ADDRESSING REMAINING GAPS IN FEDERAL, STATE, AND LOCAL INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

FEBRUARY 26, 2015

Serial No. 114–6

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

94–110 PDF WASHINGTON : 2015

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

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

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

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

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

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PETER T. KING, New York, *Chairman*

CANDICE S. MILLER, Michigan
LOU BARLETTA, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MICHAEL T. MCCAUL, Texas *(ex officio)*

BRIAN HIGGINS, New York
WILLIAM R. KEATING, Massachusetts
FILEMON VELA, Texas
BENNIE G. THOMPSON, Mississippi *(ex officio)*

MANDY BOWERS, *Subcommittee Staff Director*
DENNIS TERRY, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Staff Director*

CONTENTS

ADDRESSING REMAINING GAPS IN FEDERAL, STATE, AND LOCAL INFORMATION SHARING

Thursday, February 26, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to call, at 2:03 p.m., in Room 311, Cannon House Office Building, Hon. Peter T. King [Chairman of the subcommittee] presiding.

Present: Representatives King, Barletta, Hurd, and Keating.

Also present: Langevin.

Mr. KING. The Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence will come to order.

The subcommittee is meeting today for our first hearing of the 114th Congress to hear testimony from three National law enforcement associations regarding the importance of information sharing and on-going challenges.

I would like to welcome the Ranking Member and express my appreciation to all the witnesses who have traveled to be here today.

I recognize myself for an opening statement.

Let me just say at the outset, they are talking about votes starting somewhere in the next 20 minutes or so. So what the Ranking Member and I would like to do is do our statements and then allow time for you to make your opening statements. The vote shouldn't take long. Then we will come back for the testimony if that is agreeable to everyone.

Again, I thank you for coming down here and sorry for the inconvenience. If I can find a way to blame it on the Democrats, I will. But since we control the House, it is getting harder to do that. But I will think of something before it is over.

For our first hearing, the subcommittee is focusing on the importance of information sharing and counterterrorism cooperation between Federal, State, and local law enforcement. This hearing should demonstrate that this committee considers local law enforcement and first responders as absolutely vital in the homeland security mission and sets the stage for much of the committee's activity in the 114th Congress.

A cop or sheriff's deputy on patrol, an analyst reviewing a suspicious activity report, or a first responder interacting with the public carrying out their daily responsibilities are most likely going to be the first to identify a possible threat. In the event of a terrorist attack, they will be the first to respond. There are over 780,000 law enforcement officers in the United States, including

Federal, State, and local law enforcement officers. Ensuring that information is available and accessible to appropriate law enforcement personnel at all levels is a critical force multiplier in our Nation's effort to defend against homeland terror attacks.

Since September 11, 2001, there have been a number of terror attacks in the homeland conducted by violent Islamic extremists, the 2009 Little Rock recruiting station shooting, the Fort Hood massacre in 2009, Northwest Airlines Flight 253 on Christmas day, 2009, the 2010 attempted car bombing in Times Square, and the April 2013 bombings at the Boston Marathon.

Additionally, there have been at least two small-scale attacks inspired by ISIS, the Oklahoma City beheading in 2014 and the hatchet attack against two NYPD police officers just last October. The threat of home-grown radicalized individuals is growing. There have been 94 home-grown, violent jihadist plots in the United States since September 11, with over 70 percent occurring in the last 5 years. We are dealing with unprecedented numbers of people seeking to join ISIS and other terror groups. There are over 150 U.S. persons who have or have tried to join ISIS.

Just yesterday, three men were arrested in New York and Florida for conspiracy to provide material support to ISIS, including joining their group as fighters. This group was also discussing carrying out attacks in the homeland, specifically in Brooklyn and against the President of the United States. We have seen disrupted travelers carrying out attacks in Canada, Australia, and elsewhere. It is vital that State and local law enforcement have visibility into this threat and on-going cases in their areas of responsibility.

While progress has been made to improve the flow of information, after-accident analyses of past attacks show there are remaining challenges. A common trend in these different reviews is the need for Federal departments and agencies to view State and local law enforcements as partners in National security and counterterrorism. The need for leadership within organizations to ensure accountability, information sharing, wider access to necessary databases, and the professionalization of information sharing. It is probably true that these issues will never be perfectly addressed. But we must keep in mind that our war on terror is a decades-long effort to defeat a dedicated enemy. Anyone who doubts that should remember that today is also the anniversary of the first World Trade Center bombing that killed six and wounded thousands of people. One of those six was a neighbor of mine, Monica Rodriguez Smith. We must continue to make every possible improvement to our homeland security, including intelligence information sharing.

I look forward to the testimony of the witnesses.

[The statement of Chairman King follows:]

STATEMENT OF CHAIRMAN PETER T. KING

FEBRUARY 26, 2015

For our first hearing in the 114th Congress, the subcommittee is focusing on the importance of information sharing and counterterrorism cooperation between Federal, State, and local law enforcement. This hearing should demonstrate that this committee considers local law enforcement and first responders as absolutely vital in the homeland security mission, and set the stage for much of the committee's activity in the 114th Congress.

A cop or sheriff's deputy on the patrol, an analyst reviewing a suspicious activity report, or a first responder interacting with the public carrying out their daily responsibilities are most likely going to be the first to identify a possible threat. In the event of a terrorist attack, they will be the first to respond.

There are over 780,000 law enforcement officers in the United States (including Federal, State, and local law enforcement officers (LEOs)). Ensuring that information is available and accessible to appropriate State and local law enforcement personnel is a critical force multiplier in our Nation's efforts to defend against homeland terror attacks.

Since September 11, 2001, there have been a number of terror attacks on the homeland conducted by violent Islamist extremists: The 2009 Little Rock Recruiting Station shooting, the Fort Hood shooting (2009), Northwest Airlines Flight 253 on Christmas day 2009, the 2010 attempted car bombing in Times Square, and the April 2013 bombings at the Boston Marathon.

Additionally, there have been at least two small-scale attacks inspired by the Islamic State of Iraq and Syria (ISIS): Oklahoma beheading (2014) and the hatchet attack against four New York Police Department (NYPD) officers (2014).

The threat of home-grown, radicalized individuals is growing. There have been 94 home-grown violent jihadist plots in the United States since 9/11, with over 70% occurring in the last 5 years.

We are dealing with unprecedented numbers of people seeking to join ISIS and other terror groups. There are over 150 U.S. persons who have, or have tried, to join ISIS. Just yesterday, three men were arrested in New York and Florida for conspiracy to provide material support to ISIS, including joining the group as fighters. This group has also discussed carrying out attacks in the homeland, including targeting law enforcement and military personnel. We have seen disrupted travelers carry out attacks in Canada, Australia, and elsewhere. It is vital that State and local law enforcement have visibility into this threat and on-going cases in their areas of responsibility.

The unfortunate reality is that there is plenty of counterterrorism work to go around and this threat requires close coordination between Federal, State, and local law enforcement.

While progress has been made to improve the flow of information, action analysis of past attacks shows that there are remaining challenges. A common trend in these different reviews is the need for Federal departments and agencies to view State and local law enforcement as partners in National security and counterterrorism, the need for leadership within organizations to ensure accountability for information sharing, wider access to necessary databases, and the professionalization of analysis and information sharing.

It is probably true that these issues will never be perfectly addressed, but we must keep in mind that our war on terror is a decades-long effort to defeat a dedicated enemy. Anyone who doubts that should remember that today is also the anniversary of the first World Trade Center bombing in 1993 that killed 6 and wounded 1,000 people. We must continue to make every possible improvement to our homeland security—including intelligence and information sharing.

I would like to welcome Mr. Sena, Chief Beary, and Dr. Alexander. The input from your respective associations is critical to the subcommittee's understanding of progress made to improve the amount and quality of information shared between Federal, State, and local law enforcement and of remaining challenges.

I look forward to the panel's update and would like to thank our distinguished panel of witnesses in advance.

Mr. KING. Now I am pleased to recognize the Ranking Minority Member of the subcommittee, the gentleman from the other end of New York, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman, for holding this hearing today.

I would like to thank the witnesses for traveling here to be with us today.

In consideration of time and in deference to our panel of witnesses, I will submit my opening statement for the record. So we can proceed with our panel.

[The statement of Ranking Member Higgins follows:]

STATEMENT OF RANKING MEMBER BRIAN HIGGINS

FEBRUARY 26, 2015

I would like to thank the Chairman for holding today's hearing. I would also like to thank the witnesses for traveling to be here with us today.

Information sharing is an integral part of our Nation's security.

It has been both said and proven time and time again: Information sharing leads to better and more informed decision making and ultimately leads to a safer environment for everyone.

The idea of information sharing between Federal, State, local law enforcement has been engrained in our homeland security policies since September 11, 2001.

Since that date, the Federal Government has developed many initiatives expanding efforts at information sharing with State and local partners.

While we now have many more partnerships, such as Fusion Centers and the National Joint Terrorism Task Force, our work in this area is not complete.

The ultimate goal of intelligence is to provide accurate analysis in a timely manner.

Complacency is unacceptable.

There must be a balance that eliminates unnecessary redundancy while maintaining the competitive environment for sharing information.

That is the challenge for law enforcement officials.

Congress must do our part as well.

As we sit here today, none of us know for sure what will happen with DHS funding within the next hour or tomorrow.

That type of uncertainty will trickle down and impact all of the issues we have gathered to discuss today.

Information sharing should also be tailored, when practicable, to ensure that each law enforcement entity is getting the best and most useful information.

The true value of information sharing will never be realized if State and locals cannot respond and protect their own communities.

Intelligence officers and analysts must integrate themselves into the jurisdictions and communities they are assigned, in order to know and understand geographical and cultural sensitivities.

Also, we need the agencies as a whole, especially the DHS components, to be willing participants and provide the necessary support to assist State and locals.

So while this topic is not new, it is an issue that we cannot afford to ignore.

I recognize the position our witnesses are put in today, essentially being asked to critique an agency that is their partner and funding source, but I want to assure you that this type of open dialogue is beneficial to all parties involved.

Once Congress can understand the challenges you face, we can work together to craft effective solutions.

Again, I welcome you all, and I look forward to your testimony.

Mr. KING. Members of the subcommittee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

FEBRUARY 26, 2015

Information sharing is critical to our Nation's security. As I have said before, information sharing in the intelligence community is an evolving puzzle of pieces. Officials must gather and analyze these pieces of diverse and sometimes inconsistent information to create a single coherent picture. That picture is then shared with other officials, all of whom are working to keep our Nation safe.

