Field Intelligence Groups (FIGs) and National Mission Cells, or Drug Enforcement Agency (DEA) components, and the exchange of information to and from federal entities occurs through multiple and overlapping delivery channels. This results, at times, in uncoordinated or untimely information delivery.

Overall, BENS observed that the highest-performing centers are those that have a staff of highly trained analysts, are collocated with appropriate federal agencies—which fosters strong interagency relationships—and have a regional or multijurisdictional mission.

Recommendation 1

1) In high-threat, metro urban-areas, those federal domestic intelligence entities most relevant to their specific threat matrixes[9] should collocate to the extent possible with state fusion centers, creating better-staffed and trained, federally-assisted "integrated fusion centers."

2) Participation by selected and coordinated federal entities within these state integrated fusion centers would provide support to efforts of state and local law enforcement by capitalizing on the reengineering opportunity to create the highest value intelligence services

to customers, maximizing speed and flexibility of responses to the evolving terrorist and other national security threats, and optimizing productivity and efficiency. Existing scaled fusion centers in Los Angeles, Austin, and Atlanta serve as "good practice" prototypes from which to design and implement "best practice" integrated fusion centers.[10]

3) Ownership and management of the integrated fusion centers will continue to be by state and local stakeholders, with the federal entities operating in support and collaborating through their counterterrorism and other domestic security efforts. The federal government should concentrate intelligence appropriations in the integrated fusion centers, while continuing the FEMA grants for training and resilience to the remaining state fusion centers.

4) Given the number of state fusion centers, the proposed integrated fusion centers would improve domestic counterterrorism and countering violent extremism (CVE) performance, and public safety, by:

   a. Achieving 'scale' of intelligence analyst capability through their size and the availability and concentration of resources to provide high-value, counterterrorism support to both local and federal agencies;

   b. Capitalizing on major opportunities for cost savings by reengineering processes, reducing overhead and duplicative technology and supporting services;

   c. Providing the needed capacity to maintain a robust Terrorism Liaison Officer ("TLO") training program for all relevant public safety, fire, medical, and select private sector personnel within the integrated fusion centers' areas of responsibility;[11]

   d. Providing benefits not only to counterterrorism and CVE, but also to other aspects of the domestic national security mission (e.g., countering international criminal cartels, human and drug trafficking, as well as threats that cut across categories) through improved coordination of efforts in the field; and

   e. Continuing to drive best practices as models for the other state fusion centers within the broader national network.

5) To clarify and simplify channels of counterterrorism communication amongst the many involved entities, the new integrated fusion centers would function as a primary point of contact for federal, state, and local law enforcement, as well as private sector partners, to receive, analyze, and disseminate domestic counterterrorism and other domestic security information.

   a. The integrated fusion centers would direct upward delivery of information to the FBI at the national level with respect to counterterrorism and related information; to Department of Homeland Security (DHS) Office of Intelligence & Analysis (I&A) with respect to information related to its missions, such as critical infrastructure protection and border and transportation security; to DEA with respect to combatting drug-related crimes. In all cases, this information should continue to be available to the National Counterterrorism Center (NCTC) as the epicenter of the federal government's counterterrorism information aggregation efforts.

   b. Information flows from federal domestic intelligence agencies would be disseminated to state and local law enforcement and public safety officials, as well as to the pri-

vate sector, through the integrated fusion centers, as such SLTT entities would already be located or readily accessible there.

6) Integrated fusion centers will help bolster privacy and constitutional protections by incorporating well-trained federal entities and standardized performance metrics that are consistent with monitored civil liberties guidelines established by the Attorney General, and greater resources.

Actions Required:

1. Gain agreement by the heads of the relevant state and local public safety entities and their governors:
   a. To create a number of threat-determined, state-run, integrated fusion centers that would include appropriate elements of federal, state, and local intelligence entities; and
   b. That the Office of the Director of National Intelligence (ODNI), in consultation with, amongst others, the National Fusion Center Association (NFCA), DHS I&A and the FBI, would be responsible for determining standards and performance metrics for the national security intelligence-related efforts of those integrated fusian centers.
2. Direction by the Director of the FBI, Secretary of Homeland Security, and the Attorney General to locate their relevant component agencies (or portions of them) within these integrated fusion centers.
3. Determination by the Congress to direct necessary intelligence appropriations to the integrated fusion centers while continuing the FEMA grants to the other state fusion centers.

Supporting State and Local Efforts through Investigatory Awareness: Real-Time Collaboration between Federal Agencies and State and Local Partners

What BENS Found

BENS' research revealed that the efficient sharing of investigative information is often hampered by a lack of information systems integration, restricted SLTT access to classified or sensitive federal systems—even though those SLTT personnel may be properly cleared—or even geographical distance. Further, there is often little feedback from federal entities, such as FBI JTTFs, on information forwarded to them by state and local officials, such as law enforcement officers or fusion centers. Consequently, SLTT officials often do not know whether the information they provide is valuable to their federal counterparts, or if it is not, how to improve upon their performance.

As a result, state and local law enforcement officers may not be aware of federal CT investigations, or other domestic security matters, that affect their jurisdiction. The circumstances surrounding the FBI's investigation of one of the alleged Boston Marathon bombers are illustrative of this finding. The Boston JTTF did not notify state or local law enforcement personnel who were not part of the JTTF of their investigation into Tamerlan Tsarnaev; although it is unknown whether doing so would have prevented the attack.[1]

Recommendation 2

1) JTTFs, FBI's operational counterterrorism units, should be directed by the Bureau to:

   a. Notify in real time their state and local partners of the status of current terrorism cases within the jurisdiction of those partners; and

   b. Create investigative review groups within their jurisdictions with key state and local leadership, pursuant to guidance and review by the Department of Justice. These groups will explicitly discuss all JTTF cases and – in accordance with civil liberties protections guidelines – pass to state and local leadership information on closed investigations to permit local officials to continue investigations consistent with their authorities, independent of federal involvement.

2) This same information flow should include feedback to the SLTT partners as to the quality and utility of the information provided so that they can gain insight and thereby improve performance.

3) FBI and DHS should encourage access to classified counterterrorism information systems by appropriate security-cleared state and local personnel without the need for on-site presence of FBI or DHS personnel.

Sustained two-way communication between the federal, state, and local levels would allow for greater utilization of state and local investigators, as well as sharing the workload for FBI JTTFs and FIGs across the country. Most importantly, it would also permit state and local forces to bring their unique local knowledge and perspective to bear on CT efforts. The integrated fusion center model will also aid in this information flow.

Actions Required:

1. The Director of the FBI should issue a Directive creating a standard operating procedure to ensure FBI implementation of the above recommendations in conjunction with state and local entities, such as fusion centers and police departments.

2. Amend the Memoranda of Understanding governing information sharing between the FBI and SLTT to the extent they do not reflect this process.

Domestic Counterterrorism and Countering Violent Extremism: Enhancing Training and Interoperability at All Levels

What BENS Found

Analyst training is the essential foundation of intelligence success at all levels of government. There are inconsistent training and experience requirements across domestic security agencies, particularly between those at the federal, state, and local levels. For example, a report by the Government Accountability Office (GAO) noted that "[DHS] I&A's training program did not always focus on mission-specific requirements that its workforce needed . . ."[1]

BENS' research revealed that a lack of resources often prohibits state and local officials at fusion centers from sending their analysts to receive advanced training. This results in fusion center analysts with uneven levels of expertise and experience. A lack of common or interoperable systems and procedures between federal, state, and local agencies was also cited by SLTT officials as an area of genuine concern. There are also cultural barriers and organizational parochialisms that may inhibit interagency collaboration. Different levels of authority, varying or sometimes competing goals, distinct standard operating procedures, and unique organizational values can all contribute to an agency or individual forming perceptions—or perhaps misperceptions—about a peer that ultimately inhibit closer cooperation. Indeed, in the course of BENS' research "cultural" differences were often cited as reasons for a lack of collaboration found both within and between agencies.

The Terrorism Liaison Officer (TLO) program is a good way for fusion centers to maintain a direct connection with their community. Through this program, state and urban fusion centers train law enforcement officers, public safety officials, and private citizens on issues and behavior that may be indicative of potential terrorist activity. Some fusion centers, however, often face challenges maintaining a robust TLO program because of resource constraints.

Recommendation 3

1) With the guidance of the ODNI, in consultation with DHS I&A, and pursuant to guidelines established by the Attorney General, the FBI should determine and apply standardized training for all federal domestic counterterrorism analysts and make such training broadly available. Such training will produce higher-quality analysts focused on national domestic security missions, and will have the added benefit of creating a uniform standard for the protection of civil liberties.

2) DHS should:
   a. Continue to promote and make sustainable the Terrorist Liaison Office (TLO) Program and priority CVE programs.
   b. Promote interoperability amongst SLTT and federal partners in the domestic security mission to encourage greater effectiveness and efficiency at all levels. Reliable federal assistance is required to ensure the long-term sustainability of this capability.
3) The ODNI should place greater emphasis on the Intelligence Community Civilian Joint Duty Program using the Goldwater-Nichols model to increase the "jointness" between the federal, state, and local levels as well as among federal agencies. The ODNI should also consider expanding the Program to include non-IC organizations such as Customs and Border Protection and Immigration and Customs Enforcement, as they also participate in the domestic security mission.[14] Such jointness, both in training and in field operations, will promote effective interaction amongst intelligence entities and even between levels of government. Further, it will infuse the system with the values of constitutional protections that have been a feature of American law enforcement.

Actions Required:

1. The ODNI, in consultation with the FBI and DHS and pursuant to civil liberty protections established by the Attorney General, should develop and apply analytic standards, training protocols, and common systems and vernacular to underwrite standardized training for all federal domestic counterterrorism analysts. Such training should available to all appropriate state and local law enforcement officers. Federal assistance for SLTT participation in such training programs will most likely be required. In the field, such training should be implemented by DHS I&A.
2. The ODNI should pursue robust Goldwater-Nichols style joint training programs and standards (including with SLTT partners as practical), as well as human resource practices to ensure joint duty assignments are viewed as essential to intelligence career path enhancement.
3. DHS should continue its efforts to promote and enhance analyst training and the TLO Program, as well as advance CVE programs.

Domestic Counterterrorism and Countering Violent Extremism: Enhancing Career Paths

What BENS Found

Appropriate career paths, compensation, and incentive structures for domestic intelligence analysts are critical components to the development of a skilled cadre of professionals and a mature intelligence culture. As currently structured, however, these elements are not optimized for recruiting and retaining the needed cadre of skilled intelligence analysts.

A 2014 report by the 9/11 Commissioners urged that "[a] sustained focus on recruiting high-quality candidates for the [FBI's] analytic workforce is essential if ... progress is to continue. We hope to see a clear career path for analysts to be promoted and to serve in executive-level leadership positions in the FBI."[1] Even among non-law enforcement organizations there have been personnel management challenges. In a 2014 study the GAO concluded that DHS's Office of Intelligence and Analysis "has faced human capital challenges in recruiting and hiring the skilled workforce it needs and providing training and professional development opportunities that keep morale high and attrition low."[2]

Recommendation 4

1) Federal, state, and local agencies—particularly operational elements of the FBI, DHS, and state fusion centers—should continue to enhance the career path of and incentive systems for intelligence analysts to ensure the career path is desirable and retention is maximized.

2) This effort should include providing additional opportunities for intelligence analysts to assume substantive leadership roles within operational divisions at fusion centers, and, with respect to federal agencies, at headquarters and among appropriate field offices.

Action Required:

The Director of the FBI, the Secretary of Homeland Security, and the leadership of other relevant federal, state, and local agencies with intelligence components should continue to develop and implement personnel and talent management policies that enhance the career paths and retention of domestic intelligence analysts.

Federal Leadership & Management: Office of the Director of National Intelligence

What BENS Found

National leadership of the domestic intelligence posture is necessary to continuously adjust the response to a changing threat landscape, and to articulate an overall strategy to confront these threats. Since the September 11th terror attacks, the United States has created new domestic security structures, and, yet, there remains no central strategic leader or unified domestic security strategy at the federal level.

The ODNI was created in 2004 to "serve as the head of the intelligence community"[1] and is the only entity with the authority to oversee and manage the entire intelligence landscape. This authority applies to foreign intelligence as well as domestic, including domestic counterterrorism efforts. In 2012 the ODNI institutionalized a Domestic DNI Representative program, wherein 12 senior FBI officials across the nation were nominated to serve as the DNI's representatives and to help coordinate the federal intelligence efforts in their region.

Despite these very promising efforts, many federal, state, and local officials with whom BENS met agreed that strategic management of U.S. domestic intelligence efforts could be improved. Coordinated federal efforts also enable the U.S. government to provide effective support to its SLTT partners.

Because no other agency has the ODNI's managerial authority across the intelligence community, only ODNI can fulfill this leadership role. In 2011 the Bipartisan Policy Center's Tenth Anniversary Report Card concluded: "It still is not clear ... that the DNI is the driving force for intelligence community integration that we had envisioned."[2] BENS believes the absence of a designated domestic IC lead needs to be addressed.

Recommendation 5

1) The Director of National Intelligence should appoint a Deputy-level officer to lead the federal domestic intelligence effort. This position would have specific responsibility for:

   a. Managing and coordinating the programmatic (not operational) aspects of federal domestic intelligence collection;

   b. Directing the annual domestic threat assessment discussed below;

   c. Determining the resulting collection priorities, budgeting, and resource allocation required to support those priorities;

   d. Overseeing intelligence analysis and dissemination;

   e. Establishing – in consultation with the National Fusion Center Association –a uniform set of performance metrics and governance and interoperability standards for

the newly-formed integrated fusion centers to ensure these entities effectively support state and local law enforcement and associated intelligence elements in their efforts to fulfill the domestic security mission; and

f. Emphasizing the protection of civil liberties in all related matters.

This position requires an extensive background in domestic intelligence and/or law enforcement and should be authorized in statute. The Director of the NCTC or the Executive Assistant Director of the Intelligence Branch at FBI could logically assume this position, although a senior SLTT official with prior federal experience might also be appropriate. Additionally, this Deputy should have a dedicated subordinate official responsible for overseeing legal, privacy, and civil liberties issues, given the inherent concerns associated with domestic intelligence information gathering.

2) The ODNI's Domestic Representatives should be selected from the agency most appropriate to the threat matrix in the Domestic Representative's area of responsibility to effectively coordinate and manage the federal domestic security intelligence efforts at the regional level. For example, they should be selected from the FBI when counterterrorism, counterintelligence, or weapons of mass destruction are considered the paramount threats; DEA when international drug cartels top the region's threat matrix; or DHS' Customs and Border Patrol when the threat is primarily border penetration.

3) These Domestic DNI Representatives would:

a. Coordinate the efforts of the federal agencies in the field to ensure rationalized and focused strategic effort on those threats which are primary to their area of responsibility, including facilitating lead agency actions and deconfliction;

b. Ensure the provision of necessary federal intelligence support to SLTT entities through the integrated fusion centers, as well as other state fusion centers and the federal entities participating in them; and

c. Continue to be collocated with NCTC's and DHS I&A's regional representatives to ensure maximum coordination of federal domestic security efforts, and, to the extent practical, be collocated all or in part with integrated fusion centers.

Action Required:

1. The Director of National Intelligence should appoint a Deputy-level officer with responsibility for leading the federal domestic intelligence effort.

2. Although not required for immediate implementation of this recommendation, because of its importance, this deputy position and its duties should later be codified by an amendment to the National Security Act.

3. The Director of National Intelligence should structure the Domestic Representative Program in accordance with the above recommendation.

Creating a Domestic Threat Framework

What BENS Found

Fourteen years after 9/11, as terrorist threats continue to change and multiply, there is still no annual, unified, interagency process that assesses and prioritizes U.S. domestic security threats and intelligence requirements, matches missions, and develops a budget to support them. In short, there is no unified domestic intelligence strategy or threat framework. Absent such a unified strategic vision, each federal agency conducts its own independent domestic threat prioritization, resulting in uncoordinated or duplicated efforts. For example, a 2014 GAO report found that the Department of Homeland Security's Intelligence Priorities Framework reflected "the existing intelligence activities of [DHS component agencies], rather than outlining strategic departmental intelligence priorities."[19]

Recommendation 6

1) One of the principal responsibilities of the new Deputy-level officer for domestic intelligence at ODNI must be to lead an annual interagency assessment of U.S. domestic security threats and intelligence needs. This assessment would form the basis for establishing information collection priorities, IC budget requirements, and a resource management strategy.

2) The annual domestic threat framework should be performed in conjunction with the Director of the NCTC, the Executive Assistant Director of the FBI's Intelligence Branch, and with input from the integrated fusion centers and other federal domestic intelligence agencies as appropriate. It should incorporate (i) the National Intelligence Manager for the Western Hemisphere and Homeland's current efforts to create a common, interagency threat criteria; and (ii) the FBI's Threat Review and Prioritization process.

Action Required:

The ODNI and other relevant authorities should issue a policy directive formalizing this annual interagency exercise, similar to other interagency threat assessments, such as the National Intelligence Priorities Framework. Congress may wish to codify these responsibilities.

Redefine the Intelligence Community to Ensure Unity of Effort and Oversight

What BENS Found

The array of domestic intelligence agencies do not reflect a cohesive enterprise structure. Rather, domestic intelligence efforts are performed by a diverse collection of committed law enforcement, intelligence, and homeland security agencies at all levels of government. The agencies range from the FBI to the U.S. Coast Guard, and the DEA to the Department of Energy. This patchwork crosses different jurisdictions, each with an agency or department head, or elected official, directing and defining public safety, law enforcement, and intelligence activities for their domain.

The ODNI oversees many of the activities and budgets of the entities included in the federal Intelligence Community, a group of 17 federal agencies focused both on foreign and domestic intelligence. Yet, the statutory definition of the IC omits a number of federal agencies and entities that nonetheless perform important domestic intelligence activities as well. This disadvantages the ODNI's overall breadth of management authority, making it very difficult for that office to provide the necessary coordination pursuant to a unified domestic strategy.

Recommendation 7

1) The Intelligence Community should formally include those domestic intelligence entities performing domestic intelligence work, including those which are now excluded:
   - — Customs & Border Protection Office of Intelligence and Operations Coordination;
   - — Immigration and Customs Enforcement Office of Intelligence;
   - — Transportation Security Administration Office of Intelligence;
   - — U.S. Customs and Immigration Service Intelligence Branch; and
   - — U.S. Secret Service Protective Intelligence and Assessment Division.
2) The National Intelligence Program budget, annually developed by ODNI, should include the budgets of all those entities now within the Intelligence Community, as well as those proposed above. Not only will this better support a mission package based on the new prioritized threat assessment, but Congressional oversight of a better-organized domestic intelligence enterprise could be achieved.

Inclusion of these domestic intelligence entities and their budgets within the Intelligence Community would help ensure proper coordination of the full range of federal domestic intelligence activities, including in support of SLTT efforts determined by the annual domestic threat fromework (discussed above). This would assist the ODNI in its strategic management of the U.S. government's domestic intelligence efforts, including complionce with constitu-

tional requirements for protection of civil liberties. It would also have the important additional benefit of enabling oversight of the domestic intelligence components of those agencies by the House and Senate's Intelligence Committees, which presently do not provide oversight of these intelligence activities.

Action Required:

The Director of National Intelligence and Secretary of DHS must jointly designate these entities as defined elements of the Intelligence Community consistent with 50 USC Sec. 401a(4)(I).

Maximizing Federal Bureau of Investigation Effectiveness

What BENS Found

Since the September 11, 2001 terror attacks the FBI has made immense strides in emphasizing and expanding its intelligence-driven national security missions. The recent creation of an independent Intelligence Branch is a testament to this progress, and of the concerted leadership by Director James Comey, as well as his predecessor Robert Mueller, to continue to integrate intelligence throughout all of the Bureau's activities. The FBI's maturation into an intelligence-driven agency, however, remains a work in progress.

A recent RAND Corporation report observed: "The FBI has adopted as its new mission focus [intelligence], but its primary mission is the one it has been doing for a hundred years: law enforcement."[1] BENS has also found that legacy cultural issues, personnel policies, and organizational structures inhibit the FBI's complete transformation. As Director Comey has observed: "I've seen tremendous progress, but, to me, it's not good enough."[2]

Recommendation 8

To further enhance the FBI's ability to perform as the lead federal, domestic counterterrorism agency:

1) The newly-created FBI Executive Assistant Director for the Intelligence Branch (or the EAD for the National Security Branch, as determined by the FBI Director in consultation with the DNI) should have a reporting relationship to the ODNI for purposes of federal IC priorities and management, while preserving its direct report to the FBI Director for purposes of its operational law enforcement activities.

2) The FBI should continue to enhance internal recruitment, training and talent management programs to advance an intelligence-driven culture, all created within the context of an integrated and standardized domestic intelligence community.

Actions Required:

1. DNI and FBI Director reach agreement on the reporting relationship of the designated FBI entity. Congress may wish to consider codifying this reporting relationship.

2. Building upon progress made under FBI Directors Robert Mueller and James Comey, continue to emphasize the Bureau's intelligence-driven mission and implement policies that cultivate a skilled analytic cadre.

