STATE AND LOCAL PERSPECTIVES ON FEDERAL INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 8, 2016

Serial No. 114–84

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

25–266 PDF WASHINGTON : 2017

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

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

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

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*
JOHN L. DICKHAUS, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Staff Director*

CONTENTS

STATE AND LOCAL PERSPECTIVES ON FEDERAL INFORMATION SHARING

Thursday, September 8, 2016

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

The subcommittee met, pursuant to notice, at 10:03 a.m., in Room 311, Cannon House Office Building, Hon. Peter T. King (Chairman of the subcommittee) presiding.

Present: Representatives King, Katko, Hurd, Higgins, and Keating.

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

The subcommittee is meeting today to hear testimony from 3 National law enforcement associations regarding the importance of information sharing and on-going challenges. I would like to personally welcome the Members of the subcommittee, express my appreciation to the witnesses who traveled here today. I really appreciate you taking the time to be here. Now I recognize myself for an opening statement.

Nearly 19 months ago, this subcommittee held a hearing entitled "Addressing the Remaining Gaps in Federal, State, and Local Information Sharing." We heard from the same impressive panel that is before us again today, and a lot has happened since then.

During the initial hearing, the witnesses raised a number of important issues, including the need for cyber expertise within State and local law enforcement, providing fusion centers with greater access to FBI terrorism-related data, and concerns about the impact of encrypted communications platforms for law enforcement and counterterrorism investigations.

A number of specific recommendations for the Department of Homeland Security were also raised, such as providing greater access to security clearances, empowering I&A field personnel, and expanding the homeland security information network, just to name a few.

A number of the recommendations became legislative proposals that passed the House last year and are pending before the Senate. We have asked the witnesses to reconvene to provide an update on the status of these issues and highlight any additional challenges that need continued attention, especially in light of the administration transition next year.

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.

While carrying out critical security and public safety missions, U.S. law enforcement is facing an increased threat environment. Since September 11, 2001, there have been 166 plots within the United States linked to Islamist terror groups, with the vast majority occurring since 2009.

In May, FBI Director Comey stated that the Bureau has over 800 open cases related to individuals in the United States with links to ISIS, and I believe he said they are in all 50 States. So that is 800 open cases in 50 States of U.S. individuals linked to ISIS.

The terror group has called for attacks against law enforcement directly. In January 2015, a statement from the ISIS spokesman called on supporters to, "rise up and kill intelligence officers, police officers, soldiers, and civilians."

In March 2016, the Caliphate Cyber Army, CCA, a cyber group believed to be the ISIS hacking division, released a "kill list" with names and information on 32 police officers from across Minnesota. During the same time period, CCA published personal information of 55 New Jersey Transit officers and encouraged lone-wolf attacks against the officers.

Also troubling is the increase in domestic threats against law enforcement. In some tragic instances, these threats have turned into violence. The National Law Enforcement Memorial Fund website reports there have been 11 shooting ambush attacks on law enforcement in 2016 to date.

On July 7, 2016, a gunman killed 5 police officers in Dallas and 7 other individuals while on duty providing security at a protest rally. Three police officers were killed in an ambush attack on Sunday, July 17, 2016, in Baton Rouge. The attacker had made statements supporting attacks against law enforcement on his social media accounts.

In the past several months, there have been recurring open-source media reports that suggest multiple police departments must respond to social media threats against law enforcement officials in hundreds of jurisdictions across the United States.

I am concerned about this anti-law enforcement climate, and it adds to the dangerous nature of your jobs. Also, it involves going after terrorism and providing counterterrorism service.

I want to offer my personal appreciation, admiration, and support to the law enforcement, intelligence analysts, and first responders represented by your associations for the vital work they carry out every day, and I look forward to your update.

I want to especially thank Mr. Sena, Chief Beary, and Dr. Alexander for being here today. The input from your respective associations is critical to our understanding of what has to be done. You have been there, you know what it is about, and your testimony will be extremely valuable to us.

Now I recognize my good friend, the Ranking Minority Member from New York. For you who worked in Rochester and Albany, he

is from Buffalo, he is a little closer to the part of New York that you are familiar with.

Mr. Higgins.

[The statement of Chairman King follows:]

STATEMENT OF CHAIRMAN PETER T. KING

SEPTEMBER 8, 2016

Nearly 19 months ago, this subcommittee held a hearing entitled "Addressing Remaining Gaps in Federal, State, and Local Information Sharing." We heard from the same impressive panel before us again today.

During the initial hearing, the witnesses raised a number of important issues, including the need for cyber expertise within State and local law enforcement, providing fusion centers with greater access to FBI terrorism-related data, and concerns about the impact of encrypted communications platforms for law enforcement and counterterrorism investigations.

A number of specific recommendations for the Department of Homeland Security were also raised, such as providing greater access to security clearances, empowering I&A field personnel, and expanding the Homeland Security Information Network, just to name a few. A number of the recommendations became legislative proposals that passed the House late last year and are pending before the Senate.

We've asked the witnesses to reconvene to provide an update on the status of these issues and highlight any additional challenges that need continued attention, especially in light of the administration transition next year.

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.

While carrying out critical security and public safety missions, U.S. law enforcement is facing an increased threat environment. Since September 11, 2001, there have been 166 plots within the United States linked to Islamist terror groups with the vast majority occurring since 2009. In May, FBI Director Comey stated that the Bureau has over 800 open cases related to individuals in the United States with links to ISIS.

The terror group has called for attacks against law enforcement directly. In January 2015, a statement from the now-deceased spokesman for ISIS, Abu Mohammad al-Adnani, called on supporters to "rise up and kill intelligence officers, police officers, soldiers, and civilians."

In March 2016, the Caliphate Cyber Army (CCA), a cyber group believed to be the ISIS hacking division, released a "kill list" with names and information on 32 police officers from across Minnesota. During the same time period, CCA published personal information of 55 New Jersey Transit officers and encouraged lone-wolf attacks against the officers.

Also troubling is the increase in domestic threats against law enforcement. In some tragic instances, these threats have turned into violence. The National Law Enforcement Memorial Fund website reports there have been 11 shooting ambush attacks on law enforcement in 2016 to date. On July 7, 2016 a gunman killed 5 police officers in Dallas and 7 other individuals while on-duty providing security at a protest rally. Three police officers were killed in an ambush attack on Sunday, July 17, 2016 in Baton Rouge. The attacker had made statements supporting attacks against law enforcement on his social media accounts.

In the last several months, there have been recurring open-source media reports that suggest multiple police departments have had social media threats against law enforcement officers in hundreds of jurisdictions across the United States.

I am gravely concerned that the anti-law enforcement climate. The lack of support shown by many politicians and public figures is further enflaming tensions across the United States. Not only does this situation threaten law enforcement lives, I'm concerned it may impact their ability to operate, provide needed services, and participate in the National counterterrorism mission.

I want to offer my personal appreciation, admiration, and support to the law enforcement, intelligence analysts, and first responders represented by your associations for the vital work they carry out every day.

I look forward to the panel's update and would like to thank Mr. Sena, Chief Beary, and Dr. Alexander for being here today. The input from your respective associations is critical to the subcommittee's understanding of the threat and progress

made to improve the amount and quality of information shared between Federal, State, and local law enforcement.

Mr. HIGGINS. Thank you, Mr. Chairman.

I would like to thank the Chairman for holding this hearing and for his leadership on this issue. It is a follow-up to the hearing first held in the 114th Congress. I would also like to thank the witnesses for traveling here to be with us again today.

Today, only a few days from the 15th anniversary of the attacks on September 11, 2001, we know now, unfortunately, that information sharing is an integral part of our Nation's security. The idea and the practice of information sharing between Federal, State, and local law enforcement officials has been firmly ingrained in our homeland security policies since 9/11.

Our lessons learned have pushed the Federal Government to develop many initiatives expanding efforts at information sharing with State and local partners. Today, we have many examples of successful partnerships, such as the fusion centers and the National Joint Terrorism Task Force.

However, our work in this area is not complete. The primary intelligence mission remains collecting information and providing accurate analysis in a timely manner. The challenge becomes balancing the environment where competitive information sharing thrives while eliminating unnecessary duplication. That has and remains the challenge for law enforcement officials and its partners.