Since the 9/11 attacks, both Congress and the Executive branch have addressed the systematic problems caused by both the failure to analyze and the failure to share information between law enforcement officials and first responders. Some of those failures have been remedied by simply requiring agencies to talk to each other and their colleagues within State, local, and Tribal governments.

As easy as it may sound, this has not been a simple process. Many agencies had cultures which promoted stove-piped information and prevented external sharing. Those agencies have since undergone a cultural shift. Some are still struggling with shifting from a need-to-know culture to a need-to-share environment. However, because we know the price of failure, Congress must continue to insist upon and oversee this transition.

Our insistence must be shown by not only pushing for better information sharing, but also by providing the tools necessary to achieve a high and concise level of sharing. Congress and the Federal Government must do more to assure that State and local fusion centers can fully assist in the homeland security mission. These centers form the backbone of an information-sharing infrastructure. While DHS and FBI are helping fusion centers to build analytical and operational capabilities, they must also help these centers measure and increase their homeland security value.

State and local fusion center partners can help by identifying and documenting the specific programs and activities that are most important for executing the missions for the State and local governments. This kind of guidance has several mutual benefits for all parties involved.

It will increase the effectiveness of each fusion center, will assure that the Federal tax dollar is being spent wisely, and most importantly, it will provide clear rules that will ensure that civil rights and civil liberties are safeguarded.

State and local fusion centers and their partners must get the assistance they need to be helpful in doing their part to keep this Nation safe. Yet, as we sit here today, there are those who believe we should not fund the Department of Homeland Security. It seems intellectually dishonest to charge our witnesses here today and their partners within DHS with doing work we are not even willing to fund. As we consider the challenges we face, I look forward to hearing the assessment of each of our witnesses about the challenges that lie ahead for the information-sharing environment.

Mr. KING. We are pleased to have a very distinguished panel of witnesses before us today on this vital topic.

Mike Sena is the director of Northern California Regional Intelligence Center, the Fusion Center for the San Francisco Bay area. He also currently serves as president of the National Fusion Center Association. Mr. Sena has testified before this committee on numerous occasions and has been a great resource to the committee over the past several years.

Chief Richard Beary is president of the International Association of Chiefs of Police. Chief Beary served for 30 years as a law enforcement officer in Florida, including as chief of police for the city of Lake Mary. In 2007, he was appointed chief of police for the University of Central Florida. He has twice been awarded the Medal of Valor for performance undertaken at great personal hazard.

Dr. Cedric L. Alexander is the national president for the National Organization of Black Law Enforcement Executives. He also serves as the chief of police for the DeKalb County. Previously, Dr. Alexander was the Federal security director for the Transportation Security Administration at Dallas/Fort Worth International Airport. He also served as deputy commissioner of the New York State Division of Criminal Justice Services, chief of police in Rochester Police Department, and held several leadership roles at the University of Rochester Department of Psychiatry in New York. He began his law enforcement career in 1977 and also served with the Miami-Dade Police Department and was a law enforcement officer in Florida for 15 years.

So with that, Mr. Sena, we will begin with you. Try to keep your statements to 5 minutes if you can. We are not going to be arbitrary. If you can try to do that, we will get more in that way. Okay? Thank you very much.

Mr. Sena.

STATEMENT OF MIKE SENA, PRESIDENT, NATIONAL FUSION CENTER ASSOCIATION

Mr. SENA. Mr. Chairman, on behalf of the National Fusion Center Association, I want to thank you for inviting me today.

Our public safety and law enforcement and intelligence committees have made dramatic progress in analyzing and sharing homeland security threat information. We are sharing more information more effectively than ever before. The National network of fusion centers is playing a key role in that. One indicator of that success is in the 1-year period between August 2013 and July 2014, suspicious activity reports submitted by fusion centers supported or resulted in the initiation of 238 FBI investigations. We are providing our Federal partners with relevant information that would otherwise be difficult or impossible for them to obtain.

The National network of fusion centers can provide more comprehensive access to State and local information to support counterterrorism and other criminal investigations. No other structure can enable faster or more accurate situational awareness across State and local jurisdictions. No other construct can ensure a consistent Nation-wide focus on enforcing policies that affect citizens' privacy, civil rights, and civil liberties. While we have done great work, we know a lot more needs to be accomplished. I would like to highlight four issues as the committee considers how to help close information-sharing gaps.

First, this committee released a well-researched, thoughtful, and constructive report on fusion centers in July 2013. It accomplished and acknowledged that the National network is a National asset that needs to realize its full potential to help secure the homeland. The report's most important recommendation was calling for the development of a National strategy to guide the network of fusion centers into a more advanced and cohesive enterprise. I am happy to report we took that recommendation to heart, formed a multidisciplinary working group of State and local public safety stakeholders and the National Governors Association, and consulted closely with our Federal partners at DHS I&A, the FBI, the program manager for the Information Sharing Environment, and others.

In July 2014, we published a National Strategy for the National Network of Fusion Centers which can be found on our association's website. This committee's report also recommended that the Federal Government develop an engagement strategy for working with fusion centers, which was finalized late last year. We are now collaborating on a dozen shared priority initiatives. Our commitment to improving information sharing is as rock-solid today as it was on September 12, 2001.

Second, adequate funding for fusion centers is essential. Each fusion center is owned and operated by State and local governments, not the Federal Government. That is exactly the way it should be. State and local governments provide more than half of all the funding for fusion centers. But the Federal contribution of funding through FEMA preparedness grants remains critical to advancing information sharing. The law requires that each State allocate 25 percent of its UASI and SHSGP funding to law enforcement terrorism prevention activities, including support for fusion centers. We have been concerned that this requirement is not being met in some areas.

In fact, a GAO report from November 2014 found that States inaccurately categorized about $60 million in grant-funded projects in

fiscal year 2012 as related to fusion centers when, in fact, those funds did not support fusion centers. To fix this, we would suggest that a Governor-designated State law enforcement executive be required to review the LETP portions of each State's grant allocation plans to make sure those funds truly support prevention activities as the law intends. If inadequate funding weakens one node in our National network, then we have a new gap in homeland security information sharing. Congress should make sure that does not happen.

Third, enhancing amicable collaboration in the field will prompt more high-impact information sharing across fusion centers. Part of enhancing amicable collaboration is ensuring that there is a DHS I&A intelligence professional in every fusion center. That person must have the authority to collect and share raw information, execute joint production, and effectively share information across all classification levels. This person has to have release authority for certain types of information. Because without appropriate release authority, there is a gap in information sharing.

We were concerned to learn that last year's Intelligence Authorization Act forced a reduction in I&A's field resources. Despite the impact of that policy decision on State and local law enforcement and fusion centers, we were not consulted by the intelligence committees. Reducing personnel in the field reduces analytical collaboration and creates new information-sharing gaps. We cannot let that happen.

Fourth, to enable joint product development, which is a key advantage of Federal engagement in fusion centers, Congress should ensure that adequate resources support deployment of collaboration and communications platforms and technologies across fusion centers and our Federal, State, and local partners. Secure sharing of information at the Sensitive but Unclassified level is a key to Federal partners getting greatest benefit from State and local information and ensuring that State and local leaders have the best information to make decisions about protecting their citizens.

I would like to thank you again for your commitment on this issue, Mr. Chairman. Information sharing matters every single day for those of us who are sworn to protect our citizens.

I look forward to your questions.

[The prepared statement of Mr. Sena follows:]

PREPARED STATEMENT OF MIKE SENA

FEBRUARY 26, 2015

Mr. Chairman, thank you for inviting me to testify on this important topic. My name is Mike Sena and I am testifying today in my capacity as president of the National Fusion Center Association (NFCA). I am currently the director of the Northern California Regional Intelligence Center (NCRIC), one of the 78 fusion centers in the National Network of Fusion Centers (National Network). Fusion centers bring together law enforcement, public safety, fire service, emergency response, public health, protection of critical infrastructure and key resources (CIKR), and private-sector security personnel to understand local implications of National intelligence, as well as add State and local information and context to Federal intelligence, thus enabling local, State, and Federal officials to better protect our communities.

Up front, I will say emphatically that our public safety, law enforcement, and intelligence communities have made dramatic progress over the past decade in analyzing and sharing information related to threats to the homeland. Information

sharing on these threats—both criminal and terrorist in nature—has become routine. Relationships have been developed and sustained across State and agency lines that are helping investigators solve crimes and prevent further crimes. Technology has given us better tools to support the process of analyzing and sharing threat information, and enhancing situational awareness during critical incidents.

An essential part of the improvement is the Federal support provided to fusion centers. That Federal support includes assignment of intelligence officers and analysts, technical assistance, training and exercises, linkage to key information systems, grant funding, and security clearances. These tools add critical value to the resources committed by State and local governments to make the National Network a foundation of homeland security information sharing. Over the past several years, the State and local share of budget resources allocated to fusion centers has grown substantially—State and local governments provided over half of all funding for fusion centers in fiscal year 2014.

Federal funding support through FEMA Preparedness Grants—SHSGP and UASI—remains critically important. The NFCA has joined other law enforcement associations on a letter to Congress urging that the Law Enforcement Terrorism Prevention Activities (LETP) requirement in the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–53) be strengthened. The law requires that 25% of SHSGP and UASI funding be used for "law enforcement terrorism prevention activities" and specifies some of those types of activities including support for fusion centers. While States have latitude to allocate funding according to risk and priorities, we agree with the intent of the 2007 law and believe that terrorism prevention activities should be constant priorities, especially as grant funds have declined over the past 5 years. The Government Accountability Office (GAO) found in its November 2014 report on information sharing and fusion centers that in 2012 States inaccurately categorized about $60 million in projects as "related to fusion centers" when in fact those funds did not support fusion centers. As we have suggested in our letter to Congress, requiring a Governor-designated State law enforcement executive to review the LETP portion of grant plans would help to ensure those funds truly support terrorism prevention activities.

Thanks to fusion centers we are sharing more information more effectively than ever before. This is happening despite the fact that no single entity has the authority to enforce effective information-sharing practices. Because of the decentralized nature of public safety in America, policies on sharing information cannot be dictated by any one organization. Common policies and practices have been developed by consensus through multi-lateral and interagency policy bodies—including the Global Justice Information Sharing Initiative (Global) and the Criminal Intelligence Coordinating Council (CICC) and must be continually reinforced through day-to-day engagements between Federal, State, and local partners. As you might imagine, this is extraordinarily difficult to achieve in practice, but we have made excellent progress and are continuing to build on that progress.