Focusing the Department of Homeland Security Office of Intelligence & Analysis

What BENS Found

Since its creation in 2003 the Department of Homeland Security's intelligence mission has emphasized identifying potential terrorist threats to the homeland and assessing such threats based upon potential domestic vulnerabilities.[1] In this respect, both Secretary Jeh Johnson and Under Secretary for Intelligence and Analysis Francis Taylor have been particularly forward-thinking and taken positive steps to better position DHS to confront the changing terrorist threat. As Secretary Johnson has remarked, "I'm... concerned about those who self-radicalize... the so-called lone wolf."[2] Secretary Johnson has also stated, "I think we need to continue to build on intelligence information sharing across JTTFs, fusion centers, with the intelligence and homeland security, I think information sharing is key."[3]

Pursuant to this mission, DHS' Office of Intelligence and Analysis is responsible for collecting, analyzing, and disseminating threat-related information to DHS customers at the federal, state, and local levels, as well as managing the DHS Intelligence Enterprise, which is composed of those agencies and components within the department that have an intelligence function.[4] As Under Secretary Taylor has stated, "I&A is working closely with interagency partners to evaluate threat data and ensure relevant information reaches DHS personnel and state, local, tribal, and territorial (SLTT) partners who can use the information to reduce risks to the Homeland."[5]

Through its meetings with federal and state officials, however, BENS learned that I&A's attempt to develop an independent analytic capability rather than focus on integrating the intelligence of DHS component agencies is a primary factor limiting the office's ability to provide a unique contribution to the domestic counterterrorism mission. As it is currently executed, I&A's intelligence role is also too broad and ill-defined and often overlaps with that of other agencies. At the field level there is often confusion among state and local officials as to which federal agency, the FBI or DHS, is in the lead, notwithstanding that the FBI is the lead agency specified in legislation.

Recommendation 9

1) To ensure maximum effectiveness, the Department of Homeland Security's Office of Intelligence and Analysis should focus its attention and efforts on the intelligence derived from the unique knowledge and capabilities of the DHS components and staff. This includes:
   a. Critical infrastructure protection;
   b. Border and transportation security;

c. Aggregating intelligence derived from DHS component agencies and appropriate non-investigative information from state and local law enforcement and intelligence entities;

d. Disseminating and receiving non-investigative warning information to and from the private sector;

e. Performing o warning function for DHS leadership and its agencies with respect to assigned missians; and

f. Pursuant to the guidance of the ODNI, provide leadership ond assistance to the integrated fusion centers recommended above and to the all-crimes, all-hazards state fusion centers, including CVE programs planned and underway.

Actions Required:

1. The Secretary of Homeland Security, in conjunction with the DHS Under Secretary for Intelligence and Analysis, should continue on-going efforts to refocus the Office of Intelligence and Analysis' mission to emphasize the above priorities. This could be covered in the Office of Intelligence and Analysis Strategic Plan.

2. Congress may wish to review the twenty-five I&A functions set out in the statute to ensure they are in accord with the recommendation to focus I&A as described above.

Aiding Congressional Oversight and Budgeting

What BENS Found

U.S. domestic intelligence efforts require focused, coherent, and strong Congressional oversight. This oversight is necessary to ensure that our domestic intelligence efforts are effective and efficient and that they are conducted within legal boundaries and with proper respect to civil liberties. Since 9/11 however, nearly every study of homeland security and intelligence has concluded that Congress' committee and oversight structure is in need of reform. Both the 9/11 Commission and the Graham/Talent WMD Commission characterized Congressional oversight of intelligence as "dysfunctional."[27] BENS concurs with these conclusions.

Evidence of inefficiency can be found in the oversight of the Department of Homeland Security. Over 90 committees and subcommittees share oversight responsibilities for some portion of DHS. Likewise, at least six different Appropriations Subcommittees – from Commerce, Justice, Science and Related Agencies, to Energy and Water Development, to Homeland Security – appropriate funds to agencies conducting domestic intelligence activities.

Recommendation 10

1) All oversight and budgetary authorization actions for intelligence activities should be consolidated under the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.[28]

2) A separate appropriations subcommittee should also be established in both houses of Congress with responsibility for all intelligence activities, foreign and domestic.

Action Required:

A revision to the Rules of the House and Senate to permit the streamlining of the Intelligence Community oversight, authorization, and appropriations processes as recommended above.

Conclusion

In the fourteen years since 9/11, the terrorist threat to the United States has proven to be durable and dynamic. Since that tragic date billions have been spent at home on new domestic security structures and processes and on wars fought abroad; however, the threat remains. Therefore, it is timely and important that a review such as this be undertaken.

As it is now structured, the Nation's domestic counterterrorism and intelligence posture is not optimized to address these dynamic terrorist threats. As the terrorist threat to the United States continues to rapidly evolve, so too must our domestic security architecture.

Al-Qaida, though degraded, is increasingly reliant on regional affiliates to plan regional or transnational attacks. The civil war in Syria continues to attract and mobilize individuals worldwide, including many who become radicalized without ever leaving their home countries through sophisticated social media campaigns by radical groups. Others who go to the region to fight are beginning to return to their countries of origin. Now there are many thousands of battle-hardened and trained fighters who are radical in ideology and have the ability to return to their home countries on their own passports. It is within this context that the threat to the homeland both from abroad and from self-inspired radicals and home-grown violent extremists within looms and calls for agility in our response.

Only by arranging a more strategic, integrated, and collaborative domestic security enterprise, one in which state and local efforts complement national missions and federal efforts coherently support local capacities can the United Sates effectively confront such a dynamic threat. These efforts must be conducted within a stringent legal framework, with respect to due process, and in pursuit of a transparent judicial end-game. In a free and open nation such as ours, there will always be a need to seek a balance between security and civil liberties, but the former should never needlessly subsume the latter. BENS believes that these recommendations would make our ability to assess and contain the threat more agile and effective. The measure of our success will be a safer nation.

Appendix A: Glossary of Key Agencies

Department of Homeland Security Office of Intelligence and Analysis (I&A): responsible for intelligence collection, analysis, and sharing within the DHS intelligence enterprise and provides support to state and urban area Fusion centers.[29]

Federal Bureau of Investigation (FBI): the "exclusive lead agency" responsible for "investigating all crimes ... which involve terrorist activities" within the United States.[30]

FBI Field Intelligence Group (FIG): housed in each of the 56 FBI field offices and responsible for identifying intelligence gaps, analyzing raw intelligence, and generating and disseminating intelligence products.

FBI Joint Terrorism Task Force (JTTF): interagency teams of federal and local personnel responsible for investigating and interdicting terrorist threats. There are 103 JTTFs nationwide, with over 70 having been created since 9/11.

FBI National Security Branch (NSB): established in 2005 to integrate the FBI's counterterrorism and intelligence activities in order to "detect, deter, and disrupt national security threats."[31]

Fusion Center: state-owned and operated entities designed to address "crime prevention, response, and investigation (including terrorism)."[32] 78 centers make up the National Network of Fusion centers.

National Counterterrorism Center (NCTC): the federal government's primary organization for "analyzing and integrating" all terrorism-related intelligence.[33]

Office of the Director of National Intelligence (ODNI): created in 2004 to serve as the head of the Intelligence Community, act as the President's principal intelligence advisor, and exercise broad authority over the intelligence budget.

Appendix B: Acronyms

CIA	CENTRAL INTELLIGENCE AGENCY
CT	COUNTERTERRORISM
CVE	COUNTERING VIOLENT EXTREMISM
DEA	DRUG ENFORCEMENT ADMINISTRATION
DHS	DEPARTMENT OF HOMELAND SECURITY
DNI	DIRECTOR OF NATIONAL INTELLIGENCE
FBI	FEDERAL BUREAU OF INVESTIGATION
FEMA	FEDERAL EMERGENCY MANAGEMENT ADMINISTRATION
FIG	FIELD INTELLIGENCE GROUP
GAO	GOVERNMENT ACCOUNTABILITY OFFICE
HVE	HOMEGROWN VIOLENT EXTREMISM
I&A	DHS OFFICE OF INTELLIGENCE & ANALYSIS
IC	INTELLIGENCE COMMUNITY
JTTF	JOINT TERRORISM TASK FORCES
NCTC	NATIONAL COUNTERTERRORISM CENTER
NIPF	NATIONAL INTELLIGENCE PRIORITIES FRAMEWORK
NJTTF	NATIONAL JOINT TERRORISM TASK FORCE
NSB	NATIONAL SECURITY BRANCH
ODNI	OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
SLTT	STATE, LOCAL, TRIBAL, TERRITORIAL
TLO	TERRORISM LIAISON OFFICE

Appendix C: Staff

BENS Staff

Lauren Bedula, Staff Director
Director for Policy

Mitchell Freddura
Policy Associate

Troy Anderson
Research Associate

Rob Matsick
Research Associate

Luke Roloff
Research Associate

Appendix D: End Notes

[1] Eric Schmitt and Michael Schmidt, "West Struggles to Halt Flow of Citizens to War Zones," New York Times, Jan. 13, 2014; Retrieved from http://www.nytimes.com/2015/01/13/world/west-struggles-against-flow-to-war-zones.html?ref=world&_r=0

[2] James Clapper, "Current and Future Worldwide Threats to the National Security of the United States delivered to the Senate Armed Services Committee," Office of the Director of National Intelligence, February 11, 2014, Retrieved from: http://www.dni.gov/files/documents/WWTA%20Opening%20Remarks%20as%20Delivered%20to%20SASC_11_Feb_2014.pdf

[3] Matthew Olsen, "Hearing before the Senate Committee on Homeland Security and Governmental Affairs: The Homeland Threat Landscape and U.S. Response," Office of the Director of National Intelligence, November 14, 2013, Retrieved From: http://www.dni.gov/files/documents/2013-11-14%20SHSGAC%20HEARING%20(M.%20OLSEN).pdf

[4] Ibid.

[5] James Comey, "Statement before the Committee on Homeland Security House of Representatives Entitled Worldwide Threats to the Homeland Security," U.S. Department of Justice, September 17, 2014, Retrieved from: http://docs.house.gov/meetings/HM/HM00/20140917/102616/HHRG-113-HM00-Wstate-ComeyJ-20140917.pdf

[6] U.S. Department of Homeland Security, "Critical Infrastructure Sector Partnerships," Retrieved from: http://www.dhs.gov/critical-infrastructure-sector-partnerships

[7] U.S. Department of Homeland Security, "State and Major Urban Area Fusion Centers," Retrieved from: http://www.dhs.gov/state-and-major-urban-area-fusion-centers

[8] National Fusion Center Association, "2014-2017 National Strategy for the National Network of Fusion Centers," July 2014, Page v, Retrieved from: https://nfcausa.org/html/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers.pdf

[9] Such as Joint Terrorism Task Forces in connection with counter-terrorism; Border Patrol in connection with trafficking issues; DEA in connection with drug cartels and others, including FBI Field Intelligence Groups.

[10] These three fusion centers are collocated to varying degrees, reflecting their development history and response to their specific threat matrix. Nonetheless, they all reflect the important criteria we believe are necessary for the success of 'integrated fusion centers'.

[11] Such integrated fusion centers should be regional as appropriate to their threat matrix and geography, and so the term 'regional' logically will have different meanings for different integrated fusion centers.

[12] Majority Staff of the Committee on Homeland Security, "The Road to Boston: Counterterrorism Challenges and Lessons from the Marathon Bombings," House Homeland Security Committee Report, March 2014, Page 25, Retrieved from https://homeland.house.gov/sites/homeland.house.gov/files/documents/Boston-Bombings-Report.pdf

[13] U.S. Government Accountability Office, "DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges," June 2014, Page 27, Retrieved from: http://www.gao.gov/assets/670/663794.pdf

[14] BENS recommends the inclusion of these agencies within the defined Intelligence Community.

[15] "Today's Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of the 9/11 Commission Report," Bipartisan Policy Center, July 2014, Page 25, Retrieved from: http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/files/%20BPC%209-11%20Commission.pdf

[16] U.S. Government Accountability Office, "DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges," June 2014, Pages 26, Retrieved from: http://www.gao.gov/assets/670/663794.pdf

[17] http://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf §102A(b)(1)

[18] Bipartisan Policy Center, "Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations," Bipartisan Policy Center National Security Preparedness Group, September 2011, Page 17, Retrieved from http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/CommissionRecommendations.pdf

[19] U.S. Government Accountability Office, "DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges," June 2014, Pages 13, Retrieved from: http://www.gao.gov/assets/670/663794.pdf

[20] Brian Michael Jenkins, Andrew Leipman, Henry H. Willis, "Identifying Enemies Among Us," RAND Corporation, 2014, Page 10, Retrieved from: http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF317/RAND_CF317.pdf

[21] James Comey, "Strengthening Trust: The Way Ahead," at the Intelligence and National Security Summit hosted by Armed Forces Communications and Electronics Association International and Intelligence and National Security Alliance, September 18-19, 2014, Retrieved from: http://www.c-span.org/video/?321596-2/fbi-director-james-comey-intelligence-summit

[22] 107th United States Congress, "Homeland Security Act of 2002", November 25, 2002, §201(d)(1)(A)-(C), Retrieved from: http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

[23] Secretary for Homeland Security Jeh Johnson, "The Secretary's Vision for the Future – Challenges and Priorities," Hearing of the House Homeland Security Committee, February 26, 2014.

[24] Ibid.

[25] U.S. Department of Homeland Security Office of Intelligence and Analysis, "Strategic Plan Fiscal Year 2011 – Fiscal Year 2018," February 2011, Retrieved from: http://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf Also: U.S. Department of Homeland Security, "More About the Office of Intelligence and Analysis Mission," Retrieved from: http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission

[26] Undersecretary for Intelligence and Analysis Francis Taylor, "Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland," Hearing of the Senate Committee on Homeland Security and Governmental Affairs, September 10, 2014.

[27] The National Commission on Terrorist Attacks Upon the United States, "The Final Report of the National Commission of Terrorist Attacks Upon the United States," July 22, 2004, Page 420, Retrieved from http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf;

ALSO "World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism," December 2008, Page XXV, Retrieved from http://a.abcnews.go.com/images/TheLaw/WMD_report.pdf

[28] Except for Foreign Intelligence Surveillance Act warrant procedures, which should remain a shared responsibility between the Intelligence and Judiciary Committees' jurisdiction in both houses.

[29] U.S. Department of Homeland Security, "More About the Office of Intelligence and Analysis Mission," Retrieved from http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission#0

[30] 28 C.F.R. §0.85(l) Retrieved from http://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR&searchPath=Title+28%2FChapter+I&oldPath=Title+28&isCollapsed=true&selectedYearFrom=2014&ycord=805

[31] Federal Bureau of Investigation, "Federal Bureau of Investigation: National Security Branch," Retrieved from http://www.fbi.gov/about-us/nsb/nsb-brochure

[32] National Fusion Center Association, "2014-2017 National Strategy for the National Network of Fusian Centers," July 2014, Page 1, Retrieved from: https://nfcausa.org/html/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers.pdf

[33] National Security Act of 1947 [As Amended through P.L. 110-53, Enacted August 3, 2007], §119(d)(1), Retrieved from http://www.intelligence.senate.gov/nsaact1947.pdf

Notes:

Notes:

EDMUND G. BROWN JR.
GOVERNOR

MARK S. GHILARDUCCI
DIRECTOR

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Mark Ghilarducci
Director, California Governor's Office of Emergency Services
Governor's Homeland Security Advisor

TESTIMONY

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

Frontline Response to Terrorism in America

Tuesday, February 2, 2016

SD-342, Dirksen Senate Office Building
Washington, DC

3650 SCHRIEVER AVENUE, MATHER, CA 95655
(916) 845-8506 TELEPHONE (916) 845-8511 FAX

Chairman Johnson, Ranking Member Carper, Ladies and Gentleman of the U.S. Senate:

Thank you very much for the invitation to address you on this important topic. It is an honor to represent California and the work we are engaged in from both a homeland security and an emergency management perspective.

As California's Director of the Governor's Office of Emergency Services and Homeland Security Advisor to Governor Brown, my portfolio and responsibilities straddle both homeland security and emergency management. As a result, I bring a unique and nuanced perspective to bear today, as my "aperture", so to speak, for viewing and working many complex disasters and emergencies - whether manmade or the result of natural circumstances - is wide open.

I want to focus my testimony today on events in California that have tested our homeland security enterprise, information-sharing systems, and architecture in unique and challenging ways. I also want to talk about the current and evolving threats we face, our homeland security and information-sharing systems in response to these threats, and what we are learning from San Bernardino, to ensure that we are adequately protecting the American people:

- Post-9/11, we built information-sharing systems and a homeland security enterprise (planning, preparing, training, etc.), often times at great cost to the public taxpayer, that were generally focused on thwarting future 9/11-style spectacular attacks.

- As a result, we as a nation, have had many successes in detecting, deterring or disrupting plots against our nation by foreign terrorist organizations (FTOs) and the big attacks they aspired to carry out. As such, FTOs, and now inspired homegrown violent extremists (HVEs), have shifted their tactics away from spectacular style terrorist attacks and moved towards a recognition that attacks in the Homeland against softer targets are easier to undertake, with less barriers to overcome and with outcomes that could be just as effective.

The threat landscape has shifted towards a more diffuse, amorphous threat that focuses on homegrown radicalization and "lone wolf" actors, inspired by FTO propaganda and extremist ideology, and leveraged to act in any way possible. This "new norm" is proving to be just as deadly ... and much harder to counter.

- Today, it is many smaller or direct actions that can be carried out by very few individuals; the tactics are simpler, the targets are softer — focused on vulnerable areas of our communities, with the event then carried globally by the media and by social media within minutes, making any actual attack a propaganda boon.

- The tactics have been largely "active shooter" style events or development and detonation of homemade bombs. Soft targets are far easier to attack and can cause as much, or more fear, as well as political and economic upheaval.

- Both the San Bernardino and Boston events were too easy to execute - and it appears our ability to adequately "connect the dots" to develop a complete picture of a potential plot, and/or identify key signs of an attack remain a challenge in the lead up and execution of these incidents. Even with all of the improvements since 9/11, obtaining and/or identifying key tips and leads, and sharing that information in a timely and actionable way is more critical than ever to combat HVE.

- It is of paramount importance for local and state law enforcement and other public safety responders (Fire, Emergency Management, Public Health and EMS) to be trained and informed to this changing threat; to be made aware of signs and signals, and to have the protocol for reporting; and the system to take Suspicious Activity Reports, scrub them for actionable information and then share that information among partners agencies and organizations in a timely way.

Compounding this, FTOs and HVEs alike are utilizing technology like never before to their advantage, making it even tougher to get advance warning of plots against the Homeland.

- These malicious groups are able to leverage technology, like social media, encryption capabilities and the dark web to their advantage, to reach out to larger, more diverse portions of society, to spread their propaganda and to recruit followers. And they are doing it, for the most part, covertly, which makes it a challenge to detect.

I am often asked, "Are we prepared?" My response, "Yes… and no!"

- We have greatly improved our intelligence gathering, our equipment, our preparedness capabilities and our ability to respond once something goes "boom" … but still have challenges with timely, collaborative and actionable intelligence gathering and information-sharing.

- This makes the need of ongoing risk assessments, stable and consistent funding, training, updating of equipment, updating and leveraging of technology, and access to encrypted material, the building of common operating platforms for the input of multiple threat streams, and key information-sharing critical at all levels.

- It requires a need and ability to be flexible enough to pivot accordingly to prepare for, and be able to respond to, ever-changing threat streams.

I would like to discuss three areas that make overall collaboration and coordination a challenge today, not only in California, but across the country.

While there exist significant improvements in collaboration and relationships among responders, there remains an overall lack of a comprehensive "unity of effort" in our information-sharing environment. After 9/11, our country set out to bridge the communication divide between federal, state, and locals with a specific focus on intelligence and information-sharing at both the unclassified and classified levels, prior to and during terrorist events.

- As seen with the San Bernardino case, we continue to experience challenges in obtaining pieces of intelligence in our ability to connect the dots in the lead up to a possible act of terrorism. There were a number of signs associated with the suspects' actions and their related engagement with co-conspirators that we, as an enterprise, were unable to acquire. Some of this is due to the use of encryption technology by the bad guys, some of this was due to legal provisions in place for gaining access or tracking suspected HVEs, but some aspects of this challenge can be attributed to a simple lack of due diligence and/or gaps in information sharing and communications across all levels.

- In recent years, HVE and cybersecurity threats have evolved in fundamental ways and, in many ways, we are still reactive, rather than proactive, in countering these threats. This needs to change. Built into our homeland security enterprise must be a nimbleness and pro-activeness so that we get out in front of these threats. This needs to have its foundation and empowerment at the local and

state levels and it should start with our information-sharing. Currently there exist many organizations engaged in this intelligence arena, including the FBI, DHS, the Department of State, State Law Enforcement, Local Law Enforcement, the Fusion Centers and the international intelligence community. There remain information and intelligence stove-pipes and organizational protocols protecting designated "proprietary" information that needs to be shared. Plots and terrorist actions are carried out in communities, at the local level, and within states. The impacts of such events, of course, are felt nationally and internationally. This effort must be approached as "one team, one fight", so that we can together remain coordinated and lean as forward as legally possible, leveraging all levels of government capabilities, to all be on the same page in the effort to detect, deter, and protect lives and property. Currently, we as a nation (local, state and federal) are not optimally situated, in my humble opinion, to proactively prevent evolving HVE-style threats.