As Members of Congress, we have an important role today. When we met here in February 2015, we were recovering from a historic Government shutdown. Now, 1½ years later, we are days away from another Government shutdown with Department of Homeland Security funding and ultimately funding for our State and locals looming in the balance. So while I applaud the open and candid dialog, funding uncertainty trickles down and impacts all of the issues we have gathered here to discuss.

Moreover, the recent and on-going attacks against law enforcement highlight the fact that the true value of information sharing will never be realized if State and local law enforcement officials cannot respond and protect their own communities. At our last meeting, I encouraged intelligence and law enforcement officers to integrate themselves into jurisdictions and communities that they are assigned and in order to know and understand geographical and cultural sensitivities. Today, I would again encourage the same thing.

So while today's hearing topics are not new, they present issues that we cannot afford to ignore. This type of open dialog is beneficial to all parties involved and helps to inform the decisions that we make as a collective body.

Again, I welcome you back here before this committee, and I look forward to your testimony.

I yield back.

[The statement of Ranking Member Higgins follows:]

STATEMENT OF RANKING MEMBER BRIAN HIGGINS

SEPTEMBER 8, 2016

Today, only a few days from the fifteenth anniversary of the attacks on September 11, 2001, we now know, unfortunately, that information sharing is an integral part of our Nation's security.

The idea and the practice of information sharing between Federal, State, and local law enforcement have been firmly engrained in our homeland security policies since 9/11. Our lessons learned have pushed the Federal Government to develop many initiatives expanding efforts at information sharing with State and local partners.

Today, we have many examples of successful partnerships, such as Fusion Centers and the National Joint Terrorism Task Force; however, our work in this area is not complete. The primary intelligence mission remains collecting information and providing accurate analyses in a timely manner.

The challenge becomes balancing an environment where competitive information sharing thrives while eliminating unnecessary duplication. That has and remains the challenge for law enforcement officials and its partners.

As Members of Congress we have an important role today. When we met here in February 2015, we were recovering from a historical Government shutdown. Now, one-and-a-half years later we are days away from another Government shutdown with DHS funding and ultimately the funding of our State and locals looming in the balance.

So while I applaud an open and candid dialogue, funding uncertainty trickles down and impacts all of the issues we have gathered to discuss today.

More, the recent and on-going attacks against law enforcement highlight the fact that the true value of information sharing will never be realized if State and local law enforcement cannot respond and protect their own communities.

At our last meeting I encouraged intelligence and law enforcement officers to integrate themselves into the jurisdictions and communities they are assigned, in order to know and understand geographical and cultural sensitivities. Today I would again encourage the same thing.

So while today's hearing topics are not new, they present issues we cannot afford to ignore. This type of open dialogue is beneficial to all parties involved and helps to inform the decisions that we make as a collective body.

Mr. KING. Thank you. The Ranking Member yields back.

I want to welcome our witnesses. Just to remind Mr. Katko, if he has a statement to make for the record, he can submit it. Other Members may submit statements for the record as well.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

SEPTEMBER 8, 2016

Information sharing is critical to our Nation's security. On Sunday, we will commemorate the fifteenth year since the September 11 attacks of 2001. I cannot help but to reflect on how successful we have been when it comes to piecing the puzzle pieces together to create better information sharing within the intelligence community and the law enforcement community.

While the puzzle is still evolving, the final picture is much clearer today than it was 15 years ago. Officials have become better at not only gathering information, but also analyzing 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.

The progress that has been made in both Congress and the Executive branch have strategically addressed 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.

However, this has not been an easy process. As Members of Congress, we have pushed to eliminate cultures, which promoted stove-piped information and prevented external sharing. Our goal has become shifting away from a need-to-know culture to a need-to-share environment. Our insistence must be shown by not only pushing for better information sharing, but also by providing the tools and funding 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 remain our most useful piece of 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.

However, as we convene here today, the funding of our Federal Government, including the Department of Homeland Security, is unknown beyond the end of this month. The end of fiscal year 2016 will be here on September 30. Unless Congress acts, our law enforcement agencies will lose their ability to fund many of the operations that we need to ensure that our country is safe.

So this hearing cannot be held in a vacuum. The needs of our State and local law enforcement groups cannot be balanced on the divides of political party lines. Continuous breaks in funding and the anxiety created from "not knowing" until hours before or after a deadline are not appropriate ways to run our Government and protect our country.

So it is irresponsible for us to charge our witnesses today, all of whom are partners within DHS, to continue fighting the good fight if we are not even willing to provide continuous funding.

While I look forward to revisiting the challenges that our State, local, and Tribal law enforcements groups face in sharing and receiving information with the Federal Government, I also look forward to hearing an honest assessment from each of our witnesses about the information-sharing challenges that continue to persist in this uncertain budgetary environment.

Mr. KATKO. Thank you.

Mr. KING. OK.

Our first witness today will be Chief Beary. Chief Richard Beary is the immediate past president of the International Association of Chiefs of Police and served as the president during the first subcommittee hearing in February 2015. He 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.

Throughout his years of service, he has twice been awarded the Medal of Valor for performance undertaken at great personal hazard. Obviously, he had the Orlando tragedy occurred within his jurisdiction, and look forward to anything you have to say about that.

But, again, thank you for your testimony when you were here in the past, look forward to your testimony again this morning. Thank you for your service. You are recognized.

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

Chief BEARY. Good morning. Thank you, Chairman King, and Members of the subcommittee for inviting me to testify back in front of you again. As you know, I was here on February 26, 2015, and I sat before many of you in this room, and we talked about some very important issues. I appreciate you reconvening so that we can follow up on those issues.

Over a year ago, I spoke about issues such as going dark, the encryption that the Chairman spoke about, which is only going worse, the integral role of the National Fusion Center Network, which is critical to how we do business, and how things have advanced since 9/11 in information sharing, because we have had some incredible gains and we can never forget that.

While there is no doubt that our fusion centers remain absolutely essential and law enforcement still faces great challenges, even with legal authority on gaining access to electronic communication

pursuant to a court order, I would like to focus on a few other issues today. Those issues are terrorist attacks and information sharing around incidents like the Pulse nightclub shooting, cyber threats, and Federal funding.

During my career, 39 years, I have watched the threats to our communities evolve. While we are still dealing with the problems of violent crime, drugs, prostitution, smuggling, trafficking, and gangs, we now face additional challenges. Those challenges include violent extremism, terrorism, cyber threats, and highly organized criminals with access to specialized equipment to aid them in their mission to harm others and devastate our communities.

June 12, 2016, 2:03 a.m., it is a day I will not forget. It was in the early hours of June 12 that Omar Mateen—which normally I don't identify the shooters, but I will in this case—killed 49 people and wounded countless others inside the Pulse nightclub in downtown Orlando. Forty-nine people lost their lives and 53 others were wounded. Quite frankly, if it wasn't for incredible medical care that was close by, those numbers would have been even higher.

Members of my agency were first responders to this horrific scene, and our victim advocates assisted family members at 3 local hospitals.

Now, 3 months later, we continue to provide counseling services to victims and their families as they work to restore some type of normalcy to their lives while the FBI and the Joint Terrorism Task Force continue the criminal investigation.

This Pulse incident highlights how one heavily-armed individual can inflict numerous casualties with weapons purchased legally here in the United States.

As law enforcement continues to deal with radicalized people and groups, there is growing concern about refugees from war-torn countries coming to our country. Thus far, we have not been informed how they will be vetted or where they will be located. Our need to know is not about targeting or trafficking, but more in line with assistance during assimilation and protecting these individuals from people in communities with ill intent.

Another issue of significance is cyber threats. The cyber threat confronting the United States has never been greater. The cyber threat is real, it is here, and it is now. It seems as though we read or hear about cyber crime and cyber attacks against Government agencies, businesses, and critical infrastructure every single week in the media. However, cybersecurity is not just a National-level challenge. It affects State, local, Tribal, and territorial law enforcement agencies every day.

These agencies encounter issues ranging from cyber-enabled crime committed against local individuals and businesses to forensic cyber investigations to protecting against and responding to cyber crime, cyber attack, and intrusions. Police departments themselves have become the targets of ransomware attacks which threatens our operation and the security of our information systems and data.

Please keep in mind that nearly three-quarters of the 18,000 law enforcement agencies in this country are small with fewer than 25 sworn officers. This means many of the Nation's law enforcement agencies do not have robust IT systems, and protecting their sys-

tems from intrusions is a challenge. Therefore, we cannot and must not overlook the importance of fully engaging smaller agencies and non-urban agencies in cybersecurity exercises, training, and threats.