Even as we pat ourselves on the back, we must recognize that we are not where we need to be—or where our citizens expect us to be. That is not because of a lack of will. I have not encountered anyone at the Federal, State, or local levels who does not share the same goal of protecting our communities. Rather, it is mainly due to policy and turf challenges that require persistent effort to overcome. To that end, as president of the National Fusion Center Association I am in discussions every day with my fusion center colleagues, our Federal partners, our counterparts in other public safety disciplines, and with private-sector stakeholders to develop stronger processes and build stronger relationships. With the active support of this committee and the rest of Congress and our State legislatures, we must continue our commitment to a true Nation-wide information-sharing enterprise with the National Network of Fusion Centers as a centerpiece and build on the success we have achieved to date.

In July of 2013, this committee released a report titled "Majority Staff Report on the National Network of Fusion Centers." It reflected the painstaking work of several committee staff who visited more than 30 fusion centers across the country and met with dozens of Federal, State, and local fusion center partners. This level of investigative effort and analytical rigor contrasts with a 2012 report from the Permanent Subcommittee on Investigations under the Senate Homeland Security and Governmental Affairs Committee that was highly critical of fusion centers. Among the key findings of this committee's 2013 report was an acknowledgement that "the National Network is a National asset that needs to realize its full potential to help secure the Homeland." The report also recognized the direct impact of fusion center information sharing on terrorism investigations by noting that according to information provided by the FBI and DOJ, between December 2008 and December 2012, "176 SARs [suspicious activity reports] entered by fusion centers into the eGuardian

or Shared Spaces SAR databases [. . .] resulted in the FBI opening new terrorism investigations." "Additionally, 289 Terrorist Watchlist encounters reported by fusion centers enhanced existing FBI cases." The level of productivity mentioned in the report has increased since it was published. In the 1-year period between August 2013 and July 2014, 238 SARs submitted by fusion centers supported FBI investigations. When I hear people question the value of fusion centers to Federal counterterrorism efforts, I point them directly to these statistics. The value of the National Network is crystal clear.

From the NFCA's perspective, the most important recommendation in this committee's 2013 report was calling for the development of a National Strategy for the National Network of Fusion Centers. I am pleased to report that we took your recommendation to heart, formed a working group comprised of law enforcement and public safety groups, emergency management, and the National Governors Association, and dedicated hundreds of hours to developing that strategy. The resulting work—the National Strategy for the National Network of Fusion Centers 2014–2017—was published in July of 2014. The strategy can be found at our website: *www.nfcausa.org*.

The NFCA took the lead role in organizing the strategy development effort. We led a team that included representatives from the International Association of Chiefs of Police (IACP), the National Sheriffs Association (NSA), the Major Cities Chiefs Police Association (MCCA), the Major County Sheriffs Association (MCSA), the Association of State Criminal Investigative Agencies (ASCIA), the National Governors Association (NGA), the fire service, the Regional Information Sharing Systems (RISS), the High-Intensity Drug Trafficking Areas (HIDTA) Investigative Support Centers, and David Paulison, former administrator of FEMA. Throughout the process, we consulted with our Federal partners at Department of Homeland Security (DHS), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Office of the Program Manager for the Information Sharing Environment (PM–ISE), the Office of the Director of National Intelligence (ODNI), and other field-based information-sharing partners. We worked with all of these partners through the Criminal Intelligence Coordinating Council (CICC).

The NFCA led the strategy development effort and a dedicated team skillfully coordinated the tedious effort to solicit and organize stakeholder inputs, drafting, and feedback. During the months we spent working on this effort, our development team could sense progress being made in identifying barriers that need to be overcome and creating new consensus around information sharing and analytical collaboration. The resulting strategy objectives and priority initiatives are now driving efforts to improve analysis and sharing, including in areas related to recommendations made by this committee's 2013 report. It is an ambitious strategy—we specified 37 initiatives that advance each of the four goals—yet we are optimistic that progress will become evident soon.

The strategy development process was just the beginning. While several strategy initiatives are already well underway, we are in process of developing an implementation plan that will prioritizes our actions through 2017 to achieve objectives under the strategy.

In addition, this committee's 2013 report called for a Federal strategy to support the National Network of Fusion Centers. Late last year we worked with DHS Intelligence & Analysis, the FBI, and other members of the Information Sharing and Access Interagency Policy Committee (ISA–IPC—the Federal interagency forum that oversees the planning and implementation of the Information-Sharing Environment) to support their development of an "Engagement Strategy" which is fully complementary with our strategy. Working together with our Federal partners, we identified a dozen initiatives that will be joint priorities over the next several years. For the first time, there is a clear Federal strategy that directly supports the State and locally-driven National Network.

Central to that support our on-going engagement with the DHS Office of Intelligence and Analysis. The National Network continually relies on our partners at I&A. The support provided by I&A personnel assigned to fusion centers is critically important. I&A Under Secretary General Frank Taylor and his staff have invested considerable time and effort in determining the best path forward for I&A's deployment of personnel in the field. They have regularly interacted with the NFCA and sought our input along with that of our State and local partners. Unfortunately, the Intelligence Authorization Act of 2014 constrained I&A's choices through limiting language in the Classified annex to the bill—a move that was made by the intelligence committees without consulting any fusion center directors or other State and local stakeholders impacted by the decision.

The impact of the new I&A field deployment plan won't be known until the changes are in place, but there is concern across the National Network about what

it will mean for fusion center connectivity to certain Classified systems and information that is essential to sharing threat intelligence with State and local law enforcement and other public safety partners. One of the primary objectives in the fusion center strategy (and in the BENS report) is enhancing analytical collaboration in the field. Limiting I&A presence in fusion centers threatens to inhibit that collaboration.

Every fusion center should have an I&A intelligence professional with the authority to collect and share raw information to include release authority, execute joint production, and effectively share information across all classification levels. Decisions regarding the appropriate type of intelligence professional for each fusion center should be the result of discussions between those State and regional fusion centers and I&A.

A common misconception that is often repeated in news stories and in advocacy papers is that fusion centers are "DHS fusion centers". This is simply not true: DHS does not exercise operational control of any fusion center. State and local governments own and operate fusion centers, and we collaborate closely with DHS, the Department of Justice, and other Federal agencies to facilitate wider analysis and sharing of threat information.

Each Governor designates a primary fusion center in each State. Together with other recognized fusion centers, these centers comprise the National Network of Fusion Centers. The National network is a decentralized, distributed network of analysts, public safety partners, and in a growing number of cases CIKR and private-sector partners. Most centers have representation from DHS and in some cases the FBI and other Federal investigative agencies. This organizational structure allows for each center to be directed according to the priorities of its agency sponsor, while maintaining a direct upward and downward link to National counterterrorism intelligence. This is squarely in line with what the 9/11 Commission called for in its report.

Since fusion centers are owned and operated by State and local entities, there is wide variation among the centers in terms of budget and capabilities. Fusion center priorities in Tennessee are different from priorities in New York State and from our center in the San Francisco Bay area. The interests are different because their populations are different, and the fact that they are free to address the issues they feel need addressing is a strength of the National Network of Fusion Centers.

The first of two common threads through all the centers—and the key Federal interest—is a link to Federal partners and to each other through information-sharing mechanisms. The Critical Operational Capabilities (COCs) that are maintained (and measured through an annual assessment process facilitated by DHS) in each center ensure the centers are ready and able to support homeland security missions regardless of their local priorities.

Of central importance is the access each center has to local, regional, and State sources of information—public safety records, criminal intelligence databases, and personal relationships across communities—that allow the center to add local and regional context to National intelligence, as well as provide information and value-added intelligence to support counterterrorism and other criminal investigations that would otherwise be difficult or unlikely for lead Federal investigative agencies to obtain. Also critically important from the National perspective is that each fusion center has methods of distribution across local, regional, and State-wide technical and personal networks that Federal investigative and intelligence agencies could not possibly build or maintain.

Thus, the dual-value proposition of the National Network of Fusion Centers is that no other organizational structure can provide faster or more efficient access to State and local information that may support National counterterrorism investigations, or enable faster or more efficient situational awareness across relevant jurisdictions. Refining the processes that allow this to happen is an on-going priority and is at the heart of the strategy we are executing today.

The second of the two common threads through all centers is a focus on vigilantly protecting against infringements of citizens' privacy, civil liberties, and civil rights. Fusion centers are part of a much larger domestic security enterprise whose mission is the protection of the American people—including our ability to exercise Constitutional rights and be free from unwarranted Government intrusions in our lives. Privacy protections are not an afterthought for the NFCA, the National Network, or our Federal, State, and local partners. In fact, the first order of business last year during the development process of our National strategy was to address privacy, civil liberties, and civil rights. That is why it is literally Goal No. 1 in the strategy: "Uphold public confidence through the safeguarding of information and the protection of the person and the privacy, civil rights, and civil liberties of individuals."

All fusion centers have strong publicly-available privacy policies in place, we train our people on them, and we emphasize transparency. Privacy policies have been established across all 50 States and all operational fusion centers at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines. Training has occurred for more than 200,000 local, Tribal, State, and Federal front-line officers to identify and report suspicious activity in accord with the ISE Suspicious Activity Reporting (SAR) Functional Standard, and several thousand analysts have been trained in accord with vetting guidelines to ensure that ISE SARs are demonstrably behavior-based and their handling (retention, redress, and other related considerations) is fully compliant with privacy policies. The very first initiative in our strategy relates to training and education for law enforcement and public safety partners on fusion centers' role in the protection of privacy, civil rights, and civil liberties. The strategy's second initiative relates to conducting assessments on the impact of certain technologies on privacy, civil liberties, and civil rights of citizens, and developing policies to mitigate any impact prior to procurement. We look to the Technology Policy Framework published by the IACP in January of 2014 to support these efforts.

Measuring the impact of terrorism prevention activities is a continuing challenge across all sectors—including with fusion centers. However, fusion centers in particular have been subject to extensive and rigorous assessments in recent years. The purpose has been to ensure that gaps in critical operational capabilities of individual fusion centers are addressed to ensure they can be fully capable participants in the National Network.

There are quantitative measures like the number of SARs that are analyzed by fusion centers and shared with the FBI if they bear the indicators of terrorism-related activity. Those number in the hundreds. There are also quantitative measures like the number of "requests for information" that are generated and shared across the network of fusion centers. Those are also numerous. There are numbers of cases in which fusion centers provided critical information that enabled Federal partners to advance terrorism investigations. All of these measures indicate a high level of information sharing and analysis activity across all levels of Government and across jurisdictional lines. In other words, preparedness capability exists today that never existed in such a routine and organized fashion in the past. FEMA preparedness grants have played an essential role in the development and maturation of this capability.