- The role of the State and Governor's Homeland Security Advisor (HSA) is a critical component to ensuring that objectives, priorities, and collaborative operational actions remain coordinated within States and with local governments. The Chief Executive of a State has the ultimate responsibility for public safety and must be kept informed and engaged. The HSA who is the Governor's point person on statewide security must be a focal point for federal/state/local coordination and collaboration in ensuring a coordinated and proactive posture in support of local government and the State infrastructure. Anything other than this simply undermines the larger unity of effort and common operating platform necessary to detect, deter, prevent and protect, respond to and recover from a potential act of terrorism.

With regard to our Fusion Center network, they are an essential front-line component to our nation's homeland security, but they are often underutilized, and inconsistent in how they are managed and used.

- Fusion Centers are, without question, absolutely critical and represent one of the greatest improvements to our nation's homeland security enterprise. However, in quiet times over the last several years, they have been forced to evolve into "all-crimes/all-hazards" centers to justify their existence. This has spread them thin with regard to their mission focus, and forced them to become distracted from their core counterterrorism functions.

- Further, the coordination of the Fusion Center Network across the country is inconsistent. Some are engaged and connected with the HSA; some are not. Some Centers are established at the local level, some at the State. Makeup and organizational structure vary with different Centers integrating with DHS and some with the FBI, while still others do neither. This inconsistent architecture adds to a lack of common unity of effort at all levels and with critical information sharing.

State Coordination Role During Terrorism Events and Federal Homeland Security Funding. California is unique in that we have a very robust and standardized emergency management system that include very well coordinated fire, law enforcement, emergency medical and emergency management mutual aid systems.

- In California, our Fusion Centers are closely coordinated and oversight is provided by the HSA. These Centers, facilitated by Local Governance Boards, have incredibly strong public/private relationships that are leveraged to facilitate intelligence and information sharing, and to prepare for and respond to emergencies.

- This is all coordinated at the Region and State-levels. Building on these best practices and looking at what works in a state the size of California is important.

- What worked best in San Bernardino was this exact system. The response was very well executed, in the overall context - where the local authority lead the immediate response and was supported in a unified command through mutual aid coordinated by the Region and State. This included personnel, specialized equipment, intelligence and information, authorities and clearance of regulations, victim services, and recovery assistance.

- Outside of the FBI (as the lead federal law enforcement agency, and supported by components of DHS), there were few other federal agencies that provided direct services, incident funding, or mutual aid assistance in a coordinated way, as did California's mutual aid and standardized emergency management system. This should be highlighted as a best practice and a performance metric as a model of a strong unity of effort. The team in San Bernardino was a unified team of local, state, federal agencies, working together with wrap-around and integrated-incident objectives and assistance. The incident required the

combined efforts of multiple organizations beyond law enforcement, to include Fire and EMS, Public Health, Emergency Management, Telecommunications, and Faith Based NGOs, just to name a few.

- Maintaining the ever-changing threat matrix requires flexibility, but most of all continued funding, for all levels of government to ensure we remain vigilant and current in our collective abilities to counter terrorism.

- Since 2008, the State of California has lost approximately $150 million in HLS funding. This has had a profound impact on California, a large and complex state with multiple threat streams, an international border, and an ever-changing population demographic. It has required the HSA, State Agencies, Regional Partners, and local governments to rethink and redefine the approach to counter terrorism; but it has resulted in key functions being dropped or scaled back — functions like adequate training and exercises to account for new and changing threats, key public awareness and education programs, updating and refreshing of equipment and supplies, enhancements of technology, and development of common operating platforms.

DHS remains a good partner, but needs to be continually evaluated to be consistent with current threat streams. Its coordination and communication could be improved. Funding, training and information sharing can be inconsistent and there needs more robust coordination with the HSA, Governors and State's top homeland security officials when engaging with locals and/or private entities within states.

- DHS's policies/procedures/funding have been slow to account for evolving and changing threats. Intelligence products and capabilities, as well as our ability to acquire and develop pre-event intelligence through our Fusion Centers, have shifted more via the FBI or local sources, than from DHS. This is problematic.

- Requests or suggestions for improvement have been slow to occur.

- For example, questions about how threat assessments and Metropolitan Statistical Area (MSA) reports are developed are answered inconsistently. As a state and a local community, it is extremely difficult to build a sustainable CT effort when one year you are designated for funding through UASI and the next year you are not. There is no incentive or sustainability to develop

comprehensive programs, and this undermines the State Homeland Security Strategy. This is very frustrating and results in the inability to have a consistent, integrated unity of effort.

- Many of the DHS Agencies engage in actions that have impacts on the states, however, at times, the state is not consulted or brought into the loop until after the fact or when it is reported in the media. Three recent examples of this include the
(1) placement and movement of Central American Undocumented Alien Children within California communities; (2) the placement of Syrian Refugees within California communities; and (3) the recent engagement between DHS and California private sector businesses on cybersecurity initiatives. While it is understood that all of these topic areas have a federal nexus, the actions carried out by these programs have far reaching public safety and political/policy and economic impacts to the State. The way that DHS carries out these actions is completely opposite to any unity of effort, or a collaborative relationship related to information sharing or common operating initiatives.

- DHS and the State HSAs need better engagement and regular, consistent communication and coordination on all homeland security issues facing the country, states, and localities.

San Bernardino: State Response Efforts. There were multiple actions the State carried out during San Bernardino. In California, for major events, we do not typically operate in a unilateral local, state or federal way. Through the Standardized Emergency Management System (SEMS), in all disasters and major emergencies, we routinely engage local, state, and federal agencies from the initial call through the recovery of the incident.

- It is important to keep in mind that "all disasters are local". As such, the State works closely with local government in a collaborative and coordinated fashion in support of local government. In San Bernardino, there were several state agencies that responded to and/or provided resources or technical expertise through Regional Operations Centers to the City and County. They included the California Highway Patrol (CHP), the Governor's Office of Emergency Services (Cal OES), the California Department of Forestry and Fire Protection (Cal Fire), the Emergency Medical Services Authority (EMSA), the California Department of Transportation (Cal Trans) and California's six Fusion Centers (STAS). All entities responded together, as first responders, based within jurisdictions to help

coordinate mutual aid in the mitigation of the event and to ensure support to the investigation and long term recovery. The San Bernardino incident included this "unity of effort" and coordination by State, Regional and local law enforcement, fire and rescue, EMS and Emergency Management.

- In addition, all of the State's six Fusion Centers were actively involved in providing intelligence and operational support. The primary Center was the Joint Regional Intelligence Center (JRIC) located in Norwalk, CA, and was supported by the other five centers with Triage on Suspect Leads and Tips, Intelligence Products, analysis of and scrubbing of data, and "on scene" analyst support at the Command Post.

- The Unified Command included local, state and federal personnel. There were specialized resources and equipment facilitated by the coordinated mutual aid system including bomb dogs, SWAT, bomb vehicles, specialized communication, EMS and Crisis Management Specialists, etc.

- State personnel were also participants on FBI Joint Terrorism Task Force (JTTFs) and other key task forces related to the response and investigation.

- The Regional and State Operations Centers were activated and provided situational awareness and information coordination. The Governor proclaimed a State of Emergency, which provided key authorities, cleared regulations, provided direction to responders, facilitated costs and City and County Government recovery and assisted victims.

- I am proud to say that the relationships between local, state and federal agencies in California is very good and San Bernardino was no exception. City, County, State and Federal responders came together in San Bernardino with common objectives of saving lives, protecting further loss of life, and neutralizing the moving threat. This very dynamic and dangerous situation demanded close coordination and communication and its success can be attributed to excellent relationships, good training, appropriate equipment and supplies, and robust coordination at all levels.

- California does an extensive amount of collaboration and coordination. Given the size and complexity of California, with its multiple threats and frequency of

disasters and emergencies, this is an absolute necessity. This is all coordinated by the State and its regional partners.

Nevertheless, San Bernardino did present lessons learned, gaps, and challenges. Information and intelligence sharing at all levels is still a problem and is not at the level or quality that it needs to be to fully safeguard this country.

- As the HSA, I require timely and regular intelligence updates during an event of San Bernardino's magnitude, to keep the Governor informed, to engage with my local and federal counterparts, and to coordinate the statewide homeland security and mutual aid missions I spoke previously of.

- Our Fusion Centers, as well as other key officials, require information; all have security clearances and work on counterterrorism issues on a daily basis. They advise me and help me manage situations like this.

- When an event like San Bernardino occurs, we must be careful not to revert back to not wanting to share "proprietary" information. The FBI, in the San Bernardino case, received strong support from the States Regional Fusion Center, but along the way, it became a one way information sharing relationship between the FBI and that Fusion Center, which impacted the Fusion Center's communications responsibilities to the State. This presented challenges and resulted in the lack of relevant information getting to senior leaders and decision makers to keep them informed, particularly when the news was reporting the "proprietary" information through the open media. This required the development of a time consuming "work-a-round" to obtain necessary information at a number of critical junctions of the information sharing stage.

- During San Bernardino, a dynamic that added to confusion was the leaking of information to the media by so called "federal law enforcement sources". These near real-time media leaks were unproductive. It should not work that way – that is not how the 9/11 commission meant for information- sharing systems and coordination to happen in this post-9/11 world.

- This must be one team, one fight. With all of the money and infrastructure established (fusion centers, JTTFs, law enforcement coordination centers, to

name a few) we have spent since 9/11 to safeguard this country, we need to be past "proprietary" if we are to truly function in a manner that allows us to protect the American people.

- This approach is not only disrespectful to many who are working hard every day to serve and protect the American people, but it is highly counterproductive during an incident and results in dissatisfaction, anger, and distrust of our federal partners.

- It is important to remember that San Bernardino and future terrorist attacks of its kind that are bound to occur take place in communities within local jurisdictions and states. The response cannot be a unilateral "federal" takeover or pre-emption during the incident.

Way Forward

We must revisit, and make as a cornerstone of our national homeland security posture, a unity of effort mentality/culture and integrate that doctrine into our training, policies, and procedures as a core focus.

California is working at better integrating our Fusion Center system, by implementing updated performance metrics and updating our Joint Operational Plan, which ensures that our six Fusion Centers are unified, well-coordinated, and consistent in their response and information-sharing.

We expect that this revised plan will improve our Fusion Centers' communications during crises with partners, eliminate duplication of efforts, and enhance overall efficiency and quality of the information the system is producing and sharing.

California prides itself on pioneering new emergency management methods. From my optic, our ability to bring a "unity of effort" mentality to our overall homeland security culture will go a long way in continuing to ensure communications barriers are removed. This unity of effort needs to be built into any updated training & exercises. Our executive leadership at all levels of government, who have the responsibility for homeland security need to ensure that this performance metric is met and re-enforced.

Lastly, funding and flexibility for addressing changing threats need to be revisited to ensure that we remain nimble enough to address and prepare for changing threats to

our communities and to ensure that we have the best, most robust tools, technology, and equipment to adequately protect lives and property.

A renewed focus on and funding for training, exercises, and equipment to account for evolving threats will ensure a robust system. Additional funding for Cyber Security, Active Shooter, Countering Violent Extremism (CVE), Public Education and Awareness, establishment and expansion of the Terrorism Liaison Officers (TLO) Program, development or expansion of Common Operating and Information Platforms, and improvements in Technology are critical. In addition, the importance and benefit of the 1033 Excess Property Program for State and Local Law Enforcement needs to be continued and reinforced. The equipment obtained through this program, used for its intended purpose, is an invaluable resource and one that was essential to deal with the events in San Bernardino.

Thank you.

Office of the Fire Chief Gregg A. Cleveland
La Crosse Fire Department
726 5th Ave South, La Crosse, WI 54601 ■ (608) 789-7260 Fax (608) 789-7276
http://www.cityoflacrosse.org ClevelandG@cityoflacrosse.org
Serving La Crosse and Southwestern Wisconsin Quality Emergency Services Since 1896

Statement of Gregg A. Cleveland, Fire Chief

City of La Crosse Fire Department, La Crosse, WI

February 1, 2016

I would like to thank the Committee for allowing me to submit my statement regarding response to terrorist incidents that have plagued our great nation over the last several years. In my 37 years of service I have responded to numerous fires, explosions, mass casualty incidents, train derailments involving hazardous materials, hazardous materials transportation accidents and releases at fixed facilities, and aviation crashes. I have been fortunate to have received excellent training in response to these situations; however, such is not the ease for first responders who live and work in America's rural areas. Initial and re-current training is essential for all first responders who respond to hazardous materials incidents. Many of the incidents frequently occur in these areas and first responders are not trained to sufficient levels for the hazards they must encounter. Initial training is not adequate for 1st responders who received training when joining a fire department and respond to hazardous materials incident five later.

I would recommend that the federal government invest in initial and re-current training opportunities for rural 1st responders in response to hazardous materials and mass casualty incidents.

Fifteen years following the terrorist attacks of 9/11 radio interoperability still remains a significant obstacle to 1st responders especially for cities the size of La Crosse. The City has recently invested approximately seven (7) million dollars in a new radio system for public safety. While our radio system has been operable for less than 30 days, the system does not have the

capabilities for true interoperability because of the cost to local taxpayers. With La Crosse located on the border of Minnesota and Wisconsin our radio capabilities are limited when coming to the aid of our neighboring fire departments in Minnesota. The system is limited in our capabilities and will easily overload the system. These design issues are prevalent because systems are designed and implemented using local tax dollars. The La Crosse Radio system is designed for "La Crosse" because it serves La Crosse. La Crosse taxpayers cannot afford to build capabilities for any municipalities "outside" of La Crosse. Therefore, radio systems are designed and implemented in a piecemeal fashion. These systems should be funded at the federal level to ensure radio capabilities and needed capacities,

I recommend that congress provide funding for radio system infrastructure to ensure that systems will provide the necessary capacity and interoperability for metropolitan geographic areas.

The fire service has long understood the impact of transportation of hazardous materials on our nation's highways and rails. Each day hundreds of thousands of gallons of hazardous materials such as Bakken crude, chlorine, propane, and gasoline moves through La Crosse by rail or remain in our rail yards waiting further shipment. Tank cars waiting in rail yards pose significant threats for a terrorist who may want to use these tank cars as weapons of mass destruction. La Crosse does not have adequate staffing or equipment to deal with this threat.

I recommend congress assess a fee to the nation's railroad companies and directly share this funding with the states to enhance staffing, equipment, and training for fire departments at the local level to enhance their capacity to respond to rail disasters.

The La Crosse fire and police departments have jointly trained for response to acts of violence and civil disobedience. However, response to active shooters requires significant resources for fire and police departments. With two four year and one two year colleges in La Crosse the potential for an active shooter event is significant. The fire department does not have the staffing to handle this type of incident. The federal government has provided limited funding for the Staffing for Adequate Fire and Emergency Response, this program is woefully underfunded.

I recommend congress increase the funding for the Staffing for Adequate Fire and Emergency Response grant program to provide additional firefighters to response to the increasing demands across this nation placed upon the fire services.

In summary, the La Crosse Fire Department has spent tens of thousands of dollars in training and equipping our firefighters to prepare for response to threats of domestic terrorism. These threats have included home-made explosive and chemical devices, hazardous materials releases, and threats of violence and intentionally set fires.

Coordination and training with our local partners has been a priority because no one agency can adequately respond and mitigate an act of domestic terrorism. Some of the examples I can share with the committee are:

- La Crosse Fire provides regional hazardous materials consultation and response to nine counties including:
    - 100 miles of the Mississippi River
    - Numerous loek and dams of the Army Corp of Engineers

- Over 100 miles of rail line running along the Mississippi River and through the Mississippi National Wildlife Refuge

- La Crosse Fire provides regional Urban Search and Rescue (USAR) service and is a statewide provider of USAR service for the State of Wisconsin
- La Crosse Fire provides regional technical rescue services in collapse, high angle rescue, and other technical rescue services

The La Crosse Fire Department has been an active partner in preparing for and responding to acts of domestic terrorism; however, the costs are borne by the taxpayers of the City. I have previously outlined how Congress can assist local communities in the area of preparing La Crosse and other local agencies to respond to acts of domestic terrorism.

I would like to thank the committee for consideration of my comments.

Respectfully,

Gregg A. Cleveland

Gregg A. Cleveland, Fire Chief
La Crosse Fire Department

Post-Hearing Questions for the Record
Submitted to Wally Sparks
From Senator Ron Johnson

"Frontline Response to Terrorism in America"

February 2, 2016

1. **Please provide any suggestions on how to better allocate resources to assist local first responders. Specifically, how could Congress ensure that resources are allocated to small communities across the U.S.?**

I think the first thing to do is to set a "benchmark" for standard equipment that every police agency, whether that be local police departments or sheriff's departments, should have. The federal government has done a great job of getting all law enforcement officers access to ballistic vests through the Bulletproof Vest Partnership (BVP) Program. In today's threat environment and the ever increasing dangers posed by terrorism and radical extremists, a body worn ballistic vest is not enough. I think that the BVP Program offers a great model to work off of in that it isn't based upon the size of an agency or community, but based on the need for EVERY frontline responding officer to have access to a ballistic vest. The program provides 50% reimbursement under the grant, which helps ALL communities, offset these costs. The BVP Program also has Small Jurisdiction Priority Funding, with legislation that places the priority on funding jurisdictions with less than 100,000 residents. So, my recommendation would be to include Ballistic helmets for every officer under this program as a benchmark for necessary equipment. The next two equipment items that are critical for a terrorism response would be a ballistic shield and a tactical patrol rifle for every marked squad car and I would recommend including those under the same program.

By utilizing the BVP funding model, it still requires a commitment from agencies to fund 50% of the equipment costs, so there is a commitment and buy in on their end. Because many agencies already have this equipment, the costs would be mitigated and directed only to the agencies that currently lack this equipment. Unlike body worn bulletproof vests, the ballistic shields and helmets do not have expiration dates every five years requiring continual replacement. As part of the grant process, local agencies would have to provide an inventory of the current equipment in place (ballistic shields, helmets and patrol rifles), and the necessary equipment needed to obtain this new benchmark of necessary equipment. The process to get everyone this necessary equipment could be done over several years to mitigate the initial costs and prioritized based on current available equipment for each agency.

The last resource that is often needed for a tactical response, and perhaps one of the most controversial, is tactical vehicles (Armored Vehicles such as Bear Cats or MRAPS). Senator McCaskill raised this concern as it relates to the 1033 program with small agencies getting these without a verified need. I think the best way to address this is by determining what a reasonable response time is for getting this piece of equipment to a scene in smaller communities and having this equipment issued on a geographic basis. The need for this equipment is clear, but not every community or department needs to have their own tactical vehicle, but they do need access to one in the event of a terrorist style incident. These vehicles are defensive in nature and are critical in rescuing critically injured persons during an incident as well as providing personnel safe access into a hot zone to confront threats and minimize casualties.

I would recommend that a census be taken of the current 1033 program to determine the current geographic location of tactical vehicles issued through the program. I would then ask each state to survey all the law enforcement agencies within their states to determine department owned and purchased tactical vehicles and utilize a geo mapping program to determine availability of this equipment throughout each state. This would help define the "need" that Senator McCaskill referenced and make sure that agencies awarded such equipment were required to assist local agencies as needed in the event of a critical incident.

2. How can we better improve collaboration between federal, state, and local governments and first responders?

On the Federal level, it clearly starts with trust. To obtain trust, there must be communication, relationships and cooperation. Communication continues to be a one-way street, with everything going up and only a fraction of information going down to the local level, which is severely filtered, both from a time and content standpoint. This limited information to local agencies is likely related to two areas, restrictive policies and a lack of trust of local law enforcement. The first thing I would recommend is that all law enforcement agency executives (Police Chiefs & Sheriffs) be given the appropriate level of security clearance to have access to federal databases that contain the names and locations of individuals on the FBI watch list. Federal agencies should also be required to share any current, direct threat information with local agency executives for incidents or threats in their jurisdiction. This is directly related to the testimony provided at the hearing regarding the "See Something, Say Something" campaign. At its most basic level, this policy decision should be based upon the balance between potentially compromising some federal investigations versus thwarting countless more acts of terrorism by fully engaging the majority of law enforcement officers to save lives.

Yes, there will be investigations that will be compromised in the future, but I believe those risks pale in comparison to the lives that will be saved through the effort of local law enforcement agencies which are provided with the necessary information to fully vet threats and thwart countless acts of violence. This would be counter-cultural to these historic local – federal relations, and we know that it takes time and effort to change decades of culture. As such, I think it would require a policy directive from our federal elected officials to require such information sharing. These terrorist threats necessitate that we dramatically change our tactics if we are to effectively counter these threats and keep our citizens safe.

On the state and local level, there are still some areas that could be improved through better information sharing, but I feel the most important areas to focus on are shared training and resources. Training was a key component referenced in the testimony from all of the panelists during the hearing. This is also directly related to the concept of "one team, one fight" that Mr. Ghilarducci testified to. Outside of the large, metropolitan cities, the vast majority of law enforcement agencies are small and incidents that occur in those jurisdictions will require a response from multiple agencies and those responses need to be well coordinated to address these threats. You cannot have any effective "one team" response unless agencies train together, or at the very least, utilize the same training methods and tactics.

The best way to do this is to reward agencies for cooperative efforts in shared training, equipment and resources. I would recommend that grant funds earmarked for training be prioritized to groups of local agencies that agree to train together and share personnel and resources. I would also recommend requiring they have mutual aid agreements in place to insure a coordinated response in the event of a critical incident. This would include the sharing of resources, such as the regionalized tactical vehicles as outlined in my answer to question #1.