I would also recommend that the FBI consider adding cyber crime reporting to the Uniform Crime Reporting system. During my 39 years in Government experience, it has shown me that for something to become a priority, we have to you count it first, and if we don't count it, it is not important to us.

It should come as no surprise to Members of this committee that Federal funding is essential to our efforts, from high-intensity drug trafficking to the fusion centers and all of the resources that connect the dots so that law enforcement can be effective.

On behalf of the IACP and our more than 27,000 members in 132 countries, Chairman, thank you for allowing me to be here again, and I look forward to answering your questions.

[The prepared statement of Chief Beary follows:]

PREPARED STATEMENT OF RICHARD BEARY

SEPTEMBER 8, 2016

Good morning Chairman King and Members of the subcommittee: Thank you for inviting me to testify today on State and local perspectives on Federal information sharing. I am currently the chief of police for the University of Central Florida, the largest university in the State. I am also the immediate past president of the International Association of Chiefs of Police (IACP).

On February 26, 2015, I sat before Members of this subcommittee and testified on this very same topic. I would like to thank this committee and subcommittee for reconvening a hearing on this very important issue and for the support it has demonstrated over the years for the law enforcement field and our communities.

Over a year ago, I spoke about issues such as "going dark," the integral role of the National Network of Fusion Centers, and how things had advanced since 9/11. While there is no doubt that our fusion centers remain absolutely essential, and law enforcement still faces great challenges, even with the legal authority, to gaining access to electronic communications information pursuant to a court order, I would like to focus on a few other issues today. Those issues are terrorist attacks and information sharing around incidents like the Pulse nightclub shooting, cyber threats, and Federal funding.

During my career, I have watched the threats to our communities evolve. While we are still dealing with the problems of violent crime, drugs, prostitution, smuggling/trafficking, and gangs, we now face additional challenges. Those challenges include violent extremism, terrorism, cyber threats, and highly-organized criminals with access to specialized equipment to aid them in their mission to harm others and devastate our communities.

June 12, 2016. I will never forget this day. It was in the early hours of June 12 that Omar Mateen killed 49 people and wounded countless others inside Pulse nightclub in Orlando, Florida.

Members of my agency were first responders to this horrific scene, and our victim advocates assisted family members at 3 local hospitals. Now, 3 months later, we continue to provide counseling services to victims and their families as they work to restore some type of normalcy to their lives while the FBI and our Joint Terrorism Task Force continues the criminal investigation. This incident highlights how one heavily-armed individual can inflict numerous casualties with weapons purchased legally here in the United States.

As law enforcement continues to deal with radicalized people and groups, there is growing concern about refugees from war-torn countries coming to our country. Thus far, we have not been informed how they will be vetted or where they will be located. Our need to know is not about targeting or tracking, but more in line with assistance during assimilation and protecting them from individuals with ill intent.

Another issue of significance is cyber threats. The cyber threat confronting the United States has never been greater. The cyber threat is real, and it is here and now.

It seems like we read or hear about cyber crime and cyber attacks against Government agencies, businesses, and critical infrastructure every week in the media. However, cybersecurity is not just a National-level challenge—it affects State, local, Tribal, and territorial law enforcement agencies every day. These agencies encounter issues ranging from cyber-enabled crime committed against local individuals and businesses, to forensic cyber investigations, to protecting against and responding to cyber crime, cyber attacks, and intrusions.

Police departments themselves have become the targets of ransomware attacks, which threatens our operations and the security of our information systems and data.

Nearly three-quarters of the 18,000 law enforcement agencies throughout the United States have fewer than 25 sworn officers; nearly half have fewer than 10 sworn officers. This means that many of our Nation's law enforcement agencies do not have robust IT capabilities and protecting their systems from intrusions is a challenge.

Therefore, we cannot, and must not overlook the importance of fully engaging smaller agencies and agencies in non-urban areas in cybersecurity threat assessments as well as including them in cyber attack exercises and training. Fully engaging all law enforcement agencies in this increasingly growing threat is the only way we will be able to prepare for and prevent future attacks that threaten the security of our agencies and the United States.

I would also recommend that the FBI consider adding cyber crime reporting to the Uniform Crime Reporting system. My 39 years of Government experience has shown me that something can only become a priority for action when we begin to officially count it.

This should come as no surprise to members of this subcommittee, but Federal funding to support Federal, State, local, and Tribal agency efforts is essential. This includes Federal funding to support fusion centers, crime analysis centers, Regional Information Sharing System (RISS) Centers, and High-Intensity Drug Trafficking Areas (HIDTA). These have proven to be very effective platforms for integrating Federal, State, local, and Tribal law enforcement criminal information and intelligence, and they need to be maintained in order to insure the protection of the homeland. As these platforms continue to mature, their immense value in helping investigative agencies to "connect the dots" has been demonstrated. As part of this maturity process, de-confliction of both targets and events between these platforms is becoming an increasingly important area that needs attention and support from Congress moving forward.

On behalf of the IACP and our more than 27,000 members in 132 countries, thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.

Mr. KING. Chief Beary, thank you for your testimony. Again, thank you for being here once more and for your service over the years.

Our next witness is Mike Sena, who is the director of Northern California Regional Intelligence Center, the fusion center for the San Francisco Bay area. He also currently serves as the president of the National Fusion Center Association, representing 77 State and local fusion centers that comprise the National Network of Fusion Centers.

Mr. Sena also has testified before this committee on numerous occasions and continues to be a great resource to the committee.

We thank you for that, and we appreciate you being here today, and now you are recognized. You have been here enough. I don't have to tell you how to do it. You are the pro.

STATEMENT OF MIKE SENA, PRESIDENT, NATIONAL FUSION CENTER ASSOCIATION

Mr. SENA. Thank you. Thank you, Mr. Chairman, and Ranking Member Higgins. I would like to thank you for inviting me to testify again on this important topic.

I am proud to represent the professionals across the National Network of Fusion Centers. Since we met in February 2015, we

have seen good information-sharing progress. But we have also been reminded that gaps still exist. At the end of the day, it is about meeting the needs and expectations of the American people and also that we keep them safe while respecting their rights.

Fusion centers are at the forefront of removing barriers, developing better pathways, and maintaining relationships that help analysis and sharing happen faster. The role of fusion centers in the aftermath of attacks in San Bernardino, Orlando, Baton Rouge, and other places are clear examples of that. Fusion centers are routinely deconflicting investigative cases today thanks to support of DHS, the PM–ISE, and our partners at the risk watch centers, and HIDTAs across the country.

That means that we have better visibility into active investigations around the country, and it means our officers are safer. We are working to standardize the process for exchanging requests for information, or RFIs, among fusion centers and our partners through HSIN exchange. This will help the flow of information and help track the responses.

In the wake of high-profile attacks in recent months, suspicious activity reports, SARs, forwarded to fusion centers rose sharply. Some people sent information directly to the FBI. Most people called 9–1–1 or their local law enforcement agencies. Thanks to the ever-growing network of liaison officers, those reports are routinely forwarded to fusion centers. Our analysts work with DHS and FBI partners to vet those reports, provide local context around the information, and submit them to the FBI's eGuardian system as appropriate.

Since the beginning of fiscal year 2016, through the end of July, fusion centers have received thousands of SARs from the public. We saw a massive uptick in November and December after the Paris and San Bernardino attacks. So far for fiscal year 2016, more than 100 of those SARs have contributed to existing FBI investigations or resulted in the initiation of a new investigation, and many of those were connected to individuals on the terror watch list. That is a clear indication of the enhanced reporting, analysis, and sharing that happens through fusion centers.

You can also find encouraging evidence of the progress in the newly published 2016 annual report from the program manager for the Information Sharing Environment, or PM–ISE. If Members of this committee have not yet reviewed that report, I strongly encourage you to do so. It is available on-line at ISE.gov, and I would like to submit it for the record.*

Mr. SENA. In my written statement, I lay out in more detail the challenges we are facing, but I want to highlight some of them here.

We have consistently called for more TS/SCI clearances for appropriate fusion center personnel. Without those clearances, the types of information our people are able to factor into their analysis can be inadequate and sensitive information that should be shared is not shared.

---

*The information referred to has been retained in committee files and may also be available at *https://www.ise.gov/resources/document-library*.