Other measures are tougher to quantify, yet positive outcomes happen virtually every day in fusion centers across the country. There are hundreds of anecdotal fusion center "success stories." The vast majority of these successes relate to criminal incidents that have nothing to do with terrorism, but have everything to do with "connecting the dots" through analytical efforts and sharing information to support decision makers and front-line investigators to protect communities.

The imperative to better share information vertically and horizontally in support of terrorism prevention and counterterrorism investigations undergirds the recommendations made by Business Executives for National Security (BENS) in its report on domestic security published in 2014. I believe the BENS report contains several very helpful recommendations and I agree with many of them. In particular, establishing a domestic threat framework for assessing and prioritizing threats and information needs; enhancing intelligence analyst capabilities at all levels and establishment of standardized training for intelligence personnel; and improving the flow of information related to counterterrorism investigations to State and local partners in real time would improve our overall domestic security posture.

Some of the assumptions of the BENS report, however are not fully reflective of the role of State and local law enforcement and public safety—particularly fusion centers—in supporting National counterterrorism efforts. Counterterrorism analysis and information sharing functions are components of the fusion center mission but they are not—and they should be—the sole components. That is because our fusion centers report to Governors, State law enforcement executives, county, and municipal public safety leadership. They do not report to the Federal Government, nor should they. The vast majority of fusion centers are "all-crimes" centers, which reflects the fact that criminal intelligence analysis, data sources, interagency relationships, and information-sharing capabilities resident in the centers are useful for all types of investigations—not just terrorism. While the Federal interest in fusion centers relates primarily to their ability to contribute to counterterrorism efforts, the reality is that the fusion process is effective for any public safety effort. Whether the crime is terrorism, child abduction, gang violence, or auto theft, the fusion process maximizes efforts to prevent, deter, or investigate the crime. Institutionalized collaboration through information sharing and co-location is effective no matter the nature of the crime. Our Federal partners benefit from the all-crimes approach be-

cause it amounts to "drilling" on real-world scenarios using the fusion center critical operational capabilities every day. When a terrorism threat emerges, fusion center participants and customers "know the drill."

The BENS report recommends the establishment of regional fusion centers on top of what we have today. I fully understand the intent of that recommendation, but I believe it could have a negative effect on the ability of fusion centers in those areas to accomplish their core missions in support of chiefs, sheriffs, State investigative agencies, State police agencies, and Governors. The fact is that fusion centers are already performing the functions that are called for in the BENS report, and with the new National Strategy for the National Network of Fusion Centers being implemented, I am optimistic that the support provided by the National Network to counterterrorism investigative partners will increase.

I am still often asked whether fusion centers duplicate the FBI's JTTFs. This committee should understand that JTTFs are Federally-run investigative bodies that support the FBI's unique mission to investigate terrorism threats in this country. Fusion centers play a much different role; they're not only information-sharing hubs in States and metropolitan regions. Fusion centers are where we train a cadre of terrorism liaison officers (TLOs), including police officers, firefighters, EMS workers, and our private-sector partners on indicators and warnings of terrorism. Fusion centers have the ability to catalogue critical infrastructure in each State and region and analyze incoming suspicious activity reports (SARs) against the National threat picture and against what we know about our critical infrastructure. We have the ability to then rapidly share information and intelligence among the entire National Network and with the FBI. But often that SAR information has no nexus to terrorism. It's about drug dealing or gang activity or firearms trafficking or mortgage fraud. So the all-crimes approach mentioned above gives us the ability to analyze that information and funnel it to the right place. And we know that, sometimes, information that at first blush appears to be criminal in nature—the Torrance, California gas station robberies, the smuggling of cigarettes in North Carolina, the sale of pseudoephedrine in California—actually is linked to terrorist activity.

It does not make sense to try to separate crime and terror in our daily work of analyzing threat information and criminal activity. We have to knock that wall down. If we're going to continue to improve, we have to understand that the sharing of information makes communities safer. Our ultimate goal is to prevent terrorism. But in every community across the country there are violent crimes that terrorize neighborhoods and families and affect lives and businesses every day. Fusion centers are uniquely situated to do things that JTTFs or no other program can do. We can bring together disparate resources, data sets, analytical perspectives, and personnel in order to analyze and share information on terror, crime, or other threats to public safety. We can make sure that JTTFs get the information they need, but that the DEA and HSI and chiefs and sheriffs and governors get the information they need about non-terrorism public safety threats as well.

Fusion centers are increasingly contributing analytical and information-sharing efforts to address threats in the cyber realm against law enforcement, other Government agencies, and the private sector. Last year the NFCA created a Cyber Threat Intelligence Subcommittee to organize fusion center engagement in multi-stakeholder efforts to clarify "lanes in the road" for cyber threat analysis and information sharing, and to support efforts across the National Network to build cyber threat analysis and sharing capabilities. As this committee knows, cyber threats come in all sizes and shapes. Individual citizens have their identities stolen and personal credit wiped out, while Government agencies and companies face threats to their daily operations. An increasing number of fusion centers have analytical personnel that are trained in cyber threat analysis. And an increasing number of fusion centers are being asked to support cyber threat information sharing.

One recent example of the role fusion centers are playing in the cyber threat domain was in late November and early December 2014 during the events in Ferguson, Missouri. Cyber threats and attacks directed at public safety agencies had a significant impact during that period. To facilitate situational awareness and share information across agencies about these threats, the NFCA Cyber Intelligence Network (CIN) hosted a virtual situational awareness room (referred to as CINAWARE) on the Homeland Security Information Network (HSIN). More than 350 individuals from fusion centers and other Federal, State, and local agencies around the country participated in the CINAWARE room between mid-November and early December, with an average of 50 to 90 users in the room at any given time each day. The room was supported 24/7 including overnight support from the Multi-State Information Sharing and Analysis Center (MSISAC). During that period, there were more than 250 queries submitted and answered via the room, enabling rapid sharing of information with decision makers. Leaders in State, local, and

Federal agencies were being briefed on the information from the CINAWARE room. That level of threat information sharing was impossible only a few years ago, yet it is becoming essential.

Mr. Chairman, on behalf of the National Fusion Center Association, thank you for inviting me to testify today. I commend you for your focus on this topic. It should continue to be a high priority for this committee and for all of Congress—especially in this dynamic threat environment. Please know that my colleagues across the country together with all of our partners at the State, local, and Federal levels are working hard every day to get better and live up to the expectations of our citizens. We look forward to continuing to work closely with the committee to help meet those expectations.

Mr. KING. Thank you, Mr. Sena.

Now Chief Beary.

STATEMENT OF RICHARD BEARY, PRESIDENT, INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Chief BEARY. Good afternoon, Chairman King, and Members of the subcommittee.

I am pleased to be here today on behalf of the International Association of Chiefs and Police. The IACP is the world's largest association of law enforcement leaders, with more than 22,000 members in 98 different countries. For over 120 years, the IACP has been launching internationally-acclaimed programs, speaking out on behalf of law enforcement, conducting ground-breaking research, and providing exemplary programs and services to the law enforcement profession around the globe.

The importance of information sharing. The 9/11 terrorist attacks taught us that information exchange between local, State, Tribal, and Federal law enforcement and Homeland Security partners is absolutely critical to ensuring the safety and security of our Nation and the communities that we serve. As the 9/11 commission properly noted, the lack of effective information and intelligence sharing amongst Federal, State, Tribal, and local law enforcement agencies was a major handicap in our Nation's homeland security efforts.

However, due to the hard work of our Nation's law enforcement professionals, advances in technology, and increased partnership and trust between Federal, State, and local, we have improved this tremendously in the last 13 years that have passed since 9/11. As a result, our capacity to identify, investigate, prevent, and respond to these events has enhanced significantly.

Collaboration, information, and intelligence sharing amongst all the partner agencies needs to continue. Although we have made great strides, our work is certainly not done. For this reason, the IACP continues to work closely with its partners, making sure that communicating and the processing of information is as easy and as efficient as possible.

Through a range of efforts, from clarifying how and to whom one should report suspicious activities, and implementing technological enhancements, these initiatives aim to improve the ability on all levels of law enforcement to combat the increasingly diverse threats facing the United States. These efforts include the work of the Unified Messaging Task Force, the National SAR Initiative, the ISE Shared Space, N–Dex, E-Guardian, the National Network of Fusion Centers, and the campaign "See something, say something." All of these efforts are designed to enhance law enforcement's ability to quickly and effectively share information among and between

the essential partners at Federal, State, local, and Tribal. While there are still areas that individuals within the law enforcement community can improve, there has been substantial movement in the right direction.

Now, I have had the opportunity to review the report of the Business Executives for National Security, BENS, and I am pleased to say that, in general, the recommendations contained within the report are consistent with the work and recommendations the IACP has done over the last 14 years. In particular, I am very pleased that the report recognizes the essential and critical role that must be played by State, local, and Tribal law enforcement officers in building and sustaining an effective Nation-wide criminal information- and intelligence-sharing system.

The IACP strongly agrees with the report's recommendation that ownership and management of the integrated fusion centers should continue to be managed by State and local stakeholders with Federal entities supporting those centers. However, while the report appropriately recognizes the need for robust information-sharing capability in major urban centers, we cannot and must not overlook the importance of fully engaging agencies in non-urban areas.

Experience has repeatedly shown us that while attacks take place in densely-populated areas, planning and preparation for these crimes often occur in small or rural communities. Failure to ensure that these agencies are actively engaged in our National information and intelligence-gathering efforts, undermines our efforts to protect the public.

I want to talk just briefly about going dark. Of course, the information law enforcement is able to share, we first have to have the ability to obtain it. Unfortunately, those of us who are charged with protecting the public aren't always able to access the evidence we need to prosecute crime and prevent terrorism, even though we have a lawful authority to do so.

We have the legal authority to intercept and access communications and information pursuant to the appropriate legal processes, but we lack the technology to do so. The law has not kept pace with technology. This disconnect has created a significant public safety problem which is often referred to as going dark. In response to this critical going dark issue, the IACP 2 weeks ago held a summit to explore operational, technological, and policy changes that need to be made while ensuring that civil rights and civil liberties are protected. It is important to note that law enforcement is not seeking broad, new law enforcement or surveillance capabilities, just currently trying to stay and be able to gather the evidence that the Constitution and court orders allow us to do.