3. Please provide suggestions on how to improve the issue of overclassification of sensitive information.

My response would mirror some of the points in my previous answer on collaboration. First, provide the appropriate security clearances needed for law enforcement agency executives to have access to the federal databases containing information on potential terrorists and threats. One of the concerns we have heard from federal officials is the "overreaction" by local law enforcement when they have contact with subjects on the FBI watch list, which is only known after receiving a NCIC Hit listing a subject as a "possible terrorist organization member – caution". This obviously causes law enforcement officers on scene to consider their safety, which will impact their approach considerations. It would help if law enforcement knew "why" they were placed on this list and would also help to reduce the incidents of overreaction when these contacts occur. This information sharing will also spur

additional information on potential threats as local law enforcement agencies would then be able to vet local contacts and information that would provide significantly more feedback to the FBI and Joint Terrorism Task Forces. As a result, more federal investigations would be initiated and more attacks thwarted.

Next, I would require federal law enforcement officials to contact law enforcement agency executives from any communities where there is an active investigation ongoing. It is not uncommon to have state, federal and local law enforcement agencies conducting simultaneous investigations at the same time, involving the same or linked suspects. By sharing this information we will be able to avoid duplication of efforts, provide quicker resolution on cases and most importantly, avoid putting law enforcement officers at risk through limited information on dangerous targets, or through undercover operations where law enforcement doesn't even know who the good guys and bad guys are.

Law enforcement at every level must adopt the one team, one fight mindset, focus on stopping threats, check their collective egos at the door, and not worry about who gets the credit for the arrest. Some federal law enforcement officers treat local law officers in an inferior light, when the truth is that many local officers have a level of training, skills and experience that match, and in some cases exceed their own. Local law enforcement also knows their community and has contacts and information that federal officers conducting investigations in their communities would not have. The sharing of information and developing better relationships with all our law enforcement partners is critical in developing the trust needed to effectively combat these threats as a cohesive law enforcement team.

4. How can we improve information sharing so we can get important national security information down to the state and local level?

I touched on some of this in my previous answers through providing security clearances to state and local law enforcement agency executives and the requirement to provide real time intelligence on active, ongoing investigations in their respective communities. As it pertains to this question however, I think it is important to also recognize the value of the amount of increased information that would then flow from the local and state level up to the federal level. Just by sharing currently classified information on potential threats will yield volumes of information from local agencies that federal officials may not have access to without directly getting that from local law enforcement agencies. The FBI doesn't have direct access to the majority of Records Management Systems (RMS) from local police departments and would need to make inquiries at these departments to determine if we have had any contact with potential threats. If every local law enforcement agency executive queried their RMS systems for the 6,000+ subjects on the FBI watch list, imagine how much more information could be gathered that could facilitate potential investigations.

These police chiefs and sheriffs would be able to look at any previous police contacts, identify the context of those cases to determine activity that in hindsight is now suspicious and funnel that information up to the FBI or the local JTTF. This information could include associates, vehicles, addresses, phone numbers and even alias names used.

5. How does the rise of the lone wolf threat affect first responder training and response?

These lone wolf threats show the need for EVERY size community and department to have the required level of training to respond to an active shooter threat. This training includes active shooter response and tactical casualty care training to include both law enforcement and EMS departments. Among smaller departments, these lone wolf threats dictate the need for smaller law enforcement agencies and Fire and EMS departments to conduct joint training sessions as there will be multi-agency responses to an incident. Law enforcement, fire and EMS departments need to conduct joint scenario training and work to obtain the required equipment to conduct warm zone and hot zone responses to treat critically injured citizens and officers during an active shooter incident or terrorist attack.

The majority of law enforcement agencies have conducted active shooter / tactical response training within their own respective departments, and a significant number have coordinated some scenario exercises with other local departments. Some have also included Tactical Combat Casualty Care (TCCC) into the law enforcement training, but there is still a large deficit in that training area. Given the nature of these lone wolf threats, every first responder, both police, fire and EMS departments need to have training in TCCC. After the basic training and equipment, these respective agencies need to conduct joint training sessions to include police and EMS personnel responding together to critical incidents as a cohesive team. This is referred to as Rescue Task Force Training, which is a relatively new discipline, but that needs to be established as the new "base" level of training for all first responders from law enforcement and fire/EMS.

6. A lot of time and money is invested in applying for grants, which many small communities do not have access to. How can the federal government ensure that local first responders are spending their valuable time training rather than grant writing?

We need to remove the "competitive" nature of grant writing and determine a streamlined, needs based program that encompasses the current threat environment in our country. Given the needs for every community to have the basic training and equipment as referenced in some of the previous questions, available grant funds should be distributed on the basis of the

number of officers. In my responses to the Question #1 regarding the allocation of resources I mentioned that the BVP program model could be used to facilitate partial funding for equipment needs.

The other key grant need is for training. In Wisconsin, the state provides an annual set amount of $160 per officer to be used for training each year. That helps offset the costs associated with mandated minimum of 24 hours of training required for every sworn law enforcement officer to maintain their certification. The training is logged through the states Training and Standards Bureau each year. Instead of creating another level of grant writing and approval processes, perhaps the federal government could allocate funding on a per officer basis, administered through the states. These funds could only be used for the specified training disciplines that correlate directly to critical, terrorism related responses. Many of these new training disciplines are already being included in new police academy programs, such as in Wisconsin where the recruit academy has increased to 720 hours in 2016 to accommodate the additional training requirements.

While I am not familiar with what the other states are doing, I believe this model would provide a great, fair platform that could be modeled in other states. The other key point to these proposals for the elected officials to consider is that these grants would not go into perpetuity as it would be considered as a gap funding mechanism that would get all the law enforcement officers across the country to get up to a new standard of "required training and equipment". Perhaps one of the requirements for states to be eligible for these training funds would be that these new standards are included in academy certification programs so once every current officer has obtained this training, these grant programs would cease. Since many of the larger departments already have these levels of training, that would also mitigate some of the costs.

Most states already audit training records through their respective certification programs, much of compliance processes are already in place and wouldn't place another burden on the federal government to provide this.

Post-Hearing Questions for the Record
Submitted to Wally Sparks
From Senator Heidi Heitkamp

"Frontline Response to Terrorism in America"
February 2, 2016

1. **Would you please provide specific information or examples of how federal agencies can be better partners in sharing information on threats?**

The first thing I would recommend is that all law enforcement agency executives (Police Chiefs & Sheriffs) be given the appropriate level of security clearance to have access to federal databases that contain the names and locations of individuals on the FBI watch list. At a minimum, law enforcement agency executives should have direct access to any individuals living or working in their respective jurisdictions that are on the FBI watch list. Federal agencies should also be required to share any current, direct threat information with local agency executives for incidents or threats in their jurisdiction. This is directly related to the testimony provided at the hearing regarding the "See Something, Say Something" campaign. At its most basic level, this policy decision should be based upon the balance between potentially compromising some federal investigations versus thwarting countless more acts of terrorism by fully engaging the majority of law enforcement officers to save lives.

Next, I would require federal law enforcement officials to contact law enforcement agency executives from any communities where there is an active investigation ongoing. It is not uncommon to have state, federal and local law enforcement agencies conducting simultaneous investigations at the same time, involving the same or linked suspects. By sharing this information we will be able to avoid duplication of efforts, provide quicker resolution on cases and most importantly, avoid putting law enforcement officers at risk through limited information on dangerous targets, or through undercover operations where law enforcement doesn't even know who the good guys and bad guys are.

Yes, there will be investigations that will be compromised in the future, but I believe those risks pale in comparison to the lives that will be saved through the efforts of local law enforcement agencies which are provided with the necessary information to fully vet threats and thwart countless acts of violence.

a. How do you gauge when federal agencies have successfully provided your organization with timely, accurate and actionable information?

This is very difficult to gauge because we do not have any way to know if there is actionable information available that is not presently being shared. There is a lack of trust between federal and local agencies, and it goes both ways. Whether real or perceived, local law enforcement doesn't feel trusted by federal officials enough for them to share intelligence information with local agencies. Even when we are provided information, many local officers don't trust that they are not getting ALL the information from federal officers. While large cities sometimes have agents imbedded in the departments or in JTTF task force locations, smaller agencies have little to no direct contact with federal officers unless there is an incident in their community that requires communication. The lack of a "personal relationship" has a significant bearing on that trust. I cannot understate just how important it is to develop those relationships and work closely together when incidents occur to foster the level of trust needed to have the effective communication flow needed for local, state and federal law enforcement to adopt the "one team, one fight" mindset that is essential in combatting threats.

The information provided through Fusion centers doesn't contain real time, actionable intelligence, but still serves a purpose in recognizing trends, potential threats and providing after action reports from previous incidents.

THE POLICE COMMISSIONER
CITY OF NEW YORK

April 5, 2016

Honorable Ron Johnson
United States Senate
Chairman, Committee on Homeland Security and Governmental Affairs
Washington, DC 20510-6250

Dear Senator Johnson:

On February 2, 2016, the Committee on Homeland Security and Governmental Affairs held a hearing entitled ""Frontline Response to Terrorism in America." I attended on behalf of the New York City Police Department (NYPD). Included below are the NYPD's responses to the questions submitted by members of the committee subsequent to the hearing.

Questions from Senator Cory Booker:

1. In the White House's 2012 Strategic Implementation Plan, one of the President's objectives was to "foster community-led partnerships and preventative programming to build resilience against violent extremist radicalization..."

   A. Immediately after the attack in San Bernardino, LAPD Deputy Chief Mike Downing met with interfaith and community leaders to ensure that both law enforcement and the community was responding effectively and uniformly to ensure public safety. How can the federal government support law enforcement in engaging communities who are on the frontlines of the fight on terror? Specifically, what are the legal and technological obstacles that hamper this ability?

      (Answer) Chief Mike Downing has led the nation in setting the example of community outreach in the Muslim, Arab, South Asian, and Sikh communities. These efforts began with Chief Downing taking the lead, as a counterterrorism and intelligence chief, to develop trust in a person-to-person manner and under non-

stressful circumstances. Taking the time to develop personal relationships when things are calm ensures that, when crisis strikes, these relationships are strong and are based on trust and experience. If you wait for crisis to call your community "partners," it creates an environment where those bonds are viewed as superficial, or worse, predicated on convenience. All police departments could benefit from the example set by Chief Downing. There are no legal or technological bars to doing this kind of outreach. Building trust should not be vetted by lawyers, nor can it be done purely through social media. It starts person to person, and face to face.

B. What can law enforcement do to build trust, as Mr. Davis points out in his testimony, and bring communities in as partners to help with government responses to terror attacks? For example, if an individual appears on the FBI's radar due to information shared on social media, what is the extent to which the FBI can receive information on that individual that has been collected by State and Local agencies—specifically, prior arrests and/or contacts with the individual, and various personal information regarding that individual?

(Answer) The key to this is the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF). There are more than 100 JTTFs nationally. But it is not enough just to have one; local law enforcement must contribute local officers to be full time Task Force Officers (TFOs), with proper clearances. Those officers need to engage and be full partners, making sure that they also stay connected with their home agency and share information. There is no bar to local law enforcement sharing information with the FBI, and the FBI should be able to reciprocate.

Questions from Senator Heidi Heitkamp:

1. Would you please provide specific information or examples of how federal agencies can be better partners in sharing information on threats?

(Answer) The NYPD attends a weekly meeting at the FBI JTTF at which we go over every significant case in New York, together. In turn, we have the FBI attend our Intelligence Bureau major-case briefing and do the same. The goal is to make sure we are seamless in our approach to these cases.

A. How do you gauge when federal agencies have successfully provided your organization with timely, accurate, and actionable information?

(Answer) We gauge it by whether we get all the information they have, with nothing held back, and by whether we get it not long after the FBI or another federal agency received it. We are satisfied that the information sharing is at an all-time high both in

terms of volume and speed, and that it's flowing in both directions, to and from the NYPD and to and from our federal partners.

Questions from Senator Ron Johnson:

1. Please provide any suggestions on how to better allocate resources to assist local first responders. Specifically, how could Congress ensure that resources are allocated to small communities across the U.S.?

   (Answer) The executive budget, as submitted, cuts Urban Area Security Initiative (UASI) grants by half. This is irresponsible and dangerous in today's threat environment, particularly for urban areas. Despite that fact that the threat to urban areas is growing, the intent is to cut funding to those areas by the largest amounts. That we would deliberately lower our defenses at the such a time cannot be described as anything other than bewildering.

2. How can we better improve collaboration between federal, state, and local governments and first responders?

   (Answer) Continued support by the Department of Homeland Security (DHS) through funding for state and local fusion centers is key to this effort, as is full participation by state and local first responders on the FBI's JTTFs.

3. Please provide suggestions on how to improve the issue of overclassification of sensitive information.

   (Answer) There seems to have been significant improvement with regard to DHS and FBI being able to supply unclassified tear-line products on classified reporting that contain relevant reporting, while stripping away the classified sources and methods used to collect it.

4. How can we improve information sharing so we can get important national security information down to the state and local level?

   (Answer) We have no issues regarding information sharing in New York City. As the cofounders of the nation's first Joint Terrorism Task Force, we have been working with our federal partners since 1980. Over the past two years, under the NYPD's Deputy Commissioner for Intelligence and Counterterrorism John Miller, we've undergone a reset of our relationship that has ensured our collaboration is stronger than ever.

5. How does the rise of the lone wolf threat affect first responder training and response?

(Answer) It is a very significant problem. The "lone wolf," as we saw in Boston and San Bernardino, can pose real challenges to law enforcement. In major cities, the lone wolf threat means having more than just a SWAT team; it means having enough people trained, armed, and equipped to respond rapidly to an unfolding attack—potentially in multiple locations—and take immediate action. Accordingly, in New York City, we have trained 3,500 police officers to be able to respond to active shooters. But the threat also means developing a "rescue task force approach," which considers how to exfiltrate wounded from an attack location without waiting for the incident to be safely concluded. That approach requires establishing a "cold zone" where your command post is located and a "warm zone" where EMTs and medics with force protection can be escorted to a place where they can triage and remove victims, even while officers continue to search for attackers. For areas other than major cities, this means a mutual-aid model, under a unified incident command system, and a good deal of cross training in these tactics between regional partners.

Thank you for the opportunity to have testified before you and the committee in February. Should you require any additional information about these responses to your and your fellow Senators' follow-up questions, please contact Assistant Commissioner Jonathan Murad at jonathan.murad@nypd.org. I look forward to continuing to work with the committee and with all the NYPD's federal counterterrorism partners as we pursue this critical aspect of public safety: keeping Americans safe from terrorism.

All the best,

William J. Bratton
Police Commissioner

Post-Hearing Questions for the Record
Submitted to Chief Rhoda Mae Kerr
From Senator Ron Johnson

"Frontline Response to Terrorism in America"

February 2, 2016

1. **Please provide any suggestions on how to better allocate resources to assist local first responders. Specifically, how could Congress ensure that resources are allocated to small communities across the U.S.?**

   The State Homeland Security Grant Program (SHSGP) is designed to build the statewide capability to prevent, mitigate, prepare for and respond to a terrorist attack. Part of that mission is to develop a statewide system that would protect areas with high risk and threat, and those areas surrounding them that would assist during a terrorist attack. The state should be held accountable to make sure that federal funds are being used to develop a statewide homeland security preparedness system.

   The Federal Emergency Management Agency's (FEMA) Threat and Hazard Identification and Risk Assessment (THIRA) is supposed to help the whole community understand risks and analyze their capabilities. The states are directed to submit an annual THIRA. While some states, such as Texas, have worked well with local authorities in completing their THIRAs, fire chiefs in other states have not been consulted. It is important to make sure that states are consulting all stakeholders – local emergency response agencies, private sector business and organizations, faith-based organizations, individuals, schools and academia, and all levels of government.

   I also would like to point out that the Assistance to Firefighters Grant (AFG) and SAFER grant programs are designed to help small, rural localities, along with major cities and suburban communities. Fire departments submit applications, which then are submitted for a peer-reviewed, merit-based process based on priorities set by the national fire service organizations. The AFG and SAFER grants are meant to help local fire departments improve their baseline all-hazards response capabilities. They use a transparent process to award grants for equipment, staffing and training directly to local fire departments, which leaves out state bureaucracy.

2. **How can we better improve collaboration between federal, state, and local governments and first responders?**

   From the information sharing perspective, we need more fire and EMS representatives in state and local fusion centers and Joint Terrorism Task Forces (JTTF). The fusion centers are supposed to bring together federal, state and local officials from a broad variety of disciplines to identify terrorist threats and plots.

However, we are concerned that the fusion centers are beginning to develop a law enforcement focus, due to the needs of the law enforcement agencies that run them and the absence of other disciplines in the fusion center. During the Great Recession, it was difficult for a fire department to dedicate a firefighter to a fusion center or JTTF, when the department was forced to "brown out" a neighborhood fire station. Grants such as the Urban Areas Security Initiative (UASI) and SHSGP can provide the necessary funding to support fire and EMS staffing as part of a fusion center's operations.

Also, federal training and exercise programs allow federal, state, and local officials to work together. Austin has taken advantage of regional training programs to knock down silos and collaborate with local law enforcement and other stakeholders to develop terrorism response plans. It is important to point out the importance of regional mutual aid agreements among the local fire departments. We train together and have developed the same standard operating procedures. This forces a regional approach to fire and EMS response, which would be a benefit during the response to a terrorist incident.

In addition, it is important that federal, state and local authorities use the National Incident Management System (NIMS) during joint training and exercises. All stakeholders – federal, state, local, fire, EMS, law enforcement, emergency management, public health – must be trained in NIMS and be able to use it during major emergencies and disasters. During both the response to the Ebola outbreak and other major incidents in 2014, we saw entities that did not use NIMS nor were fluent in its operation, which created problems.

3. **Please provide suggestions on how to improve the issue of overclassification of sensitive information.**

It is important that federal and state intelligence analysts work with local officials to develop intelligence products. The IAFC has an intelligence requirements document available on its website for local fire and EMS departments to use when meeting with federal and state officials. The Joint Counterterrorism Assessment Team (JCAT) at the National Counterterrorism Center invites local first responders to work on intelligence products, such as the Fireline and the Roll Call Release, for local first responders. It also allows local first responders to educate federal intelligence analysts about the type of information that local agencies need.

It also is important to recognize that local first responders do not need to know the sources and methods of how information is obtained. We are only interested in terrorist tactics, techniques, and procedures so that we can prepare for them.

Also, the fire and EMS representatives in fusion centers can run into problems with the Law Enforcement Sensitive (LES) classification. LES is not an official classification level, so it can create silos within the fusion center.

4. **How can we improve information sharing so we can get important national security information down to the state and local level?**

   The IAFC has created the Homeland Security Intelligence Guide to help fire chiefs work with federal, state, and local agencies to learn about threats and risks to their communities (http://www.iafc.org/files/1DISASTERmgntHOMEsec/terr_HomelandSeIntelGuide4FireChiefs.pdf). The IAFC urges chiefs to build relationships with local fusion centers, local law enforcement agencies, and local FBI JTTFs. Where possible, fire departments should place staff at the local fusion center, such as we are doing in Austin. However, it is important to note that that cost, staffing and cultural concerns still present obstacles to full fire and EMS service participation in fusion centers.

   Also, I want to point out how effective fellowships for state and local first responders at federal agencies (such as the JCAT) are. However, we need to make the process for participating in these fellowships less bureaucratic. Austin had a fire captain prepared to serve as a JCAT fellow, but ran into bureaucratic issues. These federal fellowships should strive as much as possible to make the local first responder agency whole (full reimbursement for the staffer, backfill) for participating in these programs.

   The federal agencies also can share more information on the Homeland Security Information Network (HSIN). HSIN is a good one-stop shop for federal homeland security threat and risk information.

5. **How does the rise of the lone wolf threat affect first responder training and response?**

   Many local fire and EMS agencies are implementing training for active shooter incidents, which in many cases are perpetrated by lone wolf actors. This training involves working more closely with law enforcement at the scene of an incident, developing tactical operations to treat victims in buildings before the shooter has been apprehended, using advanced treat and triage techniques to aid mass casualties on scene, utilize tourniquets to control the bleeding of victims, and making sure that all response agencies and surrounding jurisdictions are fluent in how to use NIMS. It also is important that public health agencies and hospitals are active participants in the planning and training for the response to a lone wolf incident.

   Because of the random threat of a lone wolf attack and the increased threat against public safety officials, local first responder agencies are urging that their officers remain vigilant and demonstrate increased awareness. Fire and EMS personnel are encouraged to report suspicious activity – that might indicate planning for a lone wolf attack – in accordance with their agencies' suspicious activity reporting procedures and training.

6. **A lot of time and money is invested in applying for grants, which many small communities do not have access to. How can the federal government ensure that**

local first responders are spending their valuable time training rather than grant writing?

The IAFC encourages small communities with volunteer fire departments to apply for AFG and SAFER programs. These programs have fairly straightforward application processes and allow online applications. Some departments have expressed issues with using the Data Universal Numbering System (DUNS) and registering with the System for Award Management, which FEMA makes standardized for grant awardees. The state administering authority manages the SHSGP application along with the UASI application with the assistance of the UASI region.