We have strong concerns about the impact of Federal FOIA interpretations on the legal ability of State and local law enforcement to share our information and intelligence with our Federal partners. We need better standards around law enforcement sensitive information, or LES information.

Currently, there is no clear definition of LES information and no penalties for unauthorized release of that data. We have to share most information at the FOUO–LES level so it gets to the people who need it, which can still reveal sensitive information about ongoing investigations, jeopardize cases and the lives of law enforcement personnel, yet there is no way to enforce or penalize violations.

We also believe that the FBI should explore the inclusion of fusion centers in its threat review prioritization process to ensure more complete understanding of the threats facing our Nation. Right now, several fusion centers are unable to begin to assess criminal justice information databases through CJIS.

We are also unable to gain access to the Financial Crimes Enforcement Network, FinCEN, and that challenge also exists with our other partners at risk centers and HIDTAs. I am very concerned that some of our Federally-funded programs, whose mission clearly includes providing investigative support, cannot get access to data that is fundamental to good analytical work. It is a clear obstacle to information sharing and analysis, and we need to address it.

Finally, we are working with the FBI on an "enhanced engagement initiative" to ensure the FBI continues to improve its sharing of relevant counterterrorism information with fusion centers. It will also improve coordination among fusion centers to address the growing terrorism threat. We are working closely with our partners at DHS, PM–ISE, and the Criminal Intelligence Coordinating Council on this project.

I want to congratulate and thank this committee for its productive legislation during the 114th Congress. You have moved several pieces of legislation that would make a positive difference to fusion centers and the American public. We strongly encourage the Senate to consider those bills.

Next month, we will hold our fusion center training conference in Alexandria, Virginia. I would like to invite Members and staff of this committee to attend the conference to see up close the challenges we are addressing and the level of corroboration that has become routine.

Mr. Chairman, thank you for inviting me to testify today, and I look forward to your questions.

[The prepared statement of Mr. Sena follows:]

PREPARED STATEMENT OF MIKE SENA

SEPTEMBER 8, 2016

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 High Intensity Drug Trafficking Area (HIDTA) and 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, and add State and local information and context to Federal intelligence, thus enabling local, State, and Federal officials to better protect our communities.

Since we last met in February of 2015, we have seen progress in the analysis and sharing of information related to threats to the homeland. We have also seen demonstrations of gaps that still exist. As I stated in my testimony last year, our public safety, law enforcement, and intelligence communities have made dramatic progress since September 11, 2001. This progress has not come without its roadblocks. As we continue to work through those challenges with help from this committee, we believe that we are on the right path and making steady improvement. At the end of the day, it's about meeting the needs and expectations of the American people that we keep them safe while respecting their rights.

At a high level, I believe we should be working toward the following four priorities to improve our ability to do that:

1. Strong Federal support for fusion centers through SHSGP and UASI grant funding, and accountability behind the Law Enforcement Terrorism Prevention (LETP) requirement in current law.
2. Strong engagement by DHS, FBI, and other Federal partners directly with fusion centers including the forward deployment of intelligence officers and analysts at fusion centers.
3. Strong training and network development between fusion centers, police chiefs, sheriffs, fire chiefs, rank and file, emergency management and other public safety partners at all levels of government and across all geographies to ensure tips, leads, suspicious activity, and criminal intelligence data are flowing efficiently for analysis and sharing.
4. Strong connectivity and direct engagement between Federal, State, and local investigative and analytical entities with responsibility for cybersecurity.

Over the past year, we have seen the important role the National Network of Fusion Centers plays in supporting lead investigative agencies in the aftermath of horrific tragedies—both terror attacks and criminal activity—in Orlando, San Bernardino, Baton Rouge, and elsewhere. Immediately after the San Bernardino terrorist attack, analysts at the Joint Regional Intelligence Center (JRIC) were developing intelligence on suspects and sharing it directly with the San Bernardino Police Department, San Bernardino Sheriffs Office, and the FBI.

An alert sheriff's deputy who had recently received training at the JRIC called the fusion center to report that an individual matching the description of the person wanted in connection with providing weapons to the shooters was about to check out of an area hospital. The fusion center immediately passed the information to the task force that was about to launch a manhunt for the individual, enabling them to call it off before it even started. It may seem simple, but the fast and efficient flow of tips, leads, and intelligence products is challenging in practice. Fusion centers are at the forefront of removing barriers, developing better pathways, and maintaining relationships that help information analysis and sharing happen faster. The JRIC's role after the San Bernardino attack is one clear example of that.

We have found after many of the recent high-profile terror attacks over the past year (San Bernardino, Paris, Orlando) that reporting of suspicious activity by public safety personnel and by citizens rose sharply immediately after the events. Some people send information directly to the FBI. Others don't know who to call, and naturally look to their local police agency or call 9–1–1. Thanks to an ever-growing network of liaison officers, those reports are routinely forwarded to fusion centers. Analysts vet those reports, provide local context around the information reported, and share information directly with the FBI via eGuardian.

I am still often asked whether fusion centers duplicate the FBI's JTTFs. This committee knows the difference, but many people are still not fully aware 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 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 actually is linked to terrorist activity.

In the wake of serious ISIL-inspired threats to law enforcement and other public safety officers around the country, the NFCA worked closely with the FBI to prepare a "Duty to Warn" memorandum to fusion center directors and FBI field office executive management to advise them of certain protocols and assistance for identifying and warning individuals that are the targets of threats. We also worked with the FBI to produce additional guidance on deconfliction efforts between State and Federal partners on the Duty to Warn documents.

An essential part of continued 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. For example, the FBI has assigned 94 personnel either full-time or part-time to 63 out the 78 fusion centers across the country. DHS has assigned 103 personnel to the fusion centers, including intelligence officers, regional directors, and reports officers.

The support of the Program Manager for the Information Sharing Environment (PM–ISE) and his office has been critical to some of the progress we have made since the last hearing. From continuing to coordinate the development of standards for sharing information across sectors, to enabling a single sign-on capability for personnel in fusion centers and other field-based information sharing entities to access multiple criminal intelligence databases, to paving the way for coordinated deconfliction of law enforcement operational events across multiple systems, the PM–ISE and his staff have been essential partners of ours. Another PM–ISE supported project is currently under way with the Northeast Regional Intelligence Group (including all of the fusion centers in the Northeast region) that will result in deeper cooperation and coordination among information-sharing entities and a wider set of public safety partners in the region. The ISE annual report for 2016 was just published, and I strongly encourage Members of this committee to visit the ISE website and review that report for more background on the progress we are all making together.

These resources 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 well over half of all funding for fusion centers in fiscal year 2015. In addition to concrete personnel and financial resources, the dedication of time and deliberate effort to continually deepen engagement with our Federal partners has been critical. One recent example of this was past month when personnel from 14 fusion centers participated in a week-long forum at FBI headquarters to exchange information regarding best practices in analytical collaboration and information sharing between the FBI, other Federal partners, and the National Network of Fusion Centers.

ADDRESSING ON-GOING CHALLENGES

Since fusion centers are separately owned and operated by State and local entities, there is variation among the centers in terms of budget and capabilities. That variation in capabilities has an impact on the expectations of our local, county, State, and Federal public safety partners and customers. To address this, the NFCA has initiated an effort to formalize a standard process for collection of analytical tradecraft best practices and operational success stories. We are also working to establish a single virtual location for these best practices so that anyone who is part of the National Network of Fusion Centers—from new directors to analysts—has a "one-stop shop" for resources to help improve their capabilities and understand what is happening across the National Network. We are creating new opportunities for advanced training for fusion center analysts, including collaborating with our Federal partners on advanced analyst training. There is currently no broadly-accepted method for exchanging requests for information (RFIs) across the National Network of Fusion Centers and among our law enforcement partners at all levels. So we are working to standardize that process for exchanging RFIs through HSIN. Next month we will hold our annual conference in Alexandria, Virginia and will have representatives from nearly all fusion centers, all of our Federal partners, and personnel from police departments, sheriffs offices, and other public safety entities around the country. We encourage Members and staff from this committee to attend that conference to see up-close the challenges we are addressing and the level of collaboration that has become routine.