These technological issues, such as encryption capabilities that are being built in new digital devices by companies such as Apple and Google, while we have the legal authority, we do not have the technological capability to get that data. There are legal issues, policy issues. The Communications Assistance for Law Enforcement, CALEA, needs to be changed to incorporate these new communication technologies. Critical investigations increasingly rely on digital evidence lawfully captured from smart phones, tablets, and other communications devices. Our inability to access this data, either because we cannot break the encryption algorithm resident on the

device or because the device does not fall under CALEA or the developer has not built the access route, means that lives may well be at risk or lost and those guilty parties may remain free because we do not have the capability.

So, on behalf of the IACP, thank you for allowing us this opportunity to be before you today. We look forward to taking your questions.

Thank you.

[The prepared statement of Chief Beary follows:]

PREPARED STATEMENT OF RICHARD BEARY

FEBRUARY 26, 2015

Good afternoon Chairman King and Members of the subcommittee: I am pleased to be here today on behalf of the International Association of Chiefs of Police.

The IACP is the world's largest association of law enforcement leaders, with more than 22,000 members in 98 different countries. For over 120 years, the IACP has been launching internationally-acclaimed programs, speaking out on behalf of law enforcement, conducting ground-breaking research, and providing exemplary programs and services to the law enforcement profession around the globe.

IACP'S PAST EFFORTS

The IACP has a long history of commitment to information sharing. In 2002, the IACP convened the "National Summit of Criminal Intelligence Sharing".

The findings of this summit provided the groundwork for the adoption of the National Criminal Intelligence Sharing Plan and led to the creation of the Criminal Intelligence Coordinating Council. The Criminal Intelligence Coordinating Council (CICC), established in May 2004, is made up of members representing law enforcement and homeland security agencies from all levels of government and is an advocate for State, local, and Tribal law enforcement and their efforts to develop and share criminal intelligence for the purpose of promoting public safety and securing the Nation. The CICC operates at the policy level setting priorities, directing research, and preparing advisory recommendations.

In 2007, the IACP held a follow-up summit entitled "Criminal Intelligence Sharing: Measuring Success and Setting Goals for the Future". This summit reviewed the work that had been accomplished following the 2002 summit and identified remaining gaps and weaknesses in our National criminal information and intelligence-sharing framework.

Since the time, the IACP has worked closely with a wide array of Federal, State, local, and Tribal agencies on a number efforts to promote greater cooperation and collaboration.

IMPORTANCE OF INFORMATION SHARING

The 9/11 terrorist attacks taught us that information exchange between local, State, Tribal, and Federal law enforcement and homeland security partners is absolutely critical to ensuring the safety and security of our Nation and the communities we serve. As the 9/11 commission properly noted, the lack of effective information and intelligence sharing among Federal, State, Tribal, and local law enforcement agencies was a major handicap in our Nation's homeland security efforts.

However, due to the hard work of our Nation's law enforcement professionals, advances in technology, and increased partnership and trust between Federal, State, and local authorities our ability to share information has improved tremendously in the 13 years that have passed since 9/11. As a result, our capacity to identify, investigate, prevent, and respond to these events has enhanced significantly.

Collaboration, information, and intelligence sharing among Federal, State, Tribal, and local law enforcement agencies needs to continue. Although we have made great strides, our work is not done.

For this reason, the IACP continues to work closely with its Federal, State, and local partners to make the processes for communicating and sharing information as easy and efficient as possible. Through a range of efforts, from clarifying how and to whom one should report suspicious activity to and implementing technological enhancements for information-sharing systems, these initiatives aim to improve the ability of all levels of law enforcement to combat the increasingly diverse threats facing the United States.

These efforts include the work of the Unified Messaging Task Force; the National SAR Initiative; the ISE Shared Space; N–Dex; E-Guardian; the National Network of Fusion Centers and, "If you see something, say something,"

All of these efforts are designed to enhance law enforcement's ability to quickly and effectively share information among and between essential Federal, State, and local law enforcement partners. While there are still areas that individuals within the law enforcement community can improve, there has been substantial movement in the right direction.

BUSINESS EXECUTIVES FOR NATIONAL SECURITY REPORT

I have had the opportunity to review the report of the Business Executives for National Security (BENS) and I am pleased to say that, in general, the recommendations contained within the report are consistent with the work and recommendations of the IACP over the last 14 years. In particular, I am very pleased that the report recognizes the essential and critical role that must be played by State, local, and Tribal law enforcement officers in building and sustaining an effective, Nation-wide criminal information and intelligence-sharing system.

The IACP strongly agrees with the reports recommendation that ownership and management of the integrated fusion centers should continue to be managed by State and local stakeholders, with the Federal entities supporting and collaborating with their State and local counterparts through their counterterrorism and other domestic security efforts.

However, while the report appropriately recognizes the need for a robust information-sharing capability in major urban centers, we cannot, and must not, overlook the importance of fully engaging agencies in non-urban areas. Experience has repeatedly shown that while attacks may take place in densely-populated areas, planning and preparation for these crimes often occur in small or rural communities. Failure to ensure that these agencies are actively engaged in our National information- and intelligence-sharing efforts would greatly undermine our efforts.

GOING DARK

Of course, before law enforcement is able to share information and intelligence, it must first have the capability to obtain it. Unfortunately, those of us who are charged with protecting the public aren't always able to access the evidence we need to prosecute crime and prevent terrorism even though we have the lawful authority to do so. We have the legal authority to intercept and access communications and information pursuant to appropriate legal processes, but we lack the technological ability to do so.

The law hasn't kept pace with technology, and this disconnect has created a significant public safety problem, which is what we mean when we refer to "Going Dark."

In response to this critical issue, earlier this month the IACP held a "Going Dark" Summit to explore the technological, operational, and policy changes needed order to address these issues, while respecting the privacy interest, civil rights, and civil liberties of the public.

It is important to note that law enforcement is not seeking broad new surveillance capabilities above and beyond what is currently authorized by the U.S. Constitution or by lawful court orders, nor are we attempting to access or monitor the digital communications of all citizens. Rather, we are simply seeking the ability to lawfully access information that has been duly authorized by a court in the limited circumstances prescribed in specific court orders—information of potentially significant consequence for investigations of serious crimes and terrorism.

There are technological issues, such as the encryption capabilities that are being built in new digital devices, by such companies as Apple and Google, but there are also legal and policy issues, such as the Communications Assistance for Law Enforcement Act (CALEA), which needs to be changed to incorporate new communications technologies.

Critical investigations increasingly rely on digital evidence lawfully captured from smart phones, tablets, and other communications devices. Our inability to access this data, either because we cannot break the encryption algorithm resident in the device, or because the device does not fall under CALEA or the developer has not built the access route, means that lives may well be at risk or lost, and that guilty parties remain free.

We recognize the public's demand for privacy, and we respect the legal and Constitutional provisions that are designed to ensure civil rights and civil liberties of our citizens, but we must act to address these issues for our own safety and security.

In conclusion, terrorism prevention and protection of the American people can be achieved only when law enforcement works together, communicates effectively and consistently, and looks for solutions. We are committed to meeting this challenge and continue to work each day to ensure that we fulfill our mission of protecting the public.

Mr. KING. Thank you, Chief, for your testimony.

Dr. Alexander, you are recognized.

STATEMENT OF CEDRIC ALEXANDER, NATIONAL PRESIDENT, NATIONAL ORGANIZATION OF BLACK LAW ENFORCEMENT EXECUTIVES (NOBLE)

Mr. ALEXANDER. Thank you, sir.

Chairman King, Ranking Members Thompson and Higgins, and Members of the subcommittee, I bring you greeting on behalf of NOBLE and the executive board.

Again, my name is Dr. Cedric Alexander, the national president of NOBLE and currently public safety director in DeKalb County, Georgia. It is an honor to be here to participate as a witness in the House's hearing on what progress has been made to improve the amount and quality of information shared between Federal, State, and local law enforcement.

I want to acknowledge and thank Chairman King for holding this hearing and thank Ranking Members Higgins and Thompson for inviting me to participate. I speak to you from a perspective of a person who has been in law enforcement for over 37 years and also who has held a number of positions throughout the Federal, county, and State level in law enforcement across this country.

Information sharing among law enforcement agencies at the Federal, State, and local level has evolved in the years since 9/11. Today, local agencies regularly meet with State and Federal partners to facilitate the flow of information. In DeKalb County, our department has liaison offers embedded in ATF, the FBI, DEA, ICE, U.S. Marshals, and the Georgia Information Sharing Analysis Center, often refers to as GSAC.

Our experiences with these relationships have been exemplary. However, these relationships are personality-driven and sometimes not based on established systems. One of the most beneficial factors in developing and maintaining these relationships is the networking of individuals through meetings, task force exercises, investigations, and training.

Even with the abundance of cooperation with local, State, and Federal partners, there are areas for improvement. One of these areas, of course, is the lack of a centralized source of information. Currently the sources of information, of intelligence information available to law enforcement are decentralized in multiple websites and databases managed by different Federal and State agencies. Most of these sources are subject-specific repositories of information. Often this information does not cross-pollinate to other sources of information. This means that an agency seeking information must know where to look for the information, possess the proper clearances to access the information, and hold accounts to the specific source of information.

Federal and State agencies have strived to ensure that most local agencies have access to these sources. However, to further compound this issue, often intelligence information is Classified and

most agencies do not have personnel that possess the required security clearance. The process to obtain security clearance for local agents is costly and protracted. Beyond simply assessing the intelligence information, law enforcement requires software, technology, and training to standardize their capabilities with state-of-the-art equipment that will increase their total effectiveness.

In Georgia, a project to address these requirements was established. The project called the Georgia Terrorism Intelligence Project, often referred to as GTIP, was originally funded by a DHS grant and budgeted for $2.5 million in 2007 but was reduced to the current budget of $90,000. These cuts reduced GTIP budget to only 4 percent of its original budget. A continued commitment to fund GTIP would have aborted some of the other deficiencies that I am speaking about today.

Although the relationship between local, State, and Federal agencies has vastly improved, there are still instances of restraint in the sharing of information. To a degree, this is most likely to result of how most agencies' successes are measured. These instances are the exception and not the norm, but they do exist. Another area that has significant deficiencies in relationships with non-Governmental organizations and the private sector. With over 80 percent of our Nation's critical infrastructure being owned and protected by the private sector, it stands to reason that these partnerships are paramount to our National preparedness and law enforcement mandate.

Lastly, as we have seen in recent years, there is a emerging threat from cyberterrorism. Local law enforcement must play a role in detecting, deterring, and mitigating these threats. The intelligence-sharing relationship with local, State, and Federal law enforcement agencies, as well as relationships with NGOs and private sector will be key in combatting this threat. Local law enforcement will need tools, training, and, above all, the continued support of our Nation to succeed.