While UASI funds are aimed at high-threat urban areas, they can assist smaller local jurisdictions too. For example, UASI-funded training brought together all of the stakeholders in the Austin area, including smaller neighboring jurisdictions, neighboring volunteer fire departments, the U.S. Attorney's Office, public health officials, and the city manager for an annual Chemical. Biological, Radiological, Nuclear and Explosive (CBRNE) exercise. The UASI funds allowed the Austin region to provide training that it had not been able to do on its own and brought all of the stakeholders together to learn how to work together in a catastrophic situation. Austin also was able to purchase props and develop staff expertise with the initial federal funding that the city used to continue these annual CBRNE exercises after the UASI funding expired.

Post-Hearing Questions for the Record
Submitted to Chief Rhoda Mae Kerr
From Senator Heidi Heitkamp

"Frontline Response to Terrorism in America"

February 2, 2016

1. **Would you please provide specific information or examples of how federal agencies can be better partners in sharing information on threats?**

The number one priority for improving information sharing is to focus on getting timely, declassified information to local partners. Local fire and EMS organizations need to have information about threats to their jurisdictions and the tactics, techniques and procedures for which they should prepare. They do not need to have sources and methods, which is usually the classified information.

In addition, many fire chiefs still do not have security clearances, mainly because of cost and time issues. This problem is exacerbated in the volunteer fire service (which covers rural areas), where annual elections may be held for fire chief.

The Austin Fire Department participates in state and local fusion centers, and has a full-time officer assigned to the local Federal Bureau of Investigation's Joint Terrorism Task Force (JTTF). As fire chief, I attend executive level briefings. Much of the classified information that I receive does not seem to need to be classified and seems to be released to the media shortly afterward.

It would be better for the federal agencies to focus on producing unclassified information that could be used to brief city leaders and deputy and assistant chiefs, who may not have clearances. This material should be actionable, timely, and relevant.

Also, it is important for local jurisdictions to become more actively involved in information sharing. Fire chiefs should build relationships with local fusions centers, JTTFs and law enforcement officials to share information. In addition, fire and EMS departments should develop suspicious activity reporting policies based on the National Suspicious Activity Reporting Initiative. Fire departments also should take advantage of the Joint Counterterrorism Awareness Team, fellowships at the U.S. Department of Homeland Security and other opportunities for local fire and emergency service officials to work with intelligence analysts to develop products aimed at a local public safety audience.

2. **How do you gauge when federal agencies have successfully provided your organization with timely, accurate and actionable information?**

The Joint Counterterrorism Assessment Team recently produced an excellent one-page pictograph with information on complex, coordinated attacks, like what we witnessed in

Paris in November. The document addressed the challenges of responding to events in hotels or sporting venues. It was a good document, because it identified events that were happening overseas, revealed how such an attack could happen domestically, and explained tactical challenges in a manner that made it relevant to a fire department's preparedness activities.

The JCAT is a program at the National Counterterrorism Center that brings local first responders to work with federal intelligence analysts to develop homeland security intelligence products. It serves as a bridge between the information that the federal government has and the intelligence requirements of local public safety agencies.

United States Senate Committee on Homeland Security and Governmental Affairs

"Frontline Response to Terrorism in America "Hearing, February 2, 2016

Additional Questions

Response of Edward F. Davis, III

March 18, 2016

Questions for the Record from Senator Ron Johnson

1. Please provide any suggestions on how to better allocate resources to assist local first responders. Specifically, how could Congress ensure that resources are allocated to small communities across the U.S.?

Funding for equipment and officer training related to the equipment is essential for officer safety and effective response during a crisis. Large cities that are attractive targets for terrorists need up to date and adequate equipment to respond to catastrophic events. We have seen this time and time again in New York, Boston and other large cities across the US. Smaller cities need the same. However, it is not financially feasible or necessary for every small community to have its own, complete inventory of armored vehicles, swat equipment and other crisis response materials. Regional response teams can be formed with equipment close by and readily available to those communities who are members of the team. They can and should be trained together on how to use and when to use the equipment. This requires a funding commitment to these regional teams that is realistic and consistent. Unreasonable restrictions on the time period within which equipment must be employed should be eliminated. This leads to use of military grade equipment in situations where it is not warranted.

2. How can we better improve collaboration between federal, state, and local governments and first responders?

A single intelligence Czar should be appointed by the President to oversee mandatory sharing of intelligence and implementation of sharing policies and procedures. This should not sit within an existing agency's authority as in practice or perception, the silos will stay firmly in place. A new, independent authority could work across all agencies in a more effective and focused manner.

3. Please provide suggestions on how to improve the issue of overclassification of sensitive information.

I strongly believe that release of certain, sensitive information can jeopardize lives and we need to carefully guard against that in this country. On the contrary, the Brennan Center said it best when they stated that "needless classification—"overclassification"—

jeopardizes national security. Excessive secrecy prevents federal agencies from sharing information internally, with other agencies, and with state and local law enforcement, making it more difficult to draw connections and anticipate threats." http://www.brennancenter.org/publication/reducing-overclassification-through-accountability. We need to use a consistent, safety first, common sense approach in what is deemed shareable and not. If we do not do this, we will continue to run on separate, albeit parallel tracks and information and opportunities will be lost.

4. How can we improve information sharing so we can get important national security information down to the state and local level?

Fusion Centers are critically important to quality and timely information sharing at the federal, state and local levels. Funding for Fusion Centers needs to be increased with assurances that it will continue. This is how they will be most effective using highly trained analysts with clear career paths, who provide accurate and immediate information. Federal, state and local law enforcement need to continue working together as equal members of Joint Terrorism Task Forces across the country and in Fusion Centers with unrestricted access to information including closed cases, which could identify terrorists in their early stages and prevent catastrophic events.

5. How does the rise of the lone wolf threat affect first responder training and response?

Effective response by law enforcement requires a consistent and realistic commitment for funding streams. A lone wolf attack can take many forms and first responders must be prepared for immediate response. San Bernardino and Paris changed the landscape for both organized terror attacks and lone wolf attacks. First responders must be equipped and trained to face large capacity weapons and explosives including IEDs, suicide vests and other bombs when they arrive at the scene of such an attack. One incident could be unfolding simultaneously in multiple locations with various means of carnage. Law enforcement needs to have technologically advanced, state of the art equipment ranging from armored vehicles to tourniquets in every responders toolkit if they are to be successful, stay safe and assist survivors during these incidents.

First responders also need training. It is no longer the traditional swat response training that suffices. It is so important for US Department of Justice and Department of Homeland Security to continue to fund terrorism prevention and response training. This funding allows cities and towns to train with other law enforcement partners. As I testified, in the case of Boston, we trained with our medical community partners prior to the Marathon. This undoubtedly saved lives. During that training, the building of relationships and practicing emergency response together helped all of us identify gaps and agree on practices. Active shooter training is a necessary component of training for first responders and for the community and can result from a lone wolf or more organized terrorist attack. I urge funding to continue in this area also.

Questions for the Record from Senator Heidi Heitkamp

1. How can federal agencies be better partners in sharing information on threats?

A single intelligence Czar should be appointed by the President to oversee mandatory sharing of intelligence and implementation of sharing policies and procedures. This should not sit within an existing agency's authority as in practice or perception, the silos will stay firmly in place. A new, independent authority could work across all agencies in a more effective and focused manner. Information sharing practices need regular auditing if they are to be effective.

I strongly believe that release of sensitive information can jeopardize lives and we need to carefully guard against that in this country. On the contrary, the Brennan Center said it best when they stated that "needless classification—"overclassification"—jeopardizes national security. Excessive secrecy prevents federal agencies from sharing information internally, with other agencies, and with state and local law enforcement, making it more difficult to draw connections and anticipate threats." http://www.brennancenter.org/publication/reducing-overclassification-through-accountability.

We need to use a consistent, safety first, common sense approach in what is deemed shareable and not. If we do not do this, we will continue to run on separate, albeit parallel tracks resulting in lost information and prevention opportunities.

Fusion Centers are critically important to quality and timely information sharing at the federal, state and local levels. Funding for Fusion Centers needs to be increased with assurances that it will continue. This is how they will be most effective with quality analysts providing accurate and immediate information. Federal, state and local law enforcement need to continue working together as equal members of Joint Terrorism Task Forces across the country and in Fusion Centers with unrestricted access to information that could identify terrorists in their early stages and prevent catastrophic events.

Questions for the Record from Senator Cory Booker

1. In the White House's 2012 Strategic Implementation Plan, one of the President's objectives was to "foster community-led partnerships and preventative programming to build resilience against violent extremist radicalization..."

A. Immediately after the attack in San Bernardino, LAPD Deputy Chief Mike Downing met with interfaith and community leaders to ensure that both law enforcement and the community was responding effectively and uniformly to ensure public safety. How can the federal government support law enforcement in engaging communities who are on the frontlines of the fight on terror? Specifically, what are the legal and technological obstacles that hamper this ability?

There are many community/police programs that are proven effective and require funding. Examples of these are police youth dialogues, citizen and teen police academies, Jr. police programs for children, community and interfaith advisory boards for police departments and meaningful job/internship placements for youth.

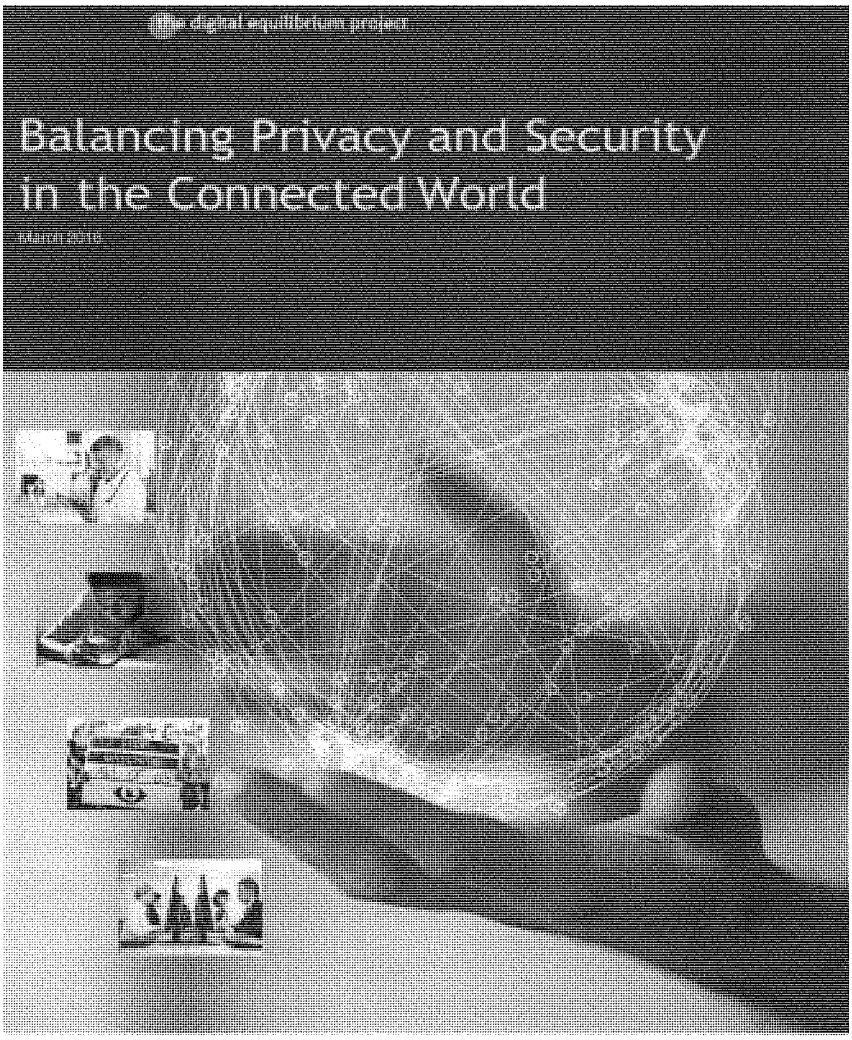
There is another area of growing controversy where the federal government could play an important role: the debate between privacy rights for people vs. the need to gather and share intelligence that could prevent further attacks.

I am currently engaged in a joint project on privacy with McKinsey and Company. Our initial white paper called "Balancing Privacy and Security in the Connected World" as a part of The Digital Equilibrium Project, is very important to this process (attached hereto and incorporated herein by reference).

B. What can law enforcement do to build trust, as Mr. Davis points out in his testimony and bring communities in as partners to help with government responses to terror attacks? For example, if an individual appears on the FBI's radar due to information shared on social media, what is the extent to which the FBI can receive information on that individual that has been collected by State and Local agencies – specifically, prior arrests and/or contacts with the individual and various personal information regarding that individual.

I defer response to the FBI on what they can receive from State and Local agencies.

There have been a multitude of explosive use of force incidents in small, medium and large cities and towns across the United States in recent years. The communities consistently call for transparency from their law enforcement officials. It has never been more important to continuously work on building trust with the communities law enforcement serves. My former colleagues recognize this and continue to build relationships every day. Law enforcement needs to reach community members and activist groups that do not usually sit down with law enforcement officials and engage them in solutions. Community policing efforts need constant care and consistent funding.


the digital equilibrium project
Balancing Privacy and Security
in the Connected World
MARCH 2016

the digital equilibrium project

Contributors

Stewart Baker
Former 1st Assistant Secretary of DHS and General Counsel of the NSA

Tim Belcher
Former CTO, RSA

Jim Bidzos
Verisign Chairman and CEO

Art Coviello
Former Executive Chairman, RSA

Dr. Ann Cavoukian, Ph.D.
Executive Director of the Privacy and Big Data Institute at Ryerson University

Larry Clinton
President and CEO
Internet Security Alliance

Michael Chertoff
Executive Chairman of The Chertoff Group U.S. Secretary of Homeland Security ('05-'09)

Richard Clarke
Former White House Advisor
Chairman and CEO, Good Harbor Security Risk Management

Edward Davis
Former Boston Police Commissioner

Brian Fitzgerald
Chief Marketing Officer, Veracode

Kasha Gauthier
Program Committee Co-Chair, NICE and Special Advisor to the Director, Boston College Cybersecurity Masters Program

J. Trevor Hughes
President and CEO, International Association of Privacy Professionals

Michael McConnell
Former Director of the NSA and Director of National Intelligence

Nuala O'Connor
President and CEO
Center for Democracy and Technology

JR Williamson
Director and Deputy CIO
Northrop Grumman

Knowledge Partner:
McKinsey & Company

Foreword

"The release of atomic power has changed everything except our way of thinking... the solution to this problem lies in the heart of mankind."

Albert Einstein

Would you feel more secure knowing your government could listen to conversations between terrorists? Are you comfortable with the idea that your Smart TV can listen to conversations in your living room? Are you glad that your increasingly intelligent car can save your life? Are you aware that it can be tricked into causing a fatal accident? Are you relieved your doctor can use advanced algorithms to help diagnose your illnesses? Are you concerned that corporations can use advanced algorithms to deny you healthcare? Do you know the insulin pump in your body can be adjusted without painful surgery? Do you know it can be wirelessly disabled without your knowledge?

The physics of the digital world are different than anything we've ever experienced. They ignore national borders. They smash together cultures, ages, continents, kids, adults, criminals, spies, geniuses and twenty-somethings into one global mosh pit, where laws, morals and politics fuse in ways we never could have imagined a few years ago.

Some of these possibilities and risks sound legitimate. Some might sound ridiculous. All are realities of the world we inhabit.

The physics of the digital world are different than anything we've ever experienced. They ignore national borders. They smash together cultures, ages, continents, kids, adults, criminals, spies, and geniuses into one global mosh pit, where laws, morals and politics fuse in ways we never could have imagined a few years ago.

We are totally unprepared for it. But we are charging ahead anyway, because humans explore, innovate, and execute. It is what we do.

We are unready because, at its heart, the internet is not just a technology. It is a new dimension where individuals, organizations and governments must interact in ways that are productive, safe and socially acceptable. But the laws, policies and social norms we have developed over centuries in our physical world are not at all capable of providing the structure we need to inhabit this new dimension peaceably, happily, and prosperously. The power we are unleashing with the internet and digital technology is very much like what Einstein alluded to with atomic power – it has already changed everything, except the way of thinking we will need to cope with it.

We see the results daily. Crimes unpunished. Loss of trust in governments and corporations. Undeterred foreign sovereign-directed attacks, without effective response. We are all digital citizens, but our digital society is a global, increasingly homogenous, and nearly lawless one that becomes more pervasive and important to us with each keystroke.

This is only the beginning. In addition to inviting another billion people to join this society, we are in the process of inviting upwards of 100 billion devices to join it: incredibly intelligent devices with embedded applications that will run our power grids, our hearts, our automobiles, our thermostats, our kids' new playthings. Without some set of norms of behavior and standards for privacy and security, we will not know how to tell these devices to behave appropriately in this interconnected digital world, any more than we know how to tell ourselves or our children.

Our amazing technologies may be planting the seeds for later disaster, even as they make tremendous improvements in our quality of life today.

That may not sound like a big deal today, but the digital and physical worlds - bits and atoms as a recent article in the Economist refers to them - are increasingly fusing into one world where actions in one dimension have real implications in the other, with less knowledge of who is doing what to whom.

Our amazing technologies may be planting the seeds for later disaster, even as they make tremendous improvements in our quality of life. Averting this disaster will rely not on new technology, but rather on re-imagining social disasters as old as human culture itself - privacy and security. Today's news and commentary make it easy to think that these concepts are anachronisms. But they are not. They are essential to the smooth functioning of the physical world, and perhaps more crucial in the digital world. They are essential because trust in our privacy and security is the oil that takes the friction out of human interaction in all its forms. Trusting the sanctity of our personal information, our privacy, and our safety gives us the ability to barter, collaborate, and cohabitate as people and nations.

Re-imagining privacy and security for the digital world is the essential pre-cursor to building the laws, policies and structures that will avert the disasters described at the start of this note. Our project sets the stage for that essential work. It convenes disparate views on issues of privacy, government/citizen relationships, corporate responsibility and the relationships of nations in the digital world. It is about ending stalemate and fostering real dialogue that can help forge the laws, policies, and social norms needed to ensure we can all explore and harness the fruits of a peaceful, safe, and secure digital age.

Thank you for listening. We hope you will join the conversation.

Preface

. . . A high level of trust in the privacy of our online communications became foundational to the explosion of the world wide web and our near-total reliance and faith in digital technologies today.

In the earliest days of the Internet, privacy and security were at peace, mostly because they largely did not exist or even matter. The first Internet was designed to share information between researchers. The concept of private communications was not a requirement. Before criminals, nations and hacktivists prowled the web, secure transfer of digital information was not necessary.

In fact, three men I know well, Ron Rivest, Adi Shamir and Leonard Adleman, arguably have had as much to do with creating today's expectations around privacy and security in the digital world as any other individuals. Building on the work of Whit Diffie and Martin Hellman, the question they posed to themselves in the mid-1970s was a simple one: "could it be possible to send a message on the internet that could be read only by the sender and intended recipient, without a prior relationship between the two?" They proved that in fact it was possible. The result was the RSA algorithm and the foundation for RSA the company (which I had the privilege to lead for many years). However, the implications of their work extend far beyond the borders of a single corporation.

By standardizing, productizing and evangelizing their invention, the company they formed laid the foundation for authenticating and encrypting information on the internet at just the right time. Just as the internet became the world wide web, when browsers and commerce servers appeared in 1994 from Netscape, Microsoft and others, they were enabled with encryption technology from RSA. This technology enabled the safe exchange of personal and payment information that is the underpinning of any commercial and consumer relationship.

They also put in motion the conflicting forces that today compete for control of the digital world. First, their work, and the tools built upon it, created an unprecedented expectation of privacy in the digital world: a high level of trust in the privacy of our online communications became foundational to the explosion of the world wide web and our near-total reliance and faith in digital technologies today. That implicit (and perhaps naive) faith fed our willingness to entrust the digital world with all manner of information about ourselves and our behaviors - information valuable to those who deliver goods and services we desire, but also to criminals, nation-states and others who wish to steal or repurpose the same. Second, by creating the concept of secure communications, they put the emerging digital world in the crosshairs of the world's law enforcement and intelligence agencies, who saw the explosion of digital communication and commensurate data gathering capability as a gold mine for tracking the threats to citizens and nations. Those organizations' ability to listen to the digital world was seen by them as imperative, and therefore completely private communication as anathema, to their goals.

The result of that gap today is a growing tension between privacy and security – not only in our digital world, but also in the physical world that has become intimately and inextricably bound to it.

Today we bestride that crossroads: the pace of change and adoption of digital technologies continues to accelerate. From 2011 to 2015, the percentage of U.S. adults owning a smartphone nearly doubled, from 35% to 68%.[1] From 2010 through 2015, average daily internet consumption similarly doubled worldwide.[2] This blinding pace of digital adoption has far outrun the laws, social norms and diplomatic constructs that we painstakingly developed over centuries to conduct affairs in our physical world. The result of that gap today is a growing tension between privacy and security – not only in our digital world, but also in the physical world that has become intimately and inextricably bound to it.

This is indeed the defining problem of the digital age. Whether we solve it will determine whether we are its masters or victims. It is what catalyzed our group, drives our work, and causes us to ask for your involvement. This work is essential to the continued economic, social, and political progress of our digital and physical world. It must begin now.