We are continuing to address obstacles to progress in information sharing and analytical capabilities. For example, we have consistently called for more TS/SCI clearances for appropriate fusion center personnel. Without those clearances, the types of information our people are able to factor into their analysis can be inadequate. In some cases, sensitive information that should be shared by Federal partners is not shared. We also believe that the FBI should explore the inclusion of fusion centers in its threat review and prioritization (TRP) process to ensure a more complete understanding of the threats facing our Nation. In addition, we have voiced strong concerns about the chilling impact of Freedom of Information Act (FOIA) interpretations on the willingness and legal ability of State and local law enforcement entities to share certain State and locally-derived information and intelligence with our Federal partners. Also, we need to create standards related to "law enforcement sensitive" (LES) information. Currently there is no official designation of LES as a classification category and no penalties for unauthorized release of LES information. If we want to share certain types of threat information with a broader public safety audience for their situational awareness and security resource decision making, it cannot be at the "Secret" level. It has to be FOUO/LES, which can still reveal sensitive information about on-going investigations and jeopardize those cases. Yet there is no way to enforce or penalize violations.

Finally, we have been working hard over the past several months to address the current inability of several fusion centers to obtain access to certain Federal criminal justice information databases through FBI CJIS. In my mind it is unacceptable that some State and local entities whose mission clearly includes providing support to investigative agencies on criminal threats cannot get access to data sets that are fundamental to good analytical work. It is a clear obstacle to information sharing and analysis up and down the chain, it is a glaring gap, and it should be remedied as soon as possible.

We are working with the FBI on an "enhanced engagement initiative" to ensure the FBI continues to improve its sharing of relevant counterterrorism information with fusion centers, while also enhancing the contribution of information and analysis from fusion centers in a coordinated and efficient manner to address the growing terrorism threat. We are working closely with our partners at DHS, the Program Manager for the Information Sharing Environment (PM–ISE), and the Criminal Intelligence Coordinating Council (CICC) on this project.

To facilitate situational awareness and share information across agencies about cyber threats, the NFCA Cyber Intelligence Network (CIN), which is a relatively new network of fusion center cyber analysts, tries to ascertain whether the intelligence developed in various States may be part of a broader trend. The CIN is comprised of over 250 Federal, State, and local law enforcement members who focus on cyber crimes. These members come together and act as a Virtual Fusion Center utilizing a cloud service provided by the Homeland Security Information Network (HSIN) to share real-time cyber threat intelligence in support of an incident, event, or mission. This level of cyber threat information sharing was impossible only a few years ago, yet now is becoming routine. Testimony by Lt. Col. Dan Cooney of the New York State Police before this committee back in May laid out several examples of how fusion centers are part of this effort. In May of 2015, the "Cyber Integration for Fusion Centers" Appendix was added to the Baseline Capabilities for State and Major Urban Area Fusion Centers guidance. Clearly, good progress has been made. But we are nowhere near where we need to be on cyber analysis and information sharing across all public safety jurisdictions. It should be a priority in the next Presidential administration and in the next Congress to focus on this challenge.

We appreciate the work that this committee has done during the 114th Congress to ensure that fusion centers have the necessary resources to carry out their missions. The House of Representatives has approved multiple bills that originated in this committee to strengthen information-sharing practices and more clearly define roles and responsibilities. We strongly encourage the Senate to consider those bills and act as soon as possible.

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. We look forward to continuing to work closely with the committee.

Mr. KING. Thank you, Mr. Sena. I will certainly pass on your comments regarding the legislation to Chairman McCaul and Ranking Member Thompson. This is a bipartisan committee, and, again, they will certainly appreciate, as I do, the comments you

made. I know the Ranking Member does, and also Chairman Katko, who is Chairman of the subcommittee as well.

Our next witness is a true expert in law enforcement, Dr. Cedric Alexander. He is the national president for the National Organization of Black Law Enforcement Executives. He also serves as chief of police for DeKalb County.

Previously, Dr. Alexander was the Federal security director for the Transportation Security Administration at Dallas/Fort Worth International Airport. He also served—now we have a New York issue—as deputy commissioner of the New York State Division of Criminal Justice Services, chief of police in the Rochester Police Department, one of the outstanding departments in the State, and held several leadership roles at the University of Rochester, Department of Psychiatry in New York.

Dr. Alexander began his law enforcement career in 1977 and also served with the Miami-Dade Police Department and was a law enforcement police officer in Florida for 15 years.

Dr. Alexander, thank you for being here again. Thank you for your career of service. We now recognize you for your testimony.

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

Chief ALEXANDER. Thank you very much as well, Chairman.

Chairman King, Ranking Members Higgins and Thompson, and Members of the subcommittee, I bring you greetings on behalf of the great State of Georgia and law enforcement throughout the State of Georgia and the community in which I live as well.

I speak to you, of course, from 40 years of law enforcement experience and have been privileged to hold a number of high positions both in Federal, State, county, and local government over the course of my career.

As we review the past year-and-a-half, attacks such as those in San Bernardino, Orlando, and Dallas provide lenses by which we as a Nation, and in particular Federal, State, and local law enforcement, must continue efforts to improve information sharing, understand and confront new and emerging threats, and ask ourselves what more needs to be done.

Let me talk a little bit about the improvements that we have seen over the last year from where I sit, sir.

Improvements in information sharing among law enforcement agencies at the Federal, State, and local level have improved since February 2015. Efforts to declassify intelligence has helped Federal authorities share pertinent information more readily, which assists State and local law enforcement to prepare and respond to emerging threats.

Colocating the Georgia information sharing and analysis center with FBI staff encourages more efficient sharing and fusion of information and intelligence. As noted in February 2015, this fusion center and other local partnerships, task forces, and meetings with State and Federal agencies facilitate information flow but are still relationship-driven and systems remain decentralized.

Cooperation and information sharing between Federal and State law enforcement, as well as other private-sector partners, are sup-

ported through several strategic plans and directives, which are the "2014 to 2017 National Strategy for the National Network of Fusion Centers," and seek to connect with the intelligence community leveraging the strengths and resources of all partners.

Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, by President Barack Obama on February 13, 2015, lays the framework for partnerships and systems development for law enforcement, Government entities, and the private sector to collaborate in the security of the Nation's cyber systems. Further support includes the FBI Law Enforcement Enterprise Portal, LEEP, which centralizes many tools, resources, and training.

Now, new and emerging threats. Even though strides have been made, information-sharing and counterterrorism efforts are still hampered by systems that are largely decentralized and not standardized, unfunded mandates and budgetary restraints, personnel gaps, and classification of information and intelligence. Furthermore, cyber attacks, exploitation of social media platforms, and legal issues challenge law enforcement capabilities.

Decentralized. Albeit there are many tools, public and private sector, whereby law enforcement may collect, analyze, develop, and share information and intelligence, but they remain relatively decentralized. Fusion centers across the country are working hard to bridge this gap, but the intelligence community mission still requires accessing several websites, software, and databases.

Furthermore, there is so much data and information available that investigators oftentimes find it difficult to identify that which is relevant and actionable intelligence. One intelligence professional discussed how many of the intelligence bulletins entail several pages with limited new and actionable intelligence and stated that these need to be condensed to critical information to avoid being overlooked.

Many agencies have turned to varying systems offered from the private sector, which have great potential, yet do not interface with one another. These challenges slow State and local law enforcement identifying and responding to threats.

Funding and personnel. I am going to move through this very quickly due to time.

Counterterrorism and intelligence capability require funding and personnel to keep pace with current and emerging threats. While the strategic plan is to develop, encourage, and use public-private partnerships to counter threats and share information, the systems still require funding.

Data, information, and intelligence in many cases require security clearances. Although numerous departments across the country are able to assign officers to task forces, such as the FBI Joint Terrorism Task Force, others do not have the personnel. Even with such assignments, briefings provided contain Classified information that are limited upon how it may be used.

I am going to go right to what more needs to be done, if I could, Chairman, with the time that I have left.

Mr. KING. Sure. Absolutely.

Chief ALEXANDER. But I want to talk here about systems. Intelligence, information, analytical tools, databases, and other re-

sources still require better centralization and simplification. Although improvements have been realized in collating intelligence, more is needed. My recommendation remains that intelligence sources, tools, and resources continue to merge and be centralized providing for a one-stop site and dashboard where the intelligence community can access, investigate, analyze, share, and produce actionable intelligence.