Very quickly, a couple of recommendations to address the gaps in accessing quality intelligence shared among State, local, and Federal law enforcement agencies. In prioritizing what is needed to move forward in the amount and quality of information shared between Federal, State, and local law enforcement, I recommend a centralized source of intelligence information. The first step will save time, prevent duplication of work, and standardize the quality intelligence information.

The Department of Homeland Security, Information Network is a move towards a centralized source of intelligence. However, it is not user-friendly and still lacks information found within other sources managed by other agencies. Further, the compartmentalization of information with HSIN is counterproductive to the sharing of information. To alleviate some of the compartmentalization of intelligence information and foster an environment of sharing of this information, the path of local agencies to acquire security clearances must be streamlined and supported by State and Federal partners. The need for these clearances at the local level cannot be understated.

Next, training is necessary so that the value of the intelligence is realized and where to go with it. Information is power. However,

the collection of information is useless if the value of it is not realized. Local, State, and Federal law enforcement must be able to develop intelligence and then know with whom to share the intelligence. Too often it can be said that the flow of intelligence information is one way, the local agencies to the State and Federal agencies. This must be addressed and, as we have experienced in DeKalb County, can be lessened with the fostering of relationships with agencies at all levels.

Finally, a commitment to fund these initiatives and further their effectiveness is the only way to ensure local, State, and Federal law enforcement will prevail in the current threat environment. Projects like GTIP are needed in every State. Every local law enforcement agency has a need to collect, analyze, and share intelligence information. They require the tools and funding to accomplish this mission.

As we have all witnessed in recent years, whether it was the Boston Marathon bombing, the Washington Naval Yard shootings, the Queens, New York hatchet attack or the terrorist attacks in Norway, Paris, Ottawa, and Copenhagen. Today, local law enforcement is essential in detecting, deterring, mitigating, and responding to these threats. The need for quality intelligence information is greater now than at any time in this country's history.

Thank you very much, sir.

[The prepared statement of Dr. Alexander follows:]

PREPARED STATEMENT OF CEDRIC ALEXANDER

FEBRUARY 26, 2015

Chairman King, Ranking Members Thompson and Higgins, and Members of the subcommittee, I bring you greetings on behalf of the executive board and members of the National Organization of Black Law Enforcement Executives—NOBLE.

My name is Dr. Cedric Alexander, national president of NOBLE, and deputy chief operating officer for public safety, DeKalb County, GA. It is an honor to be here today to participate as a witness in the House's hearing on "what progress has been made to improve the amount and quality of information shared between Federal, State, and local law enforcement". I want to acknowledge and thank Chairman King for holding this hearing and thank Ranking Member Higgins and Thompson for inviting me to participate.

I speak to you from the perspective of a person who has over 37 years of law enforcement experience and who has held positions at the highest levels both at the Federal, county, and city levels. In addition, I hold a Ph.D. in clinical psychology.

Information sharing among law enforcement agencies at the Federal, State, and local level has evolved in the years since 9/11. Today local agencies regularly meet with State and Federal partners to facilitate the flow of information. In DeKalb County, our police department has liaison officers embedded in the ATF, FBI, DEA, ICE, U.S. Marshals, and the GA Information Sharing Analysis Center (GISAC). Our experiences with these relationships have been exemplary. However, these relationships are personality-driven and not based on established systems. One of the most beneficial factors in developing and maintaining these relationships is the networking of individuals through meetings, task forces, exercises, investigations, and training.

Even with the abundance of cooperation with local, State, and Federal partners, there are areas for improvement. One of these areas is the lack of a centralized source of information. Currently the sources of intelligence information available to law enforcement are decentralized in multiple websites and databases managed by different Federal and State agencies. Most of these sources are subject-specific repositories of information. Often this information does not cross-pollinate to other sources of information. This means that an agency seeking information must know where to look for the information, possess the proper clearances to access the information, and hold accounts to the specific source of information.

Federal and State agencies have strived to ensure that most local agencies have access to these sources; however, to further compound this issue, often intelligence information is Classified and most agencies do not have personnel that possess the required security clearance. The process to obtain security clearances for local agencies is costly and protracted.

Beyond simply accessing intelligence information, local law enforcement requires software, technology, and training to standardize their capabilities with state-of-the-art equipment that will increase their total effectiveness. In Georgia a project to address these requirements was established. The project is called the Georgia Terrorism Intelligence Project (GTIP). GTIP was originally funded by a DHS grant that budgeted $2,500,000.00 in 2007 but was reduced to the current budget of $90,000.00. These cuts reduced GTIP's budget to only 4% of its original budget. A continued commitment to fund GTIP could have avoided some of the other deficiencies that I am speaking about today.

Although the relationship between local, State, and Federal agencies has vastly improved, there are still instances of restraint in the sharing of information. To a degree, this is most likely a result of how most agencies successes are measured. These instances are the exception and not the norm, but they do exist.

Another area that has significant deficiencies is the relationships with Non-Governmental Organizations (NGO) and the private sector. With over 80% of our Nation's critical infrastructure being owned and protected by the private sector, it stands to reason that these partnerships are paramount to our National preparedness and law enforcement mandate.

Lastly, as we have all seen in recent years there is an emerging threat from cyber terrorism. Local law enforcement must play a role in detecting, deterring, and mitigating these threats. The intelligence sharing and relationships with local, State, and Federal law enforcement agencies as well as relationships with NGOs and the private sector will be key in combating this threat. Local law enforcement will need tools, training, and above all the continued support of our Nation to succeed.

RECOMMENDATIONS TO ADDRESS THE GAPS IN ACCESSING QUALITY INTELLIGENCE SHARED AMONG LOCAL, STATE, AND FEDERAL LAW ENFORCEMENT AGENCIES

In prioritizing what is needed to move forward in the amount and quality of information shared between Federal, State, and local law enforcement, I recommend a centralized source of intelligence information. This first step will save time, prevent duplication of work, and standardize the quality of intelligence information. The Department of Homeland Security's Homeland Security Information Network (HSIN) is a move towards a centralized source of intelligence; however, it is not user-friendly and still lacks information found within other sources managed by other agencies. Further, the compartmentalization of information within HSIN is counterproductive to the sharing of information.

To alleviate some of the compartmentalization of intelligence information and foster an environment of sharing of this information, the path for local agencies to acquire security clearances must be streamlined and supported by State and Federal partners. The need for these clearances at the local level cannot be understated.

Next, training is necessary so that the value of the intelligence is realized and where to go with it. Information is power; however, the collection of information is useless if its value is not realized. Local, State, and Federal law enforcement must be able to develop intelligence and then know with whom to share the intelligence. Too often it can be said that the flow of intelligence information is one way, the local agencies to the State and Federal agencies. This must be addressed and as we have experienced in DeKalb County, can be lessened with the fostering of relationships with agencies at all levels.

Finally, a commitment to fund these initiatives and further their effectiveness is the only way to ensure local, State, and Federal law enforcement will prevail in the current threat environment. Projects like GTIP are needed in every State. Every local law enforcement agency has a need to collect, analyze, and share intelligence information. They require the tools and funding to accomplish this mission.

As we have all witnessed in recent years, whether it was the Boston Marathon bombings, the Washington Naval Yard shootings, the Queens New York hatchet attack or the terrorist attacks in Norway, Paris, Ottawa, and Copenhagen; today local law enforcement is essential in detecting, deterring, mitigating, and responding to these threats. The need for quality intelligence information is greater now than at any time in our Nation's history.

By implementing these recommendations on centralization, training, and funding, we believe that real progress can be made in improving not just the quantity but also the quality of intelligence information shared between local, State, and Federal

law enforcement. This would greatly improve the Nation's preparedness and overall security. I thank the subcommittee for the opportunity to testify and I would be happy to answer any questions.

Mr. KING. Thank you, Dr. Alexander. I note that you have a doctorate in clinical psychology.

Mr. ALEXANDER. Yes, sir.

Mr. KING. If you ever want to leave law enforcement, you can have a full-time job down here.

Mr. ALEXANDER. Thank you very much.

Mr. KING. Now I would like to ask unanimous consent to allow our colleague, Congressman Langevin, to participate in the subcommittee hearing.

Without objection, so ordered.

My first question is we saw yesterday in New York the three alleged terrorists who were arrested, indicted. That was an investigation that was going on for some time. It involved potential attacks in New York itself, against the President of the United States, and also traveling overseas. So it involved multiple locations. In a case like that, what is your experience, what is your understanding of how that type of information is shared throughout the progress of the investigation with local law enforcement? I guess we will start with Mr. Sena.

Mr. SENA. The sharing of the information, that process, you know, there has been a lot of discussions after Boston, you know, what was the local police department's engagement, what was their involvement? Even in the JTTF, which does a fine job, but you have individual officers that are assigned. Their job is to do investigations. In these types of cases, the goal should be on the front end, the analysts, State and local enforcement using their analysts to review that information.

So in these types of cases, it should be, as the case is being addressed and progressed and assigned, that you have that State and local input from the start. That doesn't always happen, sir, I have to tell you that now, across the country. But there is so much that State and locals have to contribute that could and should be part of every process that, you know, every Federal agency, including the JTTF, does to support their investigations.

Mr. KING. Chief Beary, I will ask you the same question. Also, expand on what Mr. Sena said. I would think the local cop on the beat could well have intelligence on these individuals that the FBI may not be aware of. They may have sources. They may have background on them. So what is your experience or your understanding of how the information is shared and at what stage?

Chief BEARY. Well, Chairman, you are absolutely correct. Let's face it, 98 percent of the law enforcement work that gets done in this country is done by State and local officers, that cop on the beat that knows who belongs and who doesn't and recognizes that suspicious activity. That is one of the challenges that face us, is generally the Federal Government, the Federal agencies do not have access to those databases. Usually we find out after the fact that that person was stopped 15 times by the police, had been arrested previously, had a lot of different contacts. That is one of the places that absolutely needs to be improved across the spectrum. The data

is there. Sometimes the databases do not allow that information to transact.

While I have seen—certainly, especially, particularly involving the FBI, the communication has been the best that I have seen it in the last 37 years. Cedric and I started the same year. I see a vast improvement. I think that the data exchange has to happen quicker. They need access to that local data. Because the information is there. It is just tying it altogether and making sure it gets in the right hands.

Mr. KING. Dr. Alexander.