Art Coviello

1 Pew. Technology Device Ownership. Available online: http ://www .pewinternet.org/2015/10/29/technology device-ownership-2015/. Last accessed January 14, 2016.

2 Jason Karaian. Quartz. "We now spend more than eight hours a day consuming media." Citing Optimedia survey. http://qz.com/416416/we-now-spend-more-than- eight-hours-a-day-consuming-media/

digital equilibrium project

Privacy & Security in the Digital Age: The Case for a New Approach

What Are We Trying to Accomplish?

The goal of the project is not to provide a complete solution for the future of privacy and security in the digital world. Attempting to do so in isolation would be naive at best. Instead, our goal is to help define the problem in ways that embrace various and legitimate viewpoints from government, industry, and privacy advocates, and create forums for discussion where solutions to these problems can be advanced. An essential precursor to this dialogue is for all sides to move past oft-repeated misinformation that has crystallized into falsehood. Ultimately, our aspiration is to restore privacy and security views to being two sides of the same coin, rather than zero-sum opposing views. After all, the only ones benefiting from today's status quo are those who are the biggest threats to the privacy and security of all of us: criminals, hacktivists and rogue nations.

Why Us?

The contributors to this project come from a wide range of backgrounds and experiences. We are former senior members of America's intelligence and law enforcement communities, leading privacy advocates, technologists, cyber security professionals, lawyers, and business executives. A common passion unites us: changing the discussion around privacy and security in the digital age to foster real progress before it is too late.

The only ones benefiting from today's status quo are those who are the biggest threats to the privacy and security of all of us: criminals, hacktivists and rogue nations

Despite our professional diversity, all of us save one are U.S. citizens. This is not because we believe this is a U.S. problem only – or that it can be solved entirely within the borders of any one nation. We start with the U.S. because it is the world's largest digital glass house. The massive social, economic, and infrastructure exposure of the US to the digital world gives our nation both the most to gain from its safety and order, and the most to lose if order devolves. By starting where the problem is most acute, the stakes highest, we believe we can spark a discussion that will become global in scope.

Why Now?

For several years, privacy advocates have waged a two-front battle. First, they contest what they see as overly intrusive – even illegal – efforts by the U.S. and other governments to gain information about citizens and non-citizens in pursuit of national security. Second, they fight corporations who they believe are collecting massive amounts of information on consumers, often without their informed consent, to use for economic gain. At the same time, the intelligence community has followed the migration of communication from phone and paper to digital technologies of all kinds, harnessing the technologies' collection and analytics power to gain new advantages in support of their missions. In the commercial sector, organizations of all stripes have poured hundreds of billions of dollars into technologies and services designed to secure their digital infrastructures, even as outsiders comprised of state and non-state actors have extracted billions of dollars in value from unprotected or poorly protected corporate digital infrastructure.

Despite massive efforts on all these fronts, most Americans would argue they feel less safe and enjoy less privacy than just a few years ago. For example, less than 10% of Americans polled in 2015 were "very confident" that either the government, landline telephone companies, or credit card companies would ensure both the privacy and security of their records.[3] And the continued theft of intellectual property, financial data and personal information from organizations of all sizes is echoed by the concerns of information security practitioners who feel the task of defending their enterprises from all manner of digital attackers is harder than ever. For example, the number of records breaches reported in the U.S. grew at 29% p.a. from 2008 through2013.[4]

Even as we slide backward in our pursuit of both security and privacy, the light-speed evolution of technology nears an inflection point that makes today's problems pale by comparison to what may come. By 2020, according to many estimates, we will see over 100 billion intelligent devices in use, all connected to our digital networks and systems. These devices will be capable of collecting data on nearly every aspect of our lives, including how we behave in our homes, how our children play, where we drive, how we manage our health and diet, and even how we live in our own backyards. The total economic impact of the internet of things could range between $3.9 and $11.1 trillion by 2025.[5]

Despite massive efforts on both security and privacy, most Americans would argue they feel less safe and enjoy less privacy than just a few years ago.

This explosion of devices will create an exponential challenge both for privacy (nearly every device in our lives will be a source of data for some provider) and security (the attack opportunities created by these devices will be literally a hundred times the level of risk we see in our digital infrastructures today). Without a set of agreed upon principles to guide our social norms, laws, policies and diplomacy to address these changes, we can expect to see catastrophic outcomes in economic, social and even physical domains. These challenges are already with us. If we do not create constructs for addressing them today, we risk losing forever the ability to contain them.

Why You?

If you are reading this paper, presumably you have some interest in and perspective on security and privacy in the digital age. Our goal is to engage you in a constructive, open dialogue that can lead to real progress. It will take many perspectives – and significant commitment – to make real progress on these issues. Your engagement is what will matter most. Regardless of your current perspective on the topic, we encourage you to read this document with an open mind. Challenge our thinking; consider how you could help advance the topic and shape the debate. We cannot use today's disagreements and experiences as reasons to withdraw back to our separate corners, while the hope and promise of our future digital world is increasingly besieged.

But before we – and you – delve into those questions and their implications, first we explain how we have gotten here, the increasing challenges that accelerating technological advances drive, and the implications for individuals, businesses, and world order.

3 Mary Madden and Lee Rainie, Pew Research Center, "Americans' Attitudes about privacy, security and surveillance." 2015. Available online: http://www .pewinternet.org/2015/05/20/americans-attitudes-about-privacysecurity-and-surveillance/. Last accessed January 14, 2016.

4 US-CERT.

5 McKinsey Global Institute. "Unlocking the Potential of the Internet of Things." June 2015. Available online: http://www.mckinsey.com/insights/business technology/the internet of things the value of digitizing the physical world. Last accessed January 14, 2016.

Section 1. Setting the Stage

How We Got Here

It is a truism at best, and cliché at worst, to talk about the 'pace of change' in technology. However, as much as we comment on the continued advanced and evolutions of technology, still we underestimate just how much technology has evolved in the past decade and how fundamentally it is shaping every element of our lives.

In the past decade, processing power has increased by greater than 20 times[6] while its cost has fallen to a small fraction of a cent per unit since 2005[7]. Chipmakers fit billions of transistors onto a single chip, making the internet of things possible and affordable. Internet traffic has increased by greater than 30 times since 2004[8], making our devices chattier and digital communication something we take for granted. Storage capacities have increased by greater than ten times from 2005 to 2015[9] making collection - and retention- of information nearly free. Over the same period, smartphone rated battery capacity increased by 2x, making mobility possible for increasingly-powerful devices. Each of these improvements by themselves is comprehensible. Taken together, the systemic change these technologies are driving is remarkable and unpredictable. For example, processing power, networking, geo-location, and software algorithms working together enable the self-driving car, the crowd-source navigation app Waze, and the changing behavior of the millions of drivers and passengers who constitute the "crowd" that sources the information for Waze by the millions in real-time to improve the service level for all. Massive increases in power and affordability on multiple dimensions simultaneously, leveraged by millions of entrepreneurs worldwide, fueled by tens of billions of dollars of investment, will continue to result in capability we could never predict even a few years before they become real, and shortly thereafter, ubiquitous.

The pace of technological improvement outstrips the ability of even our most creative minds to fully predict or comprehend.

The pace of technological improvement outstrips the ability of even our most creative minds to fully predict or comprehend. In addition, it totally overwhelms the ability of our social systems to keep pace. Our social norms develop slowly, through consensus and shared experience. While the industrial revolution has been centuries in the making, for example, we are only recently coming to grips with the environmental implications that it has spawned and how best to regulate them. Today, the very definitions of what it means to be human is being called into question by advances in genetics and artificial intelligence. In that context, is it any wonder that our definitions of privacy, for example, developed using experiences in the physical world gained over hundreds of years, are no match for the scenarios being creating daily by the lightning-fast evolution of technology?

6 Growth in number of transistors per commercially available microprocess or, 2005-2015, using the Pentium D Smithfield from 2005 (~169M transistors) and the Intel 18-core Xeon Haswell-BP (~5. IB transistors) . Wikipedia . MIT Review.

7 http://www.singularity .com/charts/page62.html

8 Cisco. 1.3 exabytes/month from 2004 to 42 exabytes/month in 2014 . Available online: http://blogs.cisco.com/sp/the-hist01y-and-future-of-internet-traffic. Last accessed January 14, 20 16

9 Extrapolated from International Data Corporation showing data storage capacity growth of ~9x from 2006 to 2012. Wikibon . Available online: http://wikibon.org/wiki/v/Announcement Brief: IBM SONAS Enterprise NAS. Last accessed January 14, 2016.

The same factors hold true on the individual front. Consumers are worried by the news reports on the erosion of privacy by corporations. Add to that the loss of trust resulting from the disclosures of Edward Snowden and others, which exacerbate the situation in ways that stoke fear, uncertainty and doubt. Finally, consider a consumer population equally troubled by the streams of cyber attacks on organizations they have entrusted with their personal information. The result is a society worried and frustrated, but unsure how or where to direct those frustrations. Ironically, they often direct those frustrations at the very enterprises and governments trying to serve them, losing sight of the fact that the cyber attacks on those organizations have arguably the most direct impacts on the sanctity of their personal information and financial and physical security.

The result is a society worried and frustrated, but unsure how or where to direct those frustrations. Ironically, they often direct those frustrations at the very enterprises and governments trying to serve them, losing sight of the fact that the cyber attacks on those organizations have arguably the most direct impacts on the sanctity of their personal information and financial and physical security.

A similar set of factors play out in the relationships between nations as well. The interconnectedness of the digital world has blurred the definition of national sovereignty even as it creates new vectors for espionage, theft of intellectual Property, and even destruction of property and infrastructure. Classic definitions, rules, and agreements fail in this new environment. For example, why is a digital incursion into a corporation that sits on American soil not treated the same way as a physical incursion would be? In addition, as we move towards the internet of things, the ability of one nation (or non-state actors in one nation) to cause physical harm to citizens in a different nation is growing rapidly. Without agreed-upon mechanisms by which to address the grievances created by those actions, it is close to inevitable that nations will choose to act alone to support their interest. At current course and speed, we are moving towards an era where we should expect catastrophic digital conflicts between nations with physical consequences to occur. Perhaps even more frightening, the ability of non-state actors, terrorist groups and even dangerous individuals to acquire and use these destructive capabilities will become easier and easier.

At current course and speed, we are moving towards an era where we should expect catastrophic digital conflicts between nations with physical consequences to occur. Perhaps even more frightening, the ability of non-state actors, terrorist groups and even dangerous individuals to acquire and use these destructive capabilities will become easier and easier.

By nearly every measure, we are losing on both sides. Those who fight for privacy see it eroding at every turn; those who are dedicated to securing our nation, our corporations and our citizens from digital attacks are finding their task harder and more thankless than ever.

The path to today has been fast, rocky and contentious. It is not a sustainable path. Because as challenging as our road had been to-date on the privacy and security fronts, technology is about to enable a step function increase in the ubiquity of digital infrastructure, and the intimacy which it pervades every aspect of our lives. That step function is commonly labeled the 'internet of things'.

Crossing the Chasm; the Fusion of the Digital and Physical Worlds

As previously noted, by 2020 some estimates say that 100 billion intelligent devices will be connected to our digital networks. These devices will occupy increasingly intimate and crucial roles in how we drive our cars, secure and manage our homes, educate our children, grow our food, deliver energy to our cities, and conduct nearly every other aspect of our lives.

These devices are doing more than adding massive scale to our digital infrastructures. Their very nature adds new urgency and new complexity to the need to resolve the security/privacy debate. Why? Because they represent a tipping point where our physical and digital worlds become irrevocably fused, as do our risks and social issues.

Why such dramatic consequences? Three reasons:

1. The increasingly critical role of these devices in our lives, coupled with limited abilities to manage or secure these devices, will add entire new categories of risk, both digital and physical. This will not go unnoticed by nation-states and non-state actors alike who will explore both the defensive and offensive implications and opportunities created by the extraordinary increase in attack surface that results.
2. The intimate role of these devices in our lives, coupled with their ability to collect and share all manner of information about their (and our) status and behavior will render some of our most basic constructs of privacy obsolete.
3. The ability of these devices to lower costs and create value for corporations, while adding convenience and new services for consumers, will make their rapid proliferation inevitable, even as angst over both the security and privacy of our world becomes more acute.

The costs to all of us as the social and legal underpinnings of our integrated physical and digital world become increasingly unstable and ineffective will be potentially incalculable.

While the U.S. may be the world's largest digital glass house today we can expect a 'digital housing boom' globally. Economies worldwide will be increasingly based on digital foundations, resulting in increasing sensitivity to the risks and opportunities for their wealth and safety that are already seen in more digitally advanced economies. For example, the number of countries with 4G mobile network access has more than quadrupled from 20 to more than 80 since 2011. Each of these nations not only adds new global citizens to the mix, but adds new perspectives on privacy and trust to the interconnected global dialogue.

The implications:

The path outlined above threatens to turn our nation-level digital glass houses into a global house of cards. This increasingly powerful and essential digital infrastructure will sit on an ever-less-capable or relevant set of social, legal and diplomatic constructs that are unable to ensure the security and privacy of individuals, organizations and nations.

The costs to all of us as the social and legal underpinnings of our integrated physical and digital world become increasingly unstable and ineffective will be potentially incalculable. Let us repeat that: incalculable. Economic trade depends on foundations of trust – as trust between nations erodes, we can expect increased friction in global trade. The continued theft of wealth in the form of intellectual property theft, for example, already costs the US more than $300 billion annually.[10]

10 The IP Commission Report, 2013. O.2. Available online: http://www.permissions.org/report to M

If the return on investment in innovation falls due to piracy and theft, we can expect enterprises to either rethink their investment strategies or pressure their government for increased intervention in forms that could foster embargoes, tariffs and other forms of trade war. As our digital devices 'cross the chasm' and become intertwined with our physical world, the likelihood of physical harm arising from compromises to digital devices becomes nearly certain. Digitally connected cars, trains, power grids, medical devices and so on create opportunities to reduce many of today's risks, but all represent opportunities for new forms of calamities. Already we see isolated examples sensationalized in the media. History shows that we can expect today's 'proof of concept' hacks to turn into tomorrow's weaponized exploits.

History shows that we can expect today's 'proof of concept' hacks to turn into tomorrow's weaponized exploits.

In summary the friction and risk that comes from a lack of new norms and constructs for digital privacy and security will fall into three categories:

- **Economic:** as described above, increased friction in the global economy could cost minimally $1-2 trillion in just a few years. The longer term threat to trade and globalization and its economic consequences are indeed incalculable, but it is a reasonable estimate that tens of trillions of dollars are at stake.
- **Existential:** as digital exploits increasingly cause physical and economic harm, the risk of existential catastrophe become very real, either directly (exploiting flaws in digital security to disable power grids for example), or as second-order effects (digital attacks or conflicts between nations escalate into traditional kinetic conflicts).
- **Societal:** even if we are able to avoid existential catastrophes, the loss of trust between consumers and providers or citizens and their governments, driven by continued erosions in privacy, will reduce our willingness to use digital technologies freely in the ways we communicate, collaborate and innovate in every aspect of society.

Section 2. The Failure of Today's Debate, and The Opportunity For a New Approach:

A famous self-help book goes by the title of 'What got you here won't get you there." The positive implication of that book is that once you have achieved a certain level of career success, getting to the next level will demand new skills and new approaches.

Unfortunately, when it comes to privacy and security, we cannot even claim success to date. The polarization of the discussion, the vested self-interest of parties on all sides, and the challenges that come from creating lasting consensus in a rapidly changing world have conspired against practical discussion.

. . . getting to the next level will demand new skills and new approaches.

What we propose:

- A new approach that is balanced and sustainable.
- An approach based not on creation of detailed polices or legislation, but instead on creating a framework for creating those instruments – a constitution if you will, not a book of laws. This framework must embody basic beliefs and guiding principles that will be meaningful beyond any evolutions of technology so that it can guide the evolution of our laws and policies as technology changes.
- A set of structures for continued dialogue and problem solving, so that continued rapid changes in the landscape of society and technology can be understood and incorporated into policy, law and public discourse.
- A framework that builds on the successes of the past- that finds and leverages analogies to today's world in free trade, diplomacy, law enforcement and social norms, while embracing the unique characteristics of speed, scale and change that are hallmarks of our new digital age.

Section 3.
A Structure for the New Approach

We hope this paper and the work that follows can lead to that framework. And we intend to start that action by inviting the many voices who need to be represented, those called out in this paper and others who wish to contribute, to come together in Washington for a mid-year meeting to begin the real work of building out the solutions framework- the 'constitution' for the digital world.

Our vision for that mid-year meeting is to begin development of a series of recommendations that can evolve into a framework to be acted on by industry and presented to the incoming administration. Our belief is that these recommendations can be a springboard to a global conversation and ultimately a better and safer digital world.

Our group collaborated over the course of two day-long meetings, complemented by several months of research, multiple interviews with stakeholders in business, privacy and government, and a myriad of individual discussions in the formation of this paper. During these discussions, we came to understand that the scope and complexity of the problem were part of the reason solutions and action have been so difficult to come by. Working together, we developed a structure, built around a set of four fundamental questions that address key dimensions of the problem. We offer that structure here as a way to inform future discussions.

We invite all the contributors to this debate to come together in Washington for a mid-year meeting to begin the real work of building out the solutions framework – the 'constitution' for the digital world.

We thought of the problem along four dimensions, in order to explore privacy and security relationships within organizations; between consumers and providers; citizens and their governments; and between nations themselves. We asked ourselves, and others, a fundamental question about each of those four areas. Moreover, we gathered input and reactions that add depth and clarity to the questions themselves. Again, our intent was not to provide final answers to these questions, but to put enough shape, substance and granularity to their dimensions to make real progress possible.

This section of this paper will be devoted to providing some depth and color to the following four questions:

1. What practices should organizations adopt to achieve their goals while protecting the privacy of their customers and other stakeholders (e.g., privacy by design)?
2. How can organizations continue to improve the protection of their digital infrastructures and adopt privacy management practices that protect their employees?
3. What privacy management practices should governments adopt to maintain civil liberties and expectations of privacy, while ensuring the safety and security of their citizens, organizations, and critical infrastructure?
4. What norms should countries adopt to protect their sovereignty while enabling global commerce and collaboration against criminal and terrorist threats?

We believe that cutting the Gordian Knot of the privacy and security debate into these constituent parts can make the next rounds of dialogue more achievable. Eventually of course, these threads will need to be knit back together into a strong fabric that unifies the varied points of view and challenges represented in each, since each domain has implications for the other. For each question we provide an examination of the question itself, a starting hypothesis for the issue, and a 'blueprint for dialogue' to help drive future discussions towards action.

Question 1: What privacy management practices should organizations adopt to achieve their goals while protecting their customers?

When it comes to personal information and its potential uses by corporations and other organizations, many elements work against transparency.

On its face, this question would seem to be simple to resolve. In an open market, consumers could simply choose to do business with providers of goods and services who managed personal information in ways the consumer was comfortable with. Market forces would strike the natural balance between privacy and convenience, just as they do with prices, quality and other aspects of a free market.

However, those market forces can only work when there is transparency - when both sides know what they are trading and open communication can enable the market, over the course of many transactions to settle on its 'natural' level. When it comes to personal information and its potential uses by corporations and other organizations, many elements work against that transparency:

The pace of change

Technology changes so fast that every element, from the ways information can be collected and what information is actually possible to collect to the ways it can be leveraged for profit or organizational gains, is in constant flux. It is impossible to expect consumers to anticipate all the ways information about them can be collected and used. It is impossible for organizations to perfectly predict all the ways they may wish or need to capture and use information in the future. And it is impossible for laws that target specific technology, collection techniques or uses of information to remain relevant for long, or to avoid unintended consequences from legislation as the technology landscape continues to shift in the future.

The growing value of insight and analytics

Even if organizations could predict their own future uses perfectly, when it comes to the use of information the competitive advantages of unlimited access and use of information are massive. In addition, more often than not, the ways organizations use information about their customers can help to deliver more value for their customers, in the form of more targeted products, more rapid response to changing needs, and more efficient creation and delivery of goods and services. So organizations are inherently motivated to seek new ways to use that information, and are usually rewarded for their efforts by increased revenues or more satisfied customers.

The risk of 'privacy arbitrage'

The massive differences in national laws that regulate collection and use of digital information can, over time, create significant imbalances in the abilities of organizations to compete effectually against better-informed, faster moving rivals. Commercial organizations in particular will be tempted to look globally for the lowest bar to privacy, and assume any higher bar they adopt will inhibit their ability to compete effectively.

Despite those challenges, we believe that elements of an open market can be leveraged to enable improvements in the relationships between consumers and providers of goods and services. What follows here are the sorts of proposals we have discussed in our group and we believe are illustrative of the broader discussions that need to take place.

We believe that elements of an open market can be leveraged to enable improvements in the relationships between consumers and providers of goods and services.

STARTING HYPOTHESIS

- While perfect transparency is impossible, organizations could make significant progress in the clarity and simplification of privacy statements. Making key elements of the organization's information collection and use of machine readable privacy data could enable automation of the consumer's preferences and help establish a more market-based approach to establishing the 'norm' around acceptable practices. It's true that efforts at machine-readable privacy policies have been tried - and have largely failed in the past. But as technology continues to advance, these approaches should not be discarded due to past failures.