Simplification and reducing data overload is key. Standardizing intelligence systems to make them more interoperable can increase the speed of gathering, analyzing, and sharing data while simplifying the process of operators. Human intelligence will remain no matter how robust our systems develop, and these continue to need enhanced access to protected and Classified information.

Moving forward, we must find new avenues to increase the availability of protected intelligence to those of law enforcement and the speed by which it is provided. Declassification of materials, security clearances, and task force liaisons play a part, but developing an access or clearance level that would allow local departments better flow of information is needed.

Training and educating State and local law enforcement to operate in cyber and high technology fields has increased, including Web-based suites of courses through the FBI. These efforts should continue, increase, and involve a security clearance program that supports local access to protected material.

In summary, sir, there is no shortage of terrorist attacks we have seen in the last year-and-a-half to drive home the message that Federal, State, and local law enforcement must effectively and efficiently share information and partner with the private sector to protect our Nation. We are also experiencing a time in our Nation where a real or perceived divide between law enforcement and the community exists. Better information flow and cooperation is also necessary for our communities.

Thank you for the opportunity to be here. I am sorry if I went over my time, sir. But if you have any questions, I will be more than glad to try to entertain them for you.

[The prepared statement of Chief Alexander follows:]

PREPARED STATEMENT OF CEDRIC ALEXANDER

SEPTEMBER 8, 2016

Chairman King, Ranking Members Higgins and Thompson, and Members of the subcommittee, I bring you greetings on behalf of law enforcement communities across America.

INTRODUCTION

My name is Dr. Cedric Alexander, member of President Barack Obama's Task Force on 21st Century Policing, 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 "State and Local Perspectives on Federal Information Sharing." I want to acknowledge and thank Chairman King for holding this hearing and the invitation to participate.

I speak to you from the perspective of a person who has over 39 years of law enforcement experience and who has held positions at the highest levels of Federal, State, county, and city governments. In addition, I hold a Ph.D. in clinical psychology.

As we review the past year-and-a-half, attacks, such as those in San Bernardino, Orlando, and Dallas provide lenses by which we as a Nation and, in particular, Federal, State, and local law enforcement, must continue efforts to improve information

sharing, understand and confront new and emerging threats, and ask ourselves, "What more needs to be done?"

IMPROVEMENTS EXPERIENCED

Improvements in information sharing among law enforcement agencies at the Federal, State, and local level have improved since February 2015. Efforts to declassify intelligence have helped Federal authorities share pertinent information more readily, which assists State and local law enforcement prepare and respond to emerging threats. Co-locating the Georgia Information Sharing and Analysis Center (GISAC) with FBI staff, encourages more efficient sharing and fusion of information and intelligence. As noted in February, this fusion center and other local partnerships, task forces, and meetings with State and Federal agencies facilitate information flow, but are still relationship-driven and systems remain decentralized.

Cooperation and information sharing between Federal, State, and local law enforcement, as well as with private-sector partners, are supported through several strategic plans and directives. The *2014–2017 National Strategy for the National Network of Fusion Centers*, seeks to connect the intelligence community, leveraging the strengths and resources of all partners.[1] *Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing*, by President Barack Obama on February 13, 2015, lays the framework for partnerships and system development for law enforcement, Government entities, and the private sector to collaborate in the security of the Nation's cyber systems.[2] Further support includes the FBI's Law Enforcement Enterprise Portal (LEEP), which centralizes many tools, resources, and training.[3]

NEW AND EMERGING THREATS

Even though strides have been made, information sharing and counterterrorism efforts are still hampered by systems that are largely decentralized and not standardized, unfunded mandates and budgetary constraints, personnel gaps, and classification of information and intelligence. Furthermore, cyber attacks, exploitation of social media platforms, and legal issues challenge law enforcement capabilities.

Decentralized.—Albeit, there are many tools, public and private sector, whereby, law enforcement may collect, analyze, develop, and share information and intelligence, but they remain relatively decentralized. Fusion centers are working to bridge this gap, but the intelligence community mission still requires accessing several websites, software, and databases. Furthermore, there is so much data and information available that investigators find it difficult to identify that which is relevant and actionable intelligence. One intelligence professional discussed how many of the intelligence bulletins entail several pages, with limited new and actionable intelligence, and stated that these need to condensed to critical information, to avoid being overlooked.[4] Many agencies have turned to varying systems offered from the private sector, which have great potential, yet, do not interface with one another. These challenges slow State and local law enforcement from identifying and responding to threats.

Funding and personnel.—Counterterrorism and intelligence capabilities require funding and personnel to keep pace with current and emerging threats. While the strategic plan is to develop, encourage, and use public-private partnerships to counter threats and share information, the systems require funding. In many cases, agencies must use open market software and applications due to budget constraints. As an example, I discussed in February 2015 that funding for the Georgia Terrorism Intelligence Project (GTIP) was reduced to $90,000, down from a $2.5 million DHS grant in 2007 and these cuts remain today.

Law enforcement across the country have seen reductions in staffing and the ability to hire and retain quality and experienced personnel. These staffing deficiencies threaten our ability to respond to traditional crime problems, as well as, those of terrorism and cyber space.

Classified information.—Data, information, and intelligence, in many cases, require security clearances. Although, numerous departments across the country are

---

[1] National Strategy for the National Network of Fusion Centers 2014–2017. Retrieved from *https://nfcusa.org/html/NationalStrategyfortheNationalNetworkofFusionCenters.pdf*.

[2] Obama, Barack, *Presidential Executive Order 13691*, February 20, 2015 Vol. 80, No. 34, Part III. Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems.

[3] Johnson, Aisha, PhD, FBI Training Academy (November 2015). FBI Investigative Technology Training: Preparing Officers for Cyber Crimes. *The Police Chief*, pp 30–32.

[4] Donahue, Lt. T.P. Intelligence Led Police Unit, DeKalb County Police Department (personal conversation) August 26, 2016.

able to assign officers to task forces, such as, the FBI Joint Terrorism Task Force (JTTF), others do not have the personnel. Even with such assignments, briefings provided contain Classified information and are limited upon how it may be used. Furthering the problem is cost and timeliness of the clearance process. Understanding that this information must be protected, the process limits the flow of information and delays action.

Cyber attacks, Social media, and Legal issues.—Cyberspace threats, social media exploitation, and navigating the legal issues are ever-increasing concerns. Cyber attacks against law enforcement agencies have drastically increased in 2015 and are higher than those against other Government organizations.[5] Social media is used to recruit terrorists and other criminal actors, plan attacks, and muster large crowds to protest events. These activities are difficult for law enforcement to identify, track, and prepare a timely response, as the speed of cyber technology and ease of maneuverability is generally outpacing our efforts. Further exasperating the issue, are legal hurdles and privacy concerns. Striking the balance between public safety and privacy is a daunting task. "Going dark" which denotes the reduced ability of law enforcement to address cyber challenges, crimes, and terrorism due to technical and legal barriers, continues to be a problem.[6] Yet, these barriers are those that protect our freedoms and privacy. There are no easy solutions to these threats and challenges, but we must continue to work collectively to solve them.

WHAT MORE NEEDS TO BE DONE: MOVING FORWARD TO RECOMMENDATIONS TO ADDRESS THE GAPS IN ACCESSING QUALITY INTELLIGENCE SHARED AMONG LOCAL, STATE, AND FEDERAL LAW ENFORCEMENT AGENCIES

Moving forward, still more must be done to improve information sharing and counterterrorism efforts within Federal, State, and Local law enforcement. My recommendations include and build upon those made in February 2015.

Systems.—Intelligence information, analytical tools, databases, and other resources, still require better centralization and simplification. Although, improvements have been realized in collating intelligence, more is needed. My recommendation remains that intelligence sources, tools and resources continue to merge and be centralized, providing for a one-stop site and dashboard, where the intelligence community can access, investigate, analyze, share, and produce actionable intelligence. Simplification and reducing data-overload is key. Standardizing intelligence systems to make them more interoperable can increase the speed of gathering, analyzing, and sharing data, while simplifying the process for operators.

Protected/Classified Materials.—Human intelligence will remain no matter how robust our systems develop, and these continue to need enhanced access to protected and Classified information. Moving forward, we still must find avenues to increase the availability of protected intelligence to those in law enforcement and the speed by which it is provided. Declassification of materials, security clearances, and task force liaisons play a part, but developing an access or clearance level that will allow local departments better flow of information is needed.