Mr. ALEXANDER. Yes, sir. Yes, you know, for years I have been saying in this profession that a lot of the source of information, particularly as it pertains to intelligence information that we are all are—and the things that have been happening in and around this country for the last number of years, a lot of this information, quite frankly, was or could have been discovered on the streets of many of our cities.

Because if we think about it, those who come into this country, infiltrate our communities, they are on the streets somewhere. Then their interactions on the street where, as you heard Chief Beary just mention, this is where our officers are. This is where they have contacts. Oftentimes, this is where they live. There is no greater source of intelligence gathering in my opinion and I have been doing this for 38 years this year. There is no greater source than information that is garnered from the streets and from our police officers.

One of the greatest challenges, and I think my colleagues here would agree, is that local funding that is needed for training in software, in all the latest technology that is out there that is available becomes very hard for local law enforcement to access or to gain. If we do gain that information, it is from our Federal partners oftentimes. They are great about sharing information.

However, what we do know is that the sooner we can gather information, collect information, and analyze that information, we also have an opportunity at a local level to disseminate that information both up, down, and across all law enforcement communities. I think it will prove to be of great benefit. But as you heard from my testimony is that funding has become a real critical issue for many of the local and State agencies that just don't have the money.

For an example, in my community alone, we don't even have the money right now to buy the basic software that will tell us, as relates to social media who is gathering where and when. That is basic information. Now, our Federal partners may obtain that information. But oftentimes by the time they get it, we would have known about it much earlier than by the time they get it to us, had we had the funding in order to do the things that we need to do at the local level.

Mr. KING. Thank you, Doctor.

The Ranking Member, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman. I am curious, the, you know, police work—police officers and police agencies take a lot of pride in what they do and expend a lot of resources to do what it is they do.

So I suspect that, you know, one of the reasons you had a problem in the first place is because of turf battles, you know, the reluctance to share information so as to potentially harm an on-going investigation that may be conducted by one agency. Thus, the success or failure of that investigation determines how that agency is viewed. To what extent do those turf battles still exist? I would also ask, you know, who has jurisdictional control over the fusion center? Does it differ with each one? Or is it based on, you know, the levels of Government, the local level being at the low end and then the Federal level being at the high end in terms of the control? Each of you I would ask that question of.

Mr. SENA. For the fusion centers, as far as who has the authority, each fusion center is designated by the Governor of each State. As far as, you know, who actually runs that, it depends on which location they are in, how they were formed. Some it is State police. Some it is Attorney General Offices from the State. Some it is local organizations. Mine is kind-of unusual because it started out within the HIDTA program, High-Intensity Drug Trafficking Area. So it depends on the mold of the jurisdiction of where they are located and who wants to take that kind of fiscal authority and leadership role.

As far as the turf battles, I can tell you that, you know, early on in my career, and we all saw this, where folks did not want to share their investigative information, there were systems put in place, like the Regional Information Sharing System, to bring law enforcement, to give them a place to put locations where they were going to do arrests, locations were there was going to be an event, subjects that they were investigating. That became an incredible resource that was developed over 40 years ago to help law enforcement to overcome those turf battle issues.

I have got to give great credit to the attorney general of the United States on the fact that they came out with a memo last May that mandates that every component within DOJ law enforcement component deconflicts, that they get over those turf issues, that they get over those constraints that they put on themselves to share that information. Now unfortunately, that same movement hasn't come to place in the Department of Homeland Security and their components. But every one in the country should be deconflicting.

The hard part on this for the Regional Information Sharing System is 2 years ago, their budget was reduced by 40 percent. Their whole job is to protect law enforcement and allow those who have gotten over the turf battle issues to share data, share investigative information and put investigators together. That is one of those things that they need the resources, they need the funding. We need to support all of our law enforcement to use those services, to know when people are put under investigation, to reduce duplication of effort, and increase the safety of officers.

Chief BEARY. Thank you for the question.

We have made great strides over the last 15 years. Again, I have been in this business a long time. Within the last 15 years, we have realized how complex these cases are.

You know, it used to be you had those turf battles because criminals stayed in their jurisdiction and they did not use electronic de-

vices and they did not travel far from home. So, generally, you knew that 20 percent of your bad guys were causing 80 percent of your problems. It was pretty easy to figure out. Well, as the country has become more reliant on technology and as we have become more transient in nature—most of us in law enforcement got it a long time ago—and to be effective, you have to work with other agencies and you have to share intelligence information. I have seen a huge change in that with, you know, it used to be dependent on the relationship you had with that agency and knowing somebody.

Now, if an FBI agent calls me or another agency calls me and I verify who they are, their identity, they are getting the information. So I think that what you have seen is we understand that crime is now global in nature. We have made great strides to push our resources and protect our public.

Mr. ALEXANDER. I concur with everything they just said, Mr. Chairman. But let me just add one other thing here. I want to put a great deal of emphasis on this. You know, there is still this notion that somehow Federal and local law enforcement don't work well together or share information. As you have just heard, there has been a history of that in the past.

But certainly in more recent years, particularly post-9/11, we have really seen a collaboration of support and strength between Federal, State, and local organizations. So that does not occur in the same sense in which we know historically it has occurred. But what I think is very important here is that inasmuch as our Federal partners may have funding to do more intelligence gathering, particularly as it relates to technology, a lot of that also needs to be put—a lot of those resources and funding also need to be put at the State and local level so they can work collaboratively together.

Nobody is waiting on—I am the only person who has got this piece of technology, I am going to share it. But here, again, we would like to be able to have an opportunity to gather that intelligence information through technology that is out there, which we can't afford, at the same speed as our Federal partners. Then we are looking at the same thing at the same time. Because what is going to be really important for us in this country is how fast we can gather information, how fast we can diagnose that information, and, more importantly, how fast we can act on it.

We have got to act on it with incredible speed because we know that we have those that are coming into this country to do harm to us every day. As you stated, Mr. Chairman, there are also those who are trying to recruit young Americans in this country. We know some parts of what that is. But the problem is we don't know all or how vast it may happen to be.

The only way we are going to know that is that we have to have the proverbial boots on the ground in local law enforcement and the funding in order to have the technology to meet that threat or any potential threat than we may have in the country.

Mr. HIGGINS. Thank you. I yield back.

Mr. KING. Thank you, Doctor.

The gentleman from Texas, Mr. Hurd—we will try to get through all of the Members we can in just about 13 minutes.

Mr. Hurd.

Mr. HURD. Thank you.

Thank you, gentlemen, for showing up today.

By way of my background, I spent 9 years as an undercover officer in the CIA. I was a HUMINT guy so I collected a lot of intelligence. I saw a lot of the stuff that is not getting down to you all.

This question is for all three of you. It is really a philosophical question. Dr. Alexander, I agree with you that the lack of centralized information is one of the problems. I also think that one of the problems is overclassification of information on the Federal side. You know, that is something us up here are going to have to fix for you because we are in that position.

But I also think the concept of need-to-know—you know, this was ingrained in me from when I was 22 years old, from my entire decade in the intelligence community. But I think we need to shift to a concept of need-to-share, right? I welcome your input and comments on how our intelligence community, our law enforcement community, we can shift the culture from this need-to-know to need-to-share.

Mr. SENA. Thank you very much for the question. You know, this whole ideology—and there has been this paradigm shift of how we used to do information sharing. I remember you know, vividly being called in by the FBI to look at some documents, highly redacted. Then as I started reading it realized that was one of my own task force officers that wrote the report. You know, but they thought they had a great lead there. That is the way it used to be.

Now we are getting more into that level of people needing to share information. Not just the law enforcement community, but we got to look for all those first responders out there, the firefighters, the emergency medical personnel, the emergency management personnel, those folks that can come across data. That is where the fusion center really comes into play. The development of terrorism liaison officers, folks who are trained to look for those signs of terrorism or other criminal activity and know to report that information to their fusion center.

The big piece of this that has to happen and has been talked about for decades is the tear line on every Classified document. There that has be an Unclassified version of every Classified document or we are losing our entire audience and the group of people that can collect the data we need to protect our country.

Thank you.

Mr. HURD. That is helpful. Thank you.

Chief BEARY. Thank you as well for the question. Overclassification has been one of those things that, quite frankly, drove me crazy for many years. Just like Mr. Sena, I have an experience where one of my detectives started an investigation and it was a terrorism-related investigation. It went to the FBI. Then when we requested an update, we were told it is Classified, we can't tell you. Well, if it wasn't for us giving you the information, you would have never known about that. So that has happened in the past. I am proud to say that does not happen right now.

The JTTF in Central Florida has done a great job and they actually reach out to us. But we have to push that intelligence is there to be shared. Again, I think a lot of that was ingrained in us from

the early 1970s, all the way back to Watergate. Law enforcement has slowly been breaking out of that and understanding that we need to share.

I think that was, quite frankly, pushed down on us by the Federal Government because the locals have been good about sharing information for a long time—again, back to that let's catch the bad guy and put him in jail. But we had those walls put up on us and the restrictions because of concerns about too much information and need to know. I absolutely endorse the concept that we need to share.

So thank you.

Mr. ALEXANDER. Thank you.

I appreciate that question as well too because it really goes to a piece of my testimony here earlier as it relates to required security clearances. If we think about the fact that we have Federal, State, and local law enforcement that is working together. Oftentimes our Federal partners, who are security cleared or have security clearances, oftentimes may want to but can't share certain information.

So it becomes important, I think, and incumbent upon us to think about, at least I do, think about that at a local and State level, how do we make sure that we can broaden or expand, if you will, opportunities for local and State law enforcement officers to have the opportunity to get those clearances so that the whole idea of a willingness to share becomes a much-valued reality. Because oftentimes information cannot be shared because maybe at the local level I am just not cleared. That clearing or security clearance that that may require for myself and other officers inside my agency oftentimes is very expensive and very protracted as I stated earlier.

So from a very fundamental basic philosophical thought about it is this, is that holding information is not going to be to our advantage in this country. We need to share as much intelligence information and trust in those that we are sharing it with because they have the right clearances in order to receive that information or are trusted with that information. But it is going to be for us very simply this, when we are able to ascertain intelligence information shared among each other and act on it and be able to talk about it collaboratively, it is going to be so effective in terms of the security of our Nation.

Mr. HURD. Thank you.

Thank you, Mr. Chairman.

Mr. KING. Mr. Hurd.

Mr. Barletta.

Mr. BARLETTA. Thank you, Mr. Chairman.

Chief Beary, in your written testimony, you state that the importance of engaging non-urban areas in information sharing should not be overlooked and that the planning and preparation for terrorist attacks often occur in small or rural communities. I agree, local law enforcement is the first line of defense in stopping any type of attacks.