- Limiting the use of PII in narrow ways (for example, one time use of health information) may be something that can be embedded in policy, but would be a major source of friction in the ability of the digital world to make rapid advances in everything from healthcare to economic productivity. However, while all the future uses of information may be impossible to predict, privacy statements could embrace broad categories of future use that a consumer could choose to accept or deny, based on their willingness to contribute their information to the organization. Choice and notice themselves are not new, but more transparency is needed to allow consumers to make more intelligent choices about future use of their personal information and ensure privacy by design.

- Some forms of a 'transactional model' could be adopted that allow for a more continuous negotiation of privacy agreements between consumers and providers. Moreover, we could perhaps change the balance of power here - rather than consumers trying to navigate complex legal language with every services they use, why can't they set the parameters and require the service providers to demonstrate they can honor them? Machine-readable parameters set by consumers could be, if made practical, one example of an approach that enables a more fluid transaction-based approach to negotiating privacy between these parties.

All in all, we submit that the major focus on certain kinds of information collection, mostly related to consumer information, threats to warp the dialogue in ways that can hamper massive progress in areas such as health, medicine and education. Accidentally creating constraints on these well-meaning, well-governed practices to put short-lived (and probably ineffective) restraints on corporations in unrelated fields would be one of the biggest tragedies to-date in our nascent digital history.

THE BLUEPRINT FOR DIALOGUE

Who We Invite to Help

Building practical models for a more transaction-based, flexible approach to privacy between consumers and providers requires many voices: EPIC, the Center for Democracy and Technology, IAPP, Electronic Frontier Foundation, the National Chamber of Commerce, The Business Roundtable, and others could have a role here. And the scientific and research community, as well as the technology industry, need to be brought into this discussion so the potential societal gains of information collection and analytics can be weighed against the commercial benefits and consumer risks.

Open questions to help facilitate the dialogue:

- What is the commercial incentive for companies to be more transparent toward their customers/better stewards of their privacy?
- How do we make it easier for regulated sectors who today must wrestle with overlapping or conflicting regulations?
- What is the forcing function that can drive momentum sufficient to overcome the inertia of incumbents that benefit from the status quo?
- How do you define data retention and usage guidelines? With what degree of granularity by industry? By use case?
- How can the concept of private/public space (with varying expectations of privacy) be related to the digital/cyber space?
- Who else should be at the table (e.g., representation from different generational views, someone who can drive political impact)?
- How do we ensure that commercial relationships evolve to match changing expectations?
- How do we reconcile the view of those who consider privacy an absolute right with others who consider it an already obsolete notion? And how do we address those that fall in the middle, between these ends of the spectrum?
- How can we design a solution flexible enough to account for changes in technological and behavioral norms as our society evolves?

Question 2: How can organizations continue to improve the protection of their digital infrastructures and adopt privacy management practices that protect their employees?

This question, like the prior one, would seem relatively simply to answer. Let's take the second part first. Employees work for their companies, and companies have a right and obligation to protect their assets and reputations, including gaining information about their employees.

Background checks for example, are an accepted part of the application process for many organizations today. As to the initial part of the question, the exploding capabilities of the digital world offer powerful new means for organizations to defend themselves, even as those capabilities have proven to give attackers new means of attaining their nefarious goals.

Board-level governance would need to mature quickly to provide context for technical investments and policy creation . . .

Unfortunately, neither question is so simple. Protecting digital networks today is not simply a function of building walls and barriers to hide behind (or to use the language of the Information security world, implementing firewalls and Intrusion Prevention Systems). As digital infrastructures become more fluid and software-based, organizations will be left with only two constants upon which they can focus: their users and the applications with which those users interact. While great scrutiny of users and quality of applications is a must, security also will require deeper insight into the behavior of systems and information, so the subtle, anomalous behaviors that are signs of compromise can be spotted and remediated. But in many nations, for example, worker privacy laws prevent collection of the very kinds of information that are essential to performing that monitoring task. As we continue to blend our professional and personal lives (and both become increasingly digital) pressure will continue to mount on employers to defend networks, but to do so without inadvertently trampling on the privacy rights of employees.

Those challenges cannot be addressed at a technical level alone. Boards of directors could play a far larger role in developing policies for privacy and security. They would need to understand digital risks as well as they understand financial and operational risks today, and be able to assess the competence of their information security programs. Most boards today are woefully unprepared on both accounts. Board-level governance would need to mature quickly to provide context for technical investments and policy creation, or security and privacy practitioners will be caught in the crossfire between employee demands and their respective job requirements.

The immaturity of corporate governance related to digital issues is not the only challenge, however. The following are even more acute:

- Organizations face a quagmire of contradictory or outdated laws and regulations; laws to protect worker privacy, for example, can make use of new behavior-based security technologies that help protect that privacy, actually illegal to implement.
- Personnel for both policy creation and security program management are hard to find. The current skills gap in information security alone is estimated at 300K-1M workers, and will only worsen as the landscape evolves. Without talented and trained professionals to help solve this problem, we will fall further and further behind.
- The complex nature of organizational supply chains, partnerships and business relationships makes the surface area of risk that must be defended nearly infinite in scope.

. . . even the largest and best-funded of security teams feel their defenses are immature and inadequate in the face of the risks they confront.

It's no wonder security teams often feel helpless or un-equipped to meet their challenges no matter how much they spend. While Gartner predicts global IT spending on security to top $100 billion by 2017, a study of IT and risk professionals by one large IT security company (RSA) shows that even the largest and best-funded of security teams feel their defenses are immature and inadequate in the face of the risks they confront.

STARTING HYPOTHESIS

- Business, academic and public sector partnerships could help create a larger flow of qualified cyber professions, both in the technical and policy/leadership domains.
- Boards of directors could add new members that offer the new skills they need, and can collaborate to create more shared knowledge and perspectives.
- Employees in privacy-oriented nations could recognize that they have more to lose by not empowering their security professionals than they do to gain by adopting inflexible postures on privacy: and enterprises could do a better job of providing transparency so their employees know how their information is being collected and protected in the workplace.
- The quality and security of applications, networks and identity management programs could be held to a level closer to that of automobiles, foods and other products where risk of flaw or compromise can lead to significant harm.
- Information sharing partnerships could continue to grow (see FS-ISAC as a model of progress in this area), built around mutual shared-interest such as supply chains, leveraging maturing models for sharing indicators of compromises and the evolving tools, tactics and procedures of adversaries.
- Integral and increased investment in new security capabilities as applications or services are developed will be required, and needs to be considered as essential to digital innovation as HVAC systems are to buildings.

THE BLUEPRINT FOR DIALOGUE

Who We Invite to Help

Myriad organizations can play a significant role in advancing the answers to this particular question. They include the Internet Security Alliance, the National Association of Corporate Directors, the International Association of Privacy Professionals, the National Infrastructure Advisory Council, the Operation Resilient Shield exercise team, the Cloud Security Alliance, The Information Sharing and Advisory Councils, The National Initiative on Cyber Education, FIDO (Fast Identity Online Alliance) and various government agencies.

Open questions to help facilitate the dialogue:

1. How could governments borrow from the nuclear (or other) industry to create and clarify a government role to help corporations protect their critical infrastructure from attack while managing privacy and security interests?
2. How might corporations and corporate boards re-think their governance and oversight programs? (e.g., Center for Audit Quality, National Association of Corporate Directors)?
3. How could we re-work the compliance v. cyber balance so that companies spend more time focused on value-add cyber security strategy and less on compliance-related work?
4. How could we develop enough talent to keep pace with the evolving needs of all the related fields and industries?
5. How could we create a forcing function or criteria for strong application, networks and identity management programs to ensure corporations are adequately protecting their employees and customers?

Question 3: What practices should governments adopt to maintain civil liberties and expectations of privacy, while ensuring safety and security of its citizens and critical infrastructure?

This question has been at the heart of much of the public and media debate in recent years, spurred by the release of classified documents by Edward Snowden and accusations of impropriety against the NSA for collection and use of digital information. The underlying privacy relationship between citizens and their government is as old as societies themselves, and has often been uneasy. However, in the digital world the ability to collect and analyze massive amounts of information without transparency to the public, coupled with the increasing digital footprint of all citizens, takes the issue into new dimensions. And the issue will become more explosive through refinement of technologies such as facial recognition, which will enable identification of individuals anyplace where a camera exists (which today, is already ubiquitous).

The underlying privacy relationship between citizens and their government is as old as societies themselves, and has often been uneasy.

In terms of our collective physical safety, this question is, in the short term at least, the most pressing to make progress on, but perhaps the most difficult as well. Terrorist organizations use the internet (and offshoots such as the so-called 'dark web') in a variety of ways, from recruitment and propaganda to planning and coordinating activities. Cybercrime costs the world's economies over more than $445 billion annually.[11] But as individuals, corporations, nations, criminals and terrorists all increasingly roam the internet together, enabling governments to protect their citizens without compromising the privacy and trust of those citizens is increasingly difficult. Here is where the most dogmatic lines seem to be drawn between privacy advocates and security professionals (including military and law enforcement).

Cybercrime costs the world's economies over more than $445 billion annually.

Interestingly, in this regard the challenges faced by enterprises and governments have many parallels. Just as organizations are adopting new approaches to information security in the face of eroding perimeters and increasing connectivity, government must find ways to defend their citizens in the face of porous national borders, increasing global flow of individuals and the democratization and ubiquity of communication made possible by the internet. Increasingly, that strategy will rely on even more information and better analytics, which, without proper governance, will further exacerbate the concerns of privacy advocates and citizens. The dearth of skill and expertise in the commercial world for cybersecurity will be a factor here as well, as governments seek to protect critical infrastructures from digital and physical attack.

11 Center for Strategic and International Studies. Net Losses: Estimating the Global Cost of Cybercrime. June 2014.

STARTING HYPOTHESIS

- Government could play a bigger role in helping define the 'how', not just the 'why' of protecting critical infrastructure, building on the NIST cybersecurity framework.
- Government could provide proper incentives for corporations to invest in cybersecurity for critical infrastructure.
- Governments could develop and enforce safety standards for software used in critical infrastructures.
- Governance and transparency could be strengthened for intelligence agencies, so that citizens can have confidence those agencies are working within the laws and guidelines that are in place.
- Government could communicate more clearly both the intentions and realities of intelligence gathering efforts. The Edward Snowden disclosures and ensuing outcry saw little to no clear, productive communications response by the White House or Congress. We need rational, fact-based debate and deliberation that result in clear action.
- Legal limits to domestic military involvement can be re-thought: digital tools can now create kinetic actions to cause real physical harm to our infrastructure (as was proven by the Stuxnet-based damage to Iranian nuclear centrifuges). The role of the military in defending US citizens could be re-defined to extend to cyber defense on U.S. soil, without running afoul of legal and constitutional constraints, or increasing the worry of citizens as to their privacy and basic freedoms.

THE BLUEPRINT FOR DIALOGUE

Who We Invite to Help

Government needs to take the lead on this issue, but since critical infrastructure represents an intersection between the public and private sector, government must partner with the commercial sector and others such as EPIC, the Center for Democracy and Technology, IAPP, Electronic Frontier Foundation, the National Chamber of Commerce, business roundtable, and others. The tech community must also move past simply disagreeing with government-led efforts, and begin recommending acceptable alternative solutions that leverage the skills and perspectives of our best innovators.

Open questions to help facilitate the dialogue:

- How should governments approach attribution and retribution to find and punish culprits of cybercrime in all its forms, even across national borders?
- When, if ever, should private companies be allowed to "hack back" and retrieve their stolen information before it's gone for good?

- What types of meta-data should be allowed to be collected and analyzed and what should the governance model be to ensure against actual or inadvertent abuse?
- How can we ensure transparency over law enforcement and defense activities without compromising their missions?
- How can spending resources be pooled between governments to, e.g., improve prosecution rates for cyber criminals (now at 2-3%)?
- Can/Must governments be more proactive, not just reactive/defensive post-attack?
- What does the hierarchy of threat, attack, and proportional government response look like?
- Should government be sharing more information?
- Is there a "NIST 2.0" to create, which is more actionable and easier to use?
- How can the cyber reinsurance market be leveraged or expanded to help?

Question 4: What norms should countries adopt to protect their sovereignty while enabling global commerce and collaboration against criminal and terrorist threats?

As long as there have been nations, there has been espionage. Spying on enemies (and friends alike) has been a known responsibility and set of actions by governments of all stripes.

Sometimes spying is (somewhat) benign, such as simply determining a nation's bargaining position on key issues; sometimes it is far more sinister in its intentions. Signals intercepts have been a part of those efforts since the days of the horse-mounted courier. In the digital world of course, espionage takes on a whole new complexion. Spying on communications has never been easier (for governments with the proper skills), and as more information of every form has become digital, more governments have gotten into the business of spying on behalf of their local corporations, in the form of intellectual property theft and communications intercepts.

When these actions become public, the outcry is understandably great. The action, however, is typically far more tepid. That is because the digital age makes the crimes of espionage at once more intimate and more difficult to prosecute. Intimate because the world largely shares one digital infrastructure, and a host of deep, complex trade relationships that makes commerce, communication and collaboration across national boundaries an absolute necessity. These crimes are more difficult to prosecute because the acts are committed remotely, through networks that make attribution difficult and evidence both ambiguous and highly technical. The perpetrators are (to the average citizen) nameless, faceless and abstract. So the outcry, while great, remains unfocused. And decisive actions by governments to address the concerns of their corporations and citizens becomes easy to avoid.

The U.S. may live in the largest digital glass house today, but a digital housing boom is under way globally.

STARTING HYPOTHESIS

We believe this situation will change. As the world becomes increasingly digital, the playing field will become more level. The U.S. may live in the largest digital glass house today, but a digital housing boom is under way globally. As more nations have more to lose by aggressive cyber activity against their allies and trading partners, pressure will mount to address this issue in a constructive way. Just as nations finally concluded that the long-term benefits of free trade outweighed the short-term benefits of capturing or sinking each other's ships on the high seas, nations will eventually come together to create digital rules of engagement. But why wait?

The risks in the meantime will remain high. Cyber intrusions that cause significant economic or physical damage create the possibility of escalation into traditional armed conflict. Even absent direct escalation into a shooting war, cyber attacks will increasingly cross the plane from bits to atoms and become kinetic in the damage they cause as we connect more of our devices to the internet. It is nearly inevitable that cyber attacks by nation states or terrorist will kill people at some point in time in the next few years. Keeping those incidents isolated, and containing their escalation into armed conflict is essential.

This is where nations must come together, to recognize the mutual interests in promoting clear rules of engagement and international law for the digital world. These agreements are not easy, but they are possible. We know nations are capable on reaching agreement on difficult and complex topics, as evidenced by the recent climate accords in Paris, where agreement was reached between 196 nations.

THE BLUEPRINT FOR DIALOGUE

Who We Invite to Help

Governments must also take the lead here, but other organizations can play a role, including The Center for Strategic and International Studies, Carnegie Endowment, the Council on Foreign Relations, the International Institute for Strategic Studies, the Royal United Services Institute, Brookings, Yale Law, and the Global Commission on Internet Governance.

Open questions to help facilitate the dialogue:

- How could we limit cyber-espionage, to eliminate nation-states targeting individual corporations or organizations for economic or political motives? We believe that espionage will continue, but the current practices of many governments to use their national power to attack private institutions or other nations creates a dangerous imbalance and tips us towards broad-scale cyber conflicts.
- How could we collaborate globally, and empower existing or new institutions to track down international/domestic non-terrorist criminals?
- How could we create 'arms control' mechanisms to limit the spread of increasingly sophisticated malware tools? Unlike traditional weapons, cyber weapons spread rapidly, are quickly reproduced and modified, and are cheap.
- How could we address the issues of non-state actors who may target governments, enterprises or individuals across national borders? These actors often have multiple roles, working for their own goals as well as providing services to governments or other non-state actors.
- How could we create Mutual Legal Assistance Treaties? The US-China agreement to curtail economic-related cyber espionage, and even parts of model treaties offered by China and Russia at the UN could be useful starting points for what a nation state agreement could look like.
- How could we ensure that digital tools (software and systems) can be created free from nation-state interference (either overt or covert) so that these tools can be trusted by users globally?

Section 4. The Prize for Success and the Price of Failure

Today, cutting edge cancer research happens at the intersection of technology, biology, physics and mathematics. The impact of thousands of potential new drugs is modeled in computer simulations that would take years each to conduct using clinical trials. Massive data sets, not crowded hospitals are the source for knowledge- and the proving ground for advances that will perhaps save millions of lives in the years ahead.

Today, capital flows easily to where it can be put to best use, and investors have better insight than ever before into the most productive opportunities for their investments...increasing return for their shareholders but funding the innovations in every field that improve the human condition and create jobs around the globe.

Today we communicate, collaborate, buy, sell, trade and chat about everything in our lives using digital technologies that are already so ubiquitous we don't even notice them; but that are destined in short order to become exponentially more intimate parts of how we live- and how we can die.

Imagine for a moment if Rivest, Shamir and Adleman (and others like them) had come to a different conclusion: that trusted, private communication was NOT practical on the internet as we know it? What would our world be like today? The internet would in all likelihood have remained largely the province of academics and researchers. The world wide web (if established at all) would most likely become a tool for researching publicly-known information. But ecommerce as we know it would not be possible, and broad use of the internet by corporations would not be practical. The transformation we have witnessed over the past few years in how we work, live and play would be a slim fraction of what we now take for granted.

It is up to us to create the constructs that enable the digital age to mature into the force for good it has shown us it can be.

The digital age that's dawned for us promises the most rapid gains in wealth, health, culture and global collaboration we have ever witnessed. It is an adolescent at best, with physical attributes and energy that far outstrips its wisdom, experience and mature sense of right and wrong. It is up to us to create the constructs that enable the digital age to mature into the force for good it has shown us it can be. And to start on that path, it is up to us to form a new kind of dialogue, based on shared long-term interests and mutual trust between ideologies, economic interests and national agendas. Only by doing so can we create the same sort of constitution for the digital world that has served our nation so well in its history.

How to Get Involved

As we stated at the outset, progress on these important issues requires a multi-lateral discussion. Sustainable solutions must balance all perspectives against a set of shared goals and desired outcomes.

Copies of this paper are available at the following sites:

The International Association of Privacy Professionals: *https://iapp.org/resources/article/digital-equilibrium-project/*

The Center for Democracy & Technology: *https://cdt.org/insight/the-digital-equilibrium-project-balancing-privacy-and-security/*

The Internet Security Alliance: *http://www.isalliance.org/privacy/*

The Equilibrium Project: *http://www.digitalequilibriumproject.com*

To inquire about participating in the mid-year conference, please email us at info@digitalequilibriumproject.com

Post-Hearing Questions for the Record
Submitted to Mark Ghilarducci
From Senator Ron Johnson

"Frontline Response to Terrorism in America"
February 2, 2016

1. Please provide any suggestions on how to better allocate resources to assist local first responders. Specifically, how could Congress ensure that resources are allocated to small communities across the U.S.?

Given new threats evolving from homegrown violent extremism (HVE) and the increase in utilization of technology and social media for radicalization purposes, it is more challenging today to predict where a terrorist attack might occur. Large cities and high profile communities are no longer the sole focus of HVE, as evidenced in a number of recent cases across the country. It is important that additional funding be made available for small communities to:

- Develop and sustain training in areas such countering violent extremism (CVE), development of Terrorism Liaison Officer (TLO) programs, and tactical active shooter capabilities that include not just tactical interdiction, but also interagency coordination of mutual aid resources, immediate action decision making, and multi-casualty incident management, etc.
- Have the ability to procure necessary equipment to adequately and safely mitigate the actions of HVE and corresponding cascading impacts;
- Obtain and provide orientations and trainings on social media use and digital forensics for recognition, detection, and deterrence of HVE and other criminal acts;
- Provide the opportunity for an embedded resources link to a regional or state fusion center. This is critical to ensure for increased and adequate information and intelligence sharing and overall officer/public safety;
- Provide best practice metries and assistance for the development of mutual aid agreements and standardized systems to ensure for the ability to either provide or accept and functionally incorporate mutual aid assistance during acts of terrorism; and
- Provide best practices and guidelines for local public safety to engage collaboratively with the Muslim community and other community based organizations (CBOs) in an effort to recognize, interdict, and deter potential radicalization.

To achieve this, a dedicated and sustainable new funding stream and line item in the Homeland Security Grant Program (HSGP) specifically to address small/medium (non-Urban Area Security Initiative) community preparedness, with associated performance metrics, will be most beneficial. This will build on the existing grant allocation models within states and also can, and should, be incorporated into the overall state homeland security strategy.

Finally, for all other areas under the HSGP, Urban Area Security Initiative (UASI) and Emergency Management Performance Grant (EMPG) funding lines (which coordinate, interrelate and support each other) it is absolutely critical to maintain and ensure that grant

funding is made sustainable, and that associated guidelines are consistent year-over-year, which would assist in formulation of long term planning and capability sustainment. Current discussions on cutting funding for Homeland Security and other related programs will not only set us back as a country, but are very dangerous given changing and evolving threats from all hazards.

2. How can we better improve collaboration between federal, state, and local governments and first responders?

The threat and complexity of terrorism, as well as other hazards we face today, requires us to think outside of a single community focus. We must think, plan, and act from the regional to the global level to remain in front of evolving threats and hazards, and to have the ability to collectively prepare for, respond to, recover from, and mitigate or manage the consequences of an event.