Training and educating State and local law enforcement to operate in cyber and high-technology fields has increased, including web-based suite of courses through the FBI.[7] These efforts should continue, increase, and involve a security clearance program that supports local access to protected materials.

Funding.—Lastly, funding these and other initiatives remains a need across local, State, and Federal law enforcement. Detecting, deterring, mitigating, and responding to threats requires the personnel, resources, and systems to be successful and funding is necessary to ensure we are ready.

SUMMARY

There is no shortage of terrorist attacks in the last year-and-a-half to drive home the message that Federal, State, and local law enforcement must effectively and efficiently share information and partner with the private sector to protect our Nation. We are also experiencing a time in our Nation where a real or perceived divide between law enforcement and the community exists. Better information flow and cooperation is also necessary with our communities.

---

[5] Emerson, James J. and Kelepecz, Betty J. (February 2016) Cyber Attacks: The Contemporary Terrorist Threat. *The Police Chief*, pp. 34–37.

[6] Guy, Sarah (January 2016) IACP Advocacy's Efforts to Address Going Dark and the Prevention of Terrorism. *The Police Chief*, pp. 10.

[7] Johnson, Aisha, PhD, FBI Training Academy (November 2015). FBI Investigative Technology Training: Preparing Officers for Cyber Crimes. *The Police Chief*, pp. 30–32.

So we ask today, "Where do we go from here?" The answer remains to continue on our course of improving information sharing and counterterrorism efforts through centralized and simplified systems, improved classification and security protocols, increased training, and focusing funding toward these objectives. I thank the subcommittee for the opportunity to testify and I would be happy to answer any questions.

EXAMPLES OF SOURCES OF LAW ENFORCEMENT INTELLIGENCE INFORMATION

HSIN.—Homeland Security Information Network (DHS managed National information)
TRIPwire.—Technical Resource for Incident Prevention (Bomb-related)
Infragard.—Information from private sector and FBI for protecting critical infrastructure
RISSNET.—Regional Information Sharing System (for law enforcement)
LEO.—Law Enforcement Online, which is an FBI program administered by FBI/DOJ

EXAMPLES OF SOFTWARE USED FOR INTELLIGENCE AND INVESTIGATIONS

LexisNexis.—A locate and research tool for persons
Accurint.—A locate and research tool for persons
TLO.—A locate and research tool for persons
Clear.—A locate and research tool for persons
SnapTrends.—A social media analytics and intelligence tool
Analysts' Notebook.—A tool that collates, analyzes and visualizes data
Pen-Link.—A tool for collection, storage, and analysis of telephonic and IP-based communications
Intelligence RMS.—An intelligence records management system database

EXAMPLES OF TECHNOLOGY USED FOR INTELLIGENCE AND INVESTIGATIONS

Computers.—Desktops, laptops
Accessories.—Printers, scanners, fax machines
Networked.—Servers, plotters, laminators, color printers
Presentation.—Conference communications, display screens

EXAMPLES OF TRAINING

Criminal Intelligence Analysis
Financial Manipulation Analysis
Software and Analytics Training
Homeland Security and Terrorism Analysis
Writing and Presenting Intelligence Reports

Mr. KING. Thank you, Dr. Alexander. I wouldn't have even thought of interrupting you. My wife is from Georgia, and she wouldn't have spoken to me again if I had interrupted someone from Georgia. So thank you.

Let me ask the question, and I don't ask this from the vantage point of Monday morning quarterbacking, but specifically to Chief Beary and generally to the entire panel, using Orlando as an example, I understand the FBI closed out the investigation initially. Whether they should have or not, that is a judgment call. I am not going to question their judgment. The reality is, though, that the FBI would not have the personnel to continue to monitor every individual that a case is opened on in the country.

Do you believe that the JTTFs, though, should stay more in contact with local police so they could at least keep some general surveillance or monitoring of someone that a case was opened on, or at least an investigation was begun on, not enough to continue to keep the case going, but also there is still some smoke—there may not be fire, but there may be smoke—so that local police could still continue to monitor to the extent they thought advisory?

Also, is there sufficient cooperation between the JTTFs? Because you could have a large State with large populations, several JTTFs, and you could have suspects or individuals, obviously, crossing JTTF lines. Are the local police informed of those individuals?

So I will start with Chief Beary as far as Orlando, and then open it up to the other two witnesses.

Chief Beary.

Chief BEARY. Thank you, Chairman King.

The answer to your question is, first, I have to say this, and I didn't put it in my testimony. I still haven't gotten my head around the fact that my hometown is the mass murder capital of the United States. I cannot believe that as I sit here in front of you in Washington, DC, today that my hometown has that dubious honor. We hope that nobody else has to experience that.

Our commitment is every one of our patrol cars now has this sticker on it, because 49 people died, and the American public has already forgotten the number of people that died.

Now I will answer your question. I had to say that, because it is important for our community.

Mr. KING. Absolutely.

Chief BEARY. The FBI officers, I can tell you in Orlando, where I am a member of the JTTF and I have personnel assigned, does a great job of sharing information. They keep us in the loop. We have meetings; we are invited to their weekly meetings. So we have great intelligence sharing.

I can't answer if that information was shared at the other office, because that investigation of the shooter in Orlando was done by the Miami office. I don't know if that was shared with those local police agencies or not. So it would not being appropriate for me to speculate.

However, I would say this. Hopefully, if it didn't happen, certainly going forward, I would hope that if the FBI closes out a couple of investigations, they would at least make those locals aware of that.

I think the other missing gap here is when people start buying weapons and they are on that list, we certainly should know that that is happening. I know there are a whole bunch of issues when it comes to guns, but if you have somebody that has been investigated as a possible terrorist and they are buying weapons, somebody needs to tell the cops, and then we will take it from there.

So thank you, and I look forward to other questions.

Mr. KING. Thank you, Chief.

Mr. Sena.

Mr. SENA. You know, as far as the JTTF relationship with not just the fusion centers, but the local and State law enforcement, I think that it has expanded to the point where we have got really good relationships in many parts of the country. Other parts, it is not as strong. As Dr. Alexander said, oftentimes it is based on relationships, relationships that people have in the local community with the FBI, with the State law enforcement, with the local law enforcement, and the fusion center. All of that has to work together closely.

In my area, twice a week we send out those suspicious activity reports where, if we are able to, the details to 13,000 law enforce-

ment officers of who we are looking at, and that way they have context of what we are doing. They know what the subjects may be. But there are also privacy concerns that we also have to look at as well, because oftentimes with suspicious activity, people have not committed a crime. We also have to be cognizant of making sure that people understand that.

But at least giving them the ability to have visibility is key. We are doing across the country a lot better at that. Can we do better across the entire network? Yes. It is mainly, we have got to move away from personality-based operations to a standard function that this is the way we do business.

Unfortunately, it has taken us 15 years to get to this point. I actually think there needs to be policies and there needs to be legislation that encourages that level of cooperation and exchange of information.

But on the backside of that, we also have to have responsibility that people protect the data and not disseminate it inappropriately, which can cause a lot of damage to the ability to investigate, collect intelligence, and also the ability for law enforcement officers to do their job.

Mr. KING. Other police officials have mentioned that to me about legislation. Any thoughts you have on legislation, because that could be tricky. But on the other hand, again, I don't know if that gets us into telling the FBI director how to do his job or not. But if you could give us some ideas on proposed legislation on that too and will greatly encourage that type of cooperation.

Mr. SENA. Dr. Alexander, you want to take that first and I can comment?

Chief ALEXANDER. No, no, you can go ahead.

Mr. SENA. OK.

As far as the legislation encouraging, throughout the country people receive grant funding or funding is delivered based on expectations that you will do some type of activity. Every time that we throw a hook out there that in order to receive your funding levels you have to accomplish X, Y, Z, that is the mechanism, whether it be suspicious activity reporting, whether it be a willingness to share data, whether it be a process to so many clearances or so much access permissions, something along those lines that if you want to receive your Federal funding or your grants or whatever it may be, that there is a requirement that you have a duty to share information, that you have a duty as a fusion center to get that information out to those people in the field, and that people in the field have an expectation that they should ask their centers, that they should ask the FBI for data, and that in return, when they ask for it, they should get it.

Mr. KING. Thank you.

Dr. Alexander.

Chief ALEXANDER. There is one piece here that I did not get a chance to share in my opening statements. If I could, sir, I would like to read it.