As a former mayor, I understand the challenges faced by local communities and law enforcement officers in remaining actively engaged in our National information and intelligence-sharing efforts. In your opinion, what can Congress do to ensure that small and

rural communities continue to be active partners in fighting terrorism and what additional tools, if any, do they need?

Chief BEARY. Thank you, sir.

I think the example is already out there and it just needs to be expanded upon and that is the Terrorism Liaison Officer program, the TLO program. I can tell you in my agency, I have more TLOs in my agency per capita than most of the major cities around me because I believe in it.

If you have those officers that are on the street and they have been trained as TLOs, they know what to look for, they know how to report it, and they are not afraid to report it. Because I think that is one of the other concerns that some local officers have is that fear that if I report something and it turns out wrong, I am going to look bad.

Well, those TLOs are incredibly well-trained. The program is there. If there is any one thing you could do from that local perspective is push that TLO program, adequately fund it, train those cops, and make sure they share that data. It is an outstanding program.

Mr. BARLETTA. Thank you.

Mr. Sena, due to the nature of their positions, law enforcement officers have daily interactions, call for service, traffic stops, or community policing initiatives with the community that they serve. What type of training and processes are in place to be alert for potentially serious suspicious behavior? What is the reporting mechanism? For instance, are first responders aware that if they see a copy of *Inspire* magazine, for example, in a home that it should raise a red flag?

Mr. SENA. Thank you very much for the question.

As far as the education part, it goes back to that terrorism liaison officer training program but also training analysts to develop products. We have got to have a highly-trained cadre of analysts that produce the things that give them those indicators, those warnings. *Inspire* magazine in itself may not be anything. Printing 80-plus pages may not be the thing for most people. But if you see indicators, whatever it may be, whatever the latest trend is for activities, they have got to have the ability to get that in their hands so that when they are out there on that call, if they see those indicators, then they know hey, this is what I just learned about in the bulletin or the briefing that I just had or whatever training they just attended.

Then the other piece of that is that, you know, understanding of the Nation-wide Suspicious Activity Reporting initiative, knowing that, you know, as the local law enforcement, you know, guy on the street, their job is to report that information to their fusion center and the Joint Terrorism Task Force so those analysts can look at that and see if there is any connection between that individual whose house they are at and any other on-going investigation. Sometimes there is no connection. But then that becomes one of those pieces that can, you know, be added on to later to that puzzle that identifies this person as a potential criminal threat.

Mr. BARLETTA. Thank you.

Thank you Mr. Chairman.

Mr. KING. We will go to Mr. Langevin. We should have enough time for Mr. Langevin. If we have time, we will go to distinguished Mr. Keating.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I appreciate the courtesy and——

Mr. KING. First let me just say that your colleague, Mr. Keating, yielded to you because he did have priority. You owe him one.

Mr. LANGEVIN. I owe him one, among many.

I want to thank our panel for your testimony here today. Mr. Sena, if I could just mention, I want to thank you for your comments on Regional Information Sharing Systems. Obviously they are incredibly important in the capabilities that they provide to law enforcement agencies. In fact, Mr. King and I have led the effort now for several years requesting funding support for the RISS centers around the country.

If I could, I will start with Chief Beary, cyber terrorism and cyber crime more broadly is an enormous concern of mine. I spend a lot of time on this issue. How were your members dealing with the rapidly-growing cyber threat? Do you feel adequately prepared to deal with this issue?

Chief BEARY. Thank you, sir.

The answer is no. We are not adequately prepared to deal with it. We have seen an enormous growth and that is only what we know about. What scares me is what we don't know about. Most local law enforcement agencies do not have the money or the technology or the time to train their personnel for these matters. We have seen great movement by the FBI and the Secret Service and others trying to ramp up their training for State and local officers. That needs to continue.

I personally believe, and I may be smashed for this but I tell it like it is, what I see across this country is I don't see crime going down, I see crime as different. I think there is a lot more crime than we know about because of cyber crime. I think that will be the growth area from now and into the future.

So we have to, first thing, get our arms around how big the problem is. Right now, we can't even say it because nobody tracks that data. There is no central repository tracking data for cyber crime. So every time we talk, we are just speculating. I think that most Americans—I have been victimized three times with my information being stolen. It is very frustrating.

So the answer is going to be we need to explore it. We need to train our officers. As a country, we need to look at the rules and the laws. Because right now they do not keep pace with what we are dealing with across this country.

Thank you.

Mr. LANGEVIN. Thank you. That is very insightful and helpful. Do either of our other witnesses want to testify on the cyber terrorism, cyber crime aspect?

Mr. SENA. Thank you very much. You know, about 2 years ago, the program manager for the Information Sharing Environment, Kshemendra Paul, invited me to his office and just so happened that Secret Service was there. We started a conversation about the development of training courses for analysts across the country. They worked with fusion center analysts to develop that training

course. They are going up on their 6th iteration of that training to get as many folks trained at the Hoover, Alabama facility to understand what the threats are coming from the cyber environment.

We also started a pilot about a year ago, working with the Multi-State Information Sharing Advisory Council, their Center for Internet Security, to develop a program of: How do we engage in the cyber threat? Everyone has a piece of it. When we look at, you know, everything from doxing, to those that, you know, are not maliciously trying to take out your money from your bank account but just trying to disrupt your daily life and routines, to those cyber terrorists that are attacking our networks and lately have been attacking law enforcement networks and capabilities.

If we lose 9–1–1 systems, if we lose our ability to control things within our law enforcement agencies, access to our own records, we can't function as Government, as law enforcement. So training analysts, training them to have that capability and our goal is to train thousands of analysts and those analysts will be producing products and currently are producing products for those law enforcement, for those public safety first responders so they know what the threats look like. So that if they become the victim of spear phishing or some other activity, they know how to report that information, we can triage it. Now with a unified message where you call three agencies, one of three, you can call those agencies to report your cyber activity, your malicious cyber activity.

So we have had some great strides in the last 2 years on that. We need to go much further because we are so far behind in law enforcement, just in the protection of our own infrastructure at a basic level. We need to protect our own infrastructure if we are going to protect our communities.

Mr. LANGEVIN. Certainly.

Mr. ALEXANDER. Yes, sir, and I certainly do concur with both gentlemen here. But also I must add too, as well, as you have already heard, is that as far as local law enforcement is concerned, our ability to fight cyber crimes or cyber terrorism is not there. We just don't have the money. We don't have the training. We don't have the access to the latest technology. Here is the thing, those who are committing these crimes, they are not MIT graduates. I have got a 12-year-old niece who knows how to get into my account.

With a little time, a little ingenuity, and a little willingness, we all can become very much victims. But very much importantly as well too, a lot of what is going on in our communities, and I think Chief Beary stated it very eloquently and he is right, crime is not going down, it is just something very different than what we know. We can't even measure cyber crimes or terrorism right now. We don't really know how vast and big a problem that it has the potential to be until we get the funding that is needed.

I will keep coming back to that, Mr. Chairman. We got to have——

Mr. KING. The message has come through loud and clear.

Mr. ALEXANDER. Yes, sir. Yes, sir. I am going to be held accountable when I get back to the great State of Georgia.

But the most important thing here is that for all of us, and I will speak for all three of us here, we are all saying the same thing,

and we are all singing from the same sheet of music as it relates to this.

Mr. LANGEVIN. Thank you.

Well you have confirmed the troubling reality that we are facing right now that we have got to get our arms around. We are way behind the curve on this.

Thank you for that.

Mr. KING. My wife's family is from Georgia. So I will tell them that you really advocated well for them today.

We probably have 2 or 3 minutes left in the vote, and so I recognize the gentleman from Massachusetts, Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman, and since we are up against a roll call, I will just ask one question and ask you if you have other suggestions to give it to this committee in writing afterwards too, but this committee has—the full committee has investigated the Boston Marathon bombings. We found out that information sharing and the lack of that was critical to perhaps preventing that from occurring.

Specifically, we found out that, No. 1, while Federal authority said, well, the access—the information was actually there for the local and State authorities through the Joint Terrorism Task Force. No. 1, how would you ever know to look for it if you are not privy to that information in the first place?

No. 2, if you were, we found out that local police had to ask permission from the Federal agencies to even share that information with their chiefs or their supervisors.

I want you to tell us what we can do to make that better. I know the FBI has made some positive steps, but I also think it should be in writing so that it transcends any administration. Just a few seconds. Any other feedback you have how this could be corrected, if you could do it in writing afterwards as well.

Mr. KING. Yeah. I would ask if you could try to keep your answers to about 30, or 40 seconds. Otherwise you have to hang around for another hour until we come back.

Mr. SENA. You know, as far as the MOUs and putting it in writing that a JTTF officer has access to data doesn't do a whole lot of good mainly because they are investigators. They are looking at cases. We actually need to have the analysts that are in fusion centers have access to that data, have the briefings, have the coordination piece with it. They are the ones that can look at the overall picture.

Each investigator looks at their case. The analysts look at the myriad of information out there and tries to provide direction to those officers and agents in the field. They are the ones that really need to be included in this discussion.

Mr. KEATING. They don't have access.

Mr. SENA. Right now there is no access permission other than on a case-by-case basis, fusion center by fusion center. That has to change.

Mr. KEATING. Chief.

Chief BEARY. Thank you, sir. Mike hit the ball out of the park on that. It has to be the analysts because the investigator is only going to look at that narrow scope of their investigation, and they don't have that broad spectrum approach, and it needs to be the

analysts that have access to that data and the ability to share it and not be afraid to.

Mr. ALEXANDER. Very quickly, sir, I think one thing in addition to what my colleagues here are saying is we need to expand the ability for those chiefs or whomever to have that intelligence information, but they have to have security clearances, to make that possible. So I think that would be——

Mr. KEATING. Well, we are working to get this in writing so that it becomes a formal process, and if you could follow up with any more specific information, I really appreciate the information about the analysts, it would be appreciated.

Our time is precious so I yield back.

Mr. KING. Thank you, Mr. Keating.

First of all, let me thank the witnesses. I am sorry we have had to run it like this, but if we didn't end it now, you would have to hang around for another hour or so before we come back.

So I want to thank you very much for your testimony. We could have gone on much longer, believe me, and it is very, very informative, very central. Some of us may have questions in writing that we will submit to you, and any response you can give us would be greatly appreciated.

So I want to thank you very much. I want to thank the Ranking Member, and the——

Do you have anything?

Okay. The hearing is adjourned.

[Whereupon, at 3:01 p.m., the subcommittee was adjourned.]

○