A reactive posture is no longer acceptable. For planning, it is important to keep in mind that events occur locally in cities and states. State or regionally-sponsored task forces or working committees engaging federal partners, and where appropriate the private sector, with set program objectives that take into account how we are all connected both locally and globally, necessitating broader collaboration and coordination. Time-sensitive, deliverable performance metrics have proven to be a good way to facilitate collaboration, coordination, and communication for a unity of effort.

We have a good system that must be maintained, but it should be continually improved and refined. Each state has a Homeland Security Advisor (HSA) with responsibility for developing, coordinating, and implementing the overall homeland security strategy for a state. It is a reasonable expectation that the HSA is well suited to facilitate this collaboration and provide the neeessary leadership, working with their colleagues in emergency management, public safety, the National Guard, DHS, and the FBI, among others, to bring together local, state, and federal entities. This is consistent with other emergency management programs that incorporate various layers and stakeholders.

In addition, the old adage, "you fight as you train" really applies to dealing with the consequences of the threats we face. The need for additional funding and identified performance metrics for training and exercises is essential. Overall, homeland security funding has significantly dropped off over the last number of years, while the complexity and challenge of evolving threats has risen. With less funding comes less training and exercises, however we need more of these. Training and exercising continuously helps identify gaps and ensures prepared, coordinated intelligenee, response, and recovery capabilities.

For example, trainings such as the federally-sponsored Joint Counterterrorism Awareness Workshop (JCTAWS), which was put on by the DHS, the National Counterterrorism Center, and the FBI, are incredibly instructive. This training represents a good example of a training metric to inelude a wide cross-section of our public safety community. My team recently participated in the JCTAWS that took place this past February in San Diego. It was a great endeavor because it

garnered wide public safety personnel interaction by including members of federal, state and local fire, emergency medical services (EMS), law enforcement, military, and emergency management communities. The threats we face today require the capabilities of all public safety and the private sector, not just one sector or discipline.

This type of training is crucial because it pushes the participants to think through potential scenarios that could occur within a state. At this recent JCTAWS training, gaps were revealed in a way that other exercises have not exposed. Tough questions were asked and tough answers were given, which more thoroughly prepares our first responders for the realities of today's threat streams. Both executive and rank-and-file representatives were present, and it made a difference in widening the scope of interaction between federal, state, and local governments and first responders. We need more frequent trainings like these.

Training curriculum recently developed here in California by local and state law enforcement personnel on how to deal with a rapidly changing situation and/or an active shooter situation, prior to a formal incident command structure being established, has been extremely well received. It has filled a gap in training that helps to ensure for the best possible management of these events while also working to ensure officer and public safety.

Another area that has proven results and has offered an exceptional opportunity to link the various levels of government and the first responder community is the TLO Program. A TLO is a public citizen or public safety official who has been trained to report suspicious activity that may be encountered during the course of his or her normal occupation. The 9/11 attacks were a catalyst for the program's implementation. In 2002, the first pilot program for TLOs was launched in California. The program linked local law enforcement to the state's fusion centers and the State Office of Homeland Security. Since its inception, California has trained more than 14,000 people as TLOs. While many of these individuals are members of local law enforcement agencies, the program also includes paramedics, firefighters, utility workers, and railroad employees. The program engages first responders and other key stakeholders in understanding threat streams and challenges, and provides the tools necessary to look for and recognize suspicious activity, as well as the ability to provide information and input into the fusion center to a potential problem.

Finally, we need to continually improve information sharing at all levels and ultimately get key information down to the personnel on the street (officers, firefighters, etc.) that are engaging daily within their communities. We need to reinforce the need for proactive and regular information exchanges, and we must provide the tools, technology and training to keep all of these personnel up to par and informed. Better metrics that minimize the stovepipe of information and encourage timely information exchange should be considered.

3. Please provide suggestions on how to improve the issue of over classification of sensitive information.

The response to this question is included in the response to question #4 below.

4. How can we improve information sharing so we can get important national security information down to the state and local level?

When intelligence products on threat streams are being drafted, the following questions should be posed:

- How do we get this information down to the lowest local level?
- How can we package this in a way that will allow for efficient dissemination, without losing time during the de-classification phase?

If these questions are woven into the intelligence analyst's workflow when they are creating the products, it will facilitate a more proactive intelligence process that will be timelier and will include state and local stakeholders as key constituents.

I receive secret and top-secret threat briefs each week at a minimum. Many of the products I receive are designated secret by the agency authoring the document. However, it is often unclear what information is actually secret or why the document is classified as secret. I often tell my team, this is great information to share with our local and state public safety partners, who could use this information to help them understand a particular threat.

It appears that much of the classification is established via agency policy, is determined to be classified by the author, or possibly is just classified because one or two items within the document are part of a larger classified effort. I understand the concern, sensitivities and desire to be conservative. But given that we are all in the public safety arena, with the same goal of protecting lives and property, and detecting and deterring the possibility of an attack, a new review of the classification process should be convened to ensure that we are maximizing our ability to educate and share information with all levels of government. In the interim, the agencies providing classified documents should consider providing an unclassified version of the classified document that can be shared with all public safety in a timely fashion.

5. How does the rise of the lone wolf threat affect first responder training and response?

The lone wolf threat is an evolving and ever-changing complex threat that greatly affects our training and response. This is a gap area. As stated above, with the new threats evolving from HVE and the increase in utilization of technology and social media for radicalization purposes, it is more challenging today to predict where a terrorist attack might occur. Large cities and high-profile communities are no longer the sole focus of HVE as evidenced in a number of recent cases across the country.

We certainly agree with how the intelligence community, specifically the Director of National Intelligence, views these threats, which are constantly morphing, multiplying, adapting, and harnessing technology in new and innovative ways. These threats are undergoing this process at a pace that are outstripping our defenses and, as seen in San Bernardino, often right under our noses.

The lone wolf threat falls into this category, which is a grave challenge and difficult to mitigate against. When we face new threats, we adapt our response frameworks accordingly. Regarding the lone wolf and HVE, we have yet to develop a comprehensive playbook with training and response doctrines that helps us get in front of this threat; we are still in a reactive posture.

We have made some progress in updating procedures, such as the updated law enforcement active shooter guidelines on engagement. Most of our successes are derived from our TLO trainings, specifically when we have included fire departments and EMS personnel into this traditional law enforcement training. Leveraging our fire and EMS resources as "sensors" in the community, as they are out doing their regular jobs, is a force multiplier that can help us mitigate. These trainings are not currently widely adopted, but TLO training that includes municipal code enforcement officers and public works personnel, who work in neighborhoods, could help us get to where we need to be by increasing awareness. In addition, as the HSA in California, I have established key metrics for each of California's fusion centers to emphasize detecting lone wolf activity and reporting and sharing information accordingly.

Nevertheless, this is a very challenging area to detect. Primarily, we need to be able to better connect the dots. We need to link actors and actions with the goal of disrupting terrorism in the preparation phase before it happens. If we cannot accomplish this, we must have the ability to respond accordingly to minimize loss of life and impact to our communities.

We need to address the lone wolf actor threat with enhancements and capability improvements. Here are a few suggestions for consideration:

- Increase information and intelligence sharing at all levels and with all disciplines – both in the detection and deterrence phase, and in the event of an attack, during the incident phase;
- Enhance technology capabilities for the establishment of common operating platforms for intelligence gathering, information sharing, and assessments;
- Enhance ability for interactive collaboration and coordination tools and ability to get real-time evolving information down to local and state first responders;
- Update the threat assessment process and funding to account for potential HVE within states and communities;
- Enhance engagement of the private sector, non-governmental organizations and CBOs;
- Enhance engagement, communication, and involvement with the Muslim Community;
- Develop interdiction and deterrence programs to intervene with individuals in the process of radicalization;
- Engage with our public education system to inform and provide awareness training to teachers and other individuals who may be observing changes in individuals and what it means;
- Enhance overall public education beyond "if you see something, say something";
- Develop and provide increased opportunity for training and exercising for HVE and CVE for public safety responders;
- Establish the TLO Program as a nation-wide program, to better assess, obtain, and scrub potential HVE activity at the local and state levels;

- Enhance the capability within fusion centers to have the technology for obtaining critical threat information and assessments within communities that can be assessed by analysis in building a potential correlation of actors or the possibility for HVE activity;
- Provide the ability for fusion center analysts to obtain top secret clearances as soon as possible so that all necessary information is shared and coordinated, thereby minimizing a potential silo in our own fusion centers;
- Continue to work on allowing law enforcement to gain access to dark web information;
- Review the classification process to allow for and facilitate the sharing of information on all levels of government. For example, if the Joint Terrorism Task Force is working a potential HVE case, at a minimum, the components of the effort should be shared so that the HSA and local authorities are aware and can work to stay in front of the potential threat; and
- Develop, incorporate, and provide additional training on responding to HVE events, such as active shooter; improvised explosives device; and chemical, biological, radiological and explosive events that include coordination and collaboration with all necessary disciplines and public safety responders at all levels.

Post-Hearing Questions for the Record
Submitted to Mark Ghilarducci
From Senator Heidi Heitkamp

"Frontline Response to Terrorism in America"
February 2, 2016

1. Would you please provide specific information or examples of how federal agencies can be better partners in sharing information on threats?

We have seen our Intelligence Community, led by the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), evolve this past year to increasingly provide timely intelligence products and alerts on a range of threats, including cybersecurity, terrorism, domestic extremism, and transnational criminal organizations. Their Joint Intelligence Bulletins (JIBs) have been a tremendous asset in this area. We have seen a noticeable improvement in timely dissemination of these products.

Our federal partners have also increased video teleconferences and physical briefings, notably the DHS and the FBI, after important developments, such as an arrest or threat. This has all been very positive and has assisted with overall information sharing. However, to combat homegrown violent extremism (HVE) and evolving threats, we must provide information and intelligence products proactively. Intelligence and information leading up to, or associated with, a potential lone wolf attack, and/or associated with a particular group or individual being observed within a community or within a state, is important for a proactive security posture and could have an impact in protecting lives and property. Sharing that information with a wider "need to know" audience is critical if we are going to be able to combat these new threats.

It is a well-accepted principal in emergency management that all emergencies are local. This principle equally applies to all acts of terrorism. The consequences of every terrorist attack have a direct impact on local communities. On balance, with the right information being shared in a timely manner, the collective efforts of the local community, the state, and the federal government, can better detect, deter, and mitigate a potential HVE attack.

When intelligence products on threat streams are being drafted, the following questions should be posed:

- How do we get this information down to the lowest local level?
- How can we package this in a way that will allow for efficient dissemination, without losing time during the de-classification phase?

If these questions are woven into the intelligence analyst's workflow when they are creating the products, it will facilitate a more proactive intelligence process that will be timelier and will include state and local stakeholders as key constituents.

The threat and complexity of terrorism, as well as other hazards we face today, requires us to think outside of a single community focus. We must think, plan, and act regionally as well as globally to remain in front of evolving threats and hazards, and to have the ability to collectively prepare for, respond to, recover from, and mitigate or manage the consequences of an event.

A reactive posture is no longer acceptable. For planning, it is important to keep in mind that events occur locally in cities and states. State or regionally-sponsored task forces or working committees engaging federal partners, and where appropriate the private sector, with set program objectives that take into account how we are all connected globally are felt locally, necessitating broader collaboration and coordination. Time-sensitive, deliverable performance metrics have proven to be a good way to facilitate collaboration, coordination, and communication for a unity of effort.

We have a good system that must be maintained, but it should be continually improved and refined. Each state has a Homeland Security Advisor (HSA) with responsibility for developing, coordinating, and implementing the overall Homeland Security Strategy for a state. It is a reasonable expectation that the HSA is well suited to facilitate this collaboration and provide the necessary leadership, working with their colleagues in emergency management, public safety, the National Guard, DHS, and the FBI, among others, to bring together local, state, and federal entities. This is consistent with other emergency management programs that incorporate various layers and stakeholders.

In addition, the old adage, "you fight as you train" really applies to dealing with the consequences of the threats we face. The need for additional funding and identified performance metrics for training and exercises is essential. Overall, homeland security funding has significantly dropped off over the last number of years, while the complexity and challenge of evolving threats has risen. With less funding comes less training and exercises, however we need more of these. Training and exercising continuously helps identify gaps and ensures prepared, coordinated intelligence, response, and recovery capabilities.

For example, trainings such as the federally-sponsored Joint Counterterrorism Awareness Workshop (JCTAWS), which was put on by the DHS, the National Counterterrorism Center, and the FBI, are incredibly instructive. This training represents a good example of a training metric to include a wide cross-section of our public safety community. My team recently participated in the JCTAWS that took place this past February in San Diego. It was a great endeavor because it garnered wide public safety personnel interaction by including members of federal, state and local fire, emergency medical services (EMS), law enforcement, military, and emergency management communities. The threats we face today require the capabilities of all public safety and the private sector, not just one sector or discipline.

This type of training is crucial because it pushes the participants to think through potential scenarios that could occur within a state. At this recent JCTAWS training, gaps were revealed in a way that other exercises have not exposed. Tough questions were asked and tough answers were given, which more thoroughly prepares our first responders for the realities of today's threat streams. Both executive and rank-and-file representatives were present, and it made a

difference in widening the scope of interaction between federal, state, and local governments and first responders. We need more frequent trainings like these.

Training curriculum recently developed here in California by local and state law enforcement personnel on how to deal with a rapidly changing situation and/or an active shooter situation, prior to a formal incident command structure being established, has been extremely well received. It has filled a gap in training that helps to ensure for the best possible management of these events while also working to ensure officer and public safety.

Another area that has proven results and has offered an exceptional opportunity to link the various levels of government and the first responder community is the Terrorism Liaison Officer (TLO) Program. A TLO is a public citizen or public safety official who has been trained to report suspicious activity that may be encountered during the course of his or her normal occupation. The 9/11 attacks were a catalyst for the program's implementation. In 2002, the first pilot program for TLOs was launched in California. The program linked local law enforcement to the state's fusion centers and the State Office of Homeland Security. Since its inception, California has trained more than 14,000 people as TLOs. While many of these individuals are members of local law enforcement agencies, the program also includes paramedics, firefighters, utility workers, and railroad employees. The program engages first responders and other key stakeholders in understanding threat streams and challenges, and provides the tools necessary to look for and recognize suspicious activity, as well as the ability to provide information and input into the fusion center to a potential problem.

Finally, we need to continually improve information sharing at all levels and ultimately get key information down to the personnel on the street (officers, firefighters, etc.) that are engaging daily within their communities. We need to reinforce the need for proactive and regular information exchanges, and we must provide the tools, technology and training to keep all of these personnel up to par and informed. Better metrics that minimize the stovepipe of information and encourage timely information exchange should be considered.

a. How do you gauge when federal agencies have successfully provided your organization with timely, accurate and actionable information?

We gauge federal partners' timely information provision in two ways: strategic timeliness and operational timeliness. Information provided comes to us in various forms, but a written intelligence product or a telephone call is typically the most common.

A product is strategically timely if it helps us understand a development soon after it has occurred, for example within a week or two. Strategic products help us put key developments into context, and are relayed simply.

Information is operationally timely, for example, if our partners provide us information on the issue before we read about it in the news. On operational issues we need to be in lock step with our federal colleagues, even though we are not privy to every detail or case. This is an area that

requires continual attention and a proactive effort to ensure information is shared in a timeframe that can address the needs of senior leaders and decision makers, as well as to ensure for identification of commonalities, trends, and de-confliction on other statewide security initiatives or threats.

In my role as the Governor's HSA, I am responsible to the Chief Executive (the Governor) and the people of California to ensure their safety, security, and protection. To do that job to the best of my abilities, I have an expectation that threats occurring to, or in, California will be brought to my attention in a timely manner and with sufficient information that I can use to address statewide security needs. I have implemented specific performance metrics for my fusion centers and with my federal partners to ensure that this happens. Overall, they do a great job in keeping me informed; but there is always room for improvement, particularly with changing and evolving threats.

Post-Hearing Questions for the Record
Submitted to Mr. Mark Ghilarducci
From Senator Cory Booker

"Frontline Response to Terrorism in America"

February 2, 2016

1. In the White House's 2012 Strategic Implementation Plan, one of the President's objectives was to "foster community-led partnerships and preventative programming to build resilience against violent extremist radicalization..."

   A. Immediately after the attack in San Bernardino, LAPD Deputy Chief Mike Downing met with interfaith and community leaders to ensure that both law enforcement and the community was responding effectively and uniformly to ensure public safety. How can the federal government support law enforcement in engaging communities who are on the frontlines of the fight on terror? Specifically, what are the legal and technological obstacles that hamper this ability?

The federal government can support law enforcement by:

- Ensuring that there is a sustainable and consistent homeland security grant funding stream to states. As noted in my testimony, since 2008, the State of California has lost approximately $150 million in homeland security funding. This has had a profound impact on California, a large and complex state with multiple threat streams, an international border, and an ever-changing population demographic. It has required the Homeland Security Advisor (HSA), state agencies, regional partners, and local governments to rethink and redefine the approach to counter terrorism, and has resulted in key functions being dropped or scaled back. The evolving threat presented by homegrown violent extremism (HVE) requires all levels of government to double their efforts to detect, deter, and where possible, interdict, to disrupt the process of radicalization. Understanding and detecting HVE and lone wolf actors is a complex and very difficult process. There is a tremendous need for increased training and orientation on HVE and countering violent extremism (CVE), as well as building and enhancing the capability of our fusion centers to connect the dots when scrubbing suspicious activity reports and assessing particular threat indicators. Further increased information and intelligence sharing is necessary between local and state law enforcement, Joint Terrorism Task Forces (JTTFs) and fusion centers to ensure that we are all on a common page in detecting and deterring, and if necessary, responding to the consequences of an actual attack. Additionally, training is essential and should not be limited to law enforcement, but should be provided to local and state public safety workers in connection with federal counterparts and select private sector partners. It is necessary to increase exercises that depict real-world scenarios and the

need to share information and coordinate an effective, safe response that minimizes life and property loss.

- Supporting key public awareness and education programs, and expanding outreach programs to state and local communities. This effort requires increased collaboration with non-governmental organizations (NGOs) and community-based organizations (CBOs), particularly within the Muslim community. It also involves engagement with our education institutions to develop and instruct an awareness of HVE and the radicalization process. This new and unique challenge is not addressed by law enforcement alone; it requires the combined effort of many community groups and organizations with an enhanced effort in public awareness beyond the traditional "see something, say something" slogan. HVE requires us to rethink our operational strategies, to remain proactive, and in front of this evolving threat, not simply positioned to react when an attack occurs.

- Updating and refreshing equipment and supplies, allowing for states and fusion centers to build common operating platforms to share and coordinate information in real-time. This will allow for adequate situational awareness and effective utilization of resources to detect, deter, and respond.

- Enhancement of technology to develop common operating platforms and the ability to assess the dark web where much of the HVE radicalization activities occur. Continual review and legislative action is necessary to provide law enforcement with the tools necessary to effectively detect HVE, such as the San Bernardino attack, before they occur.

Smart practices drawn from progressive global community engagement CVE programs, such as those found in Scandinavia or the United Kingdom, could also provide a template for broader intra-government community engagement strategies. Building trust in communities takes time, dedication, and should ideally nest into an overall strategy. The key is to build trust with the communities of focus. Once trust is built, larger government initiatives will have a firm foundation to work from. This is a long term effort. Current grant funding allocations, notwithstanding, are insufficient to address this new threat, and also need to be reconsidered related to hard performance periods. Many of the programs and efforts needed to build community trust must be long term, typically longer than the traditional 2- or 3-year grant performance period.

Finally, technically speaking, we need to ensure that information sharing is happening at every point, at the public level as well as within and between each level of government, including classified and unclassified channels. Sharing more information where we can, and when appropriate, at the lowest common denominator, will aide in the key trust-building phase.

B. What can law enforcement do to build trust, as Mr. Davis points out in his testimony, and bring communities in as partners to help with government responses to terror attacks? For example, if an individual appears on the FBI's radar due to information shared on social media, what is the extent to which the FBI can receive information on that individual that has been collected by State and Local agencies – specifically,

prior arrests and/or contacts with the individual, and various personal information regarding that individual?

Law enforcement has many tools available to build the trust referenced in the response to the first question above. The evolving threat of HVE however, is different than others, as it is based in extreme ideologies. An expanded effort, with expanded tools, best practices and a broader, more inclusive way of thinking and acting is necessary. It will take the community members' engagement to effectively deal with this threat. We need to ensure our law enforcement have the "guardian mindset" and are open and understanding of the problem at hand. They also need to understand the communities they are guarding, and that starts with a robust education program and sustainable funds to ensure that these programs and training can be carried out.

With regard to the FBI accessing state information, in accordance with Title 28 CFR Part 23, upon request, we provide the FBI or any law enforcement organization pertinent information related to cases that they are working. We take great care to protect all sensitive personal and privacy information in accordance with our privacy policy and legal guidelines. We work to not just provide information upon request; we would rather be proactive with providing key information in a coordinated effort. But we can't do this without two-way information exchange. We must know if the FBI is working on a particular HVE case in our state and the respective areas of responsibility prior to learning about the case after an arrest, or an actual act. To be clear, overall information sharing is good with the FBI, but we all need to look at continual improvement. The HVE threat demands that we all are as proactive as possible and continuously sharing information to connect the dots and pick up signals, tips, or leads that could lead to averting a possible attack.