Mr. KING. Absolutely.

Chief ALEXANDER. It is under funding and personnel. Counterterrorism and intelligence capabilities require funding and personnel to keep pace with current and emerging threats. While the stra-

tegic plan is to develop, encourage, and use public-private partnerships to counter threats and share information, the systems require funding. I will give you an example.

As we discussed in February 2015, the funding for the Georgia Terrorism Intelligence Project, GTIP, which we refer to it as, was reduced to $90,000, down from a $2.5 million DHS grant in 2007, and these cuts still remain today.

One of the biggest challenges I think my two colleagues here would agree with me on, Chairman, is that with all the emerging threats certainly that we have seen over the last couple of years, with the threats that we know that are still relevant that are out there today, with the amount of information that we are receiving and yet probably missing as well, it is going to be critical, I believe, to the infrastructure and public safety of our communities, particularly all our communities, but certainly to local communities in which myself, like Chief Beary, serve.

The more information that we are able to ascertain that is relevant to what may be pertinent to our communities, understanding that there are different levels of secrecy, but for us at very much of a local level, it becomes incumbent to have as much information as we have so that we can at least try to forecast, predict, prepare ourselves for what may be potentially be the next threat. We have to have funding to do that.

Even though we struggle with this whole decentralized piece of information sharing, I think that is a challenge in and of itself. But JTTF and the FBI and others really have done a tremendous job in supporting local law enforcement. But at the end of the day, sir, it certainly does come down to funding, and it comes down to having the ability to keep up with all the latest technology that is continually evolving each and every day.

Because one thing we know about the bad guys, whether they are domestic or foreign, many of them have the same technological advantages sometimes that we do. They look at some of the same information that we do, and they prepare oftentimes as we do.

So for us, it becomes critically important to have as much access to intelligence information, and that is guided, quite frankly, through being able to be funded so that we can work on some of these challenges that we know are constantly emerging in front of us, sir.

Mr. KING. Thank you, Dr. Alexander.

Ranking Member.

Mr. HIGGINS. Thank you, Mr. Chairman.

Thank you, gentlemen, for the work that you do. The fusion centers, the Joint Terrorism Task Force, it is always a question of resources, and it can never be enough. The more people that need to be investigated, the more people you need to fund relative to our law enforcement activities.

When you get into these kinds of issues, in counterterrorism intelligence you never get credit for what didn't happen. The whole emphasis is about preventing things from happening. So you do great work, and they do great work throughout our communities to keep everybody safe.

But I just can't help but conclude our big problem is guns. You look at Orlando, you had an individual for a time was on the FBI

watch list, 49 people dead, 53 people wounded, one shooter, one shooter. Semiautomatic rifle, semiautomatic pistol, legally purchased.

Newtown, Connecticut, 20 kids dead between the ages of 6 and 7, first grade. Most of those kids had multiple wounds. Six adults. Those adults were throwing themselves in front of the kids to try to protect them. The shooter also shot and killed his mother.

The kid was thought to have very significant mental health issues. Sixteen mass shootings, 8 of the gunmen involved in those had criminal histories and documented mental health problems that did not prevent them from buying a gun.

Why would any law-abiding citizen that invokes a Constitutional right to bear arms as a responsible citizen, and the vast majority of gun owners in this country I believe are, why would they defend someone that has terrorist activity in their history to purchase a gun legally?

I understand the Second Amendment, but the Framers of the Constitution could never have anticipated the kind of hell that was inflicted on innocent people in Orlando, in Newtown, in these other places where we have had gun violence.

I would ask you to comment. I mean, you represent, at least two of you, you represent chiefs of police. We are allowing terrorists, people with mental health issues, they outgun the very police officers that take an oath to protect us.

Now, I heard one response in the so-called defense of the Second Amendment when the Newtown shooting occurred, that we should allow more guns in the school. That would have created a mass shootout.

In terms of our law enforcement officials, again, they take an oath to protect all of us. Don't we at least have an obligation to them to ensure that they at least have a fighting chance in a situation where there is going to be a confrontation with some lunatic that legally buys a gun in this country? That is anti-American. That is anti-American.

I would ask you to comment.

Chief BEARY. Thank you, Congressman.

On behalf of the International Association of Chiefs of Police, we have taken a very strong position on this through the years. We absolutely support expanded background checks. We support closing the gun show loophole.

Just to put this in perspective, my wife recently just got married, and she had to get a new driver's license. To get a new driver's license, she had to show her birth certificate, she had to get two utility bills and a lease to get a driver's license. But somebody can get out of prison, go to a gun show, show no identification at all, and buy as many weapons as they want. Something is wrong with that, OK? Then it is the men and women that we represent that have to deal with that threat, OK?

So our association supports closing those loopholes and background checks.

The other thing that I have to tell you as a law enforcement officer, that we are seeing about the incredible increases about violent crime, we are seeing more weapons than we have ever seen before, and the shootouts are going to continue. The only reason the homi-

cide rate is not double what it is right now in this country is because of incredible medical care. If not, the homicide rate would be comparable to the 1970's, which people like to talk about.

That is a fact that I am willing to stand on right here in front of you or anybody else. We have to do a better job.

Mr. HIGGINS. Well said.

Chief ALEXANDER. Yes, sir. Certainly, I do wholeheartedly agree with my colleague, Chief Beary.

But let me say this a little. Over a year ago, I had two police officers respond to a call for service. Upon arrival to the scene, there were two bad guys that opened fire on them with long rifles. They engaged in a shootout that lasted probably for about 3 or 4 minutes, and that is a very long time. They were armed at that time, our officers, were armed with .40 caliber handguns. One of the subjects had an AK–47, another one with an extended magazine on a handgun.

Both officers were hit. One was severely hit in the thigh, the other one was hit in the lower leg. But they found each other and they stayed in the fight until backup officers got there.

I can't tell you how angry that makes me, how scary that was for all of us, because we almost lost an officer who almost bled out and who almost lost his leg. But thanks to medical science and Grady Hospital there, which is our trauma center there in Atlanta, they were able to save both of those officers.

This is a real serious issue when we start talking about gun control. I think most of us as Americans certainly do support the Second Amendment. I do. It is a Constitutional right that we all have. But this whole idea of our right is somewhat going amok in many cases, because oftentimes, when I hear people talk about it, they usually talk out of both sides of their mouth. On one hand, they want gun control, but yet on the other hand they don't. So I don't know which is which. I understand the strong lobbying of the NRA and the impact that it has on this country as it relates to gun control.

But this is a real serious problem for us. Quite frankly, if we go back and look at some of the prior shootings across this country, people who had no history of any involvement in any type of terrorist group, who just came out of nowhere, whether they were a college student or whomever they may have been, there were no signs, because the accessibility, quite frankly, of weapons is so easy in this country.

The greatest majority of people, you are right, Chairman, that own firearms in this country are law-abiding citizens. But we also know that at any given moment, any law-abiding citizen, because of stressors that may be imposed on his or her life, or life takes a different course and people lose themselves, and if they have accessibility to a weapon they could use it in a deadly way.

But it is not those who rightfully own these weapons that I am concerned about, it is the millions of weapons that are stolen from cars and homes every year that go reported, and oftentimes not reported, and find themselves on the streets of American cities.

You can take a city like Chicago, Illinois, for an example, and I think is a perfect example. There are a number of guns that they take off the street on a daily basis, but yet the number of killings

that take place is just unimaginable. But yet, we as a Nation, quite frankly, still have not done anything, I don't think, wholly, to really address this whole gun issue.

So we are going to have to decide which way do we want this. We want to exercise our Second Amendment rights, but at the same time too there are going to have to be some real hard decisions and legislation made. Maybe it will be under the next Presidential administration. I don't know. But we keep talking about it and talking about it and talking about it.

When I think about Connecticut and I think about those small babies that lost their lives, I mean, it almost brings tears to my eyes, even to this moment, because it is sad and it is shameful. But it goes on every day in this country still. It just doesn't happen in one place in a schoolhouse. It happens across communities, across cities, and across the country.

So I don't know the answer to that question, and I think we all can talk about it ad nauseam, but the reality of it is that as a Nation we are going to have to find a way to even hold those that are responsible gun owners, and that is me and a whole bunch of us.

But we have got to make sure that we keep the possessions of those weapons somewhere that is secure, that is locked, whether in our homes, in our cars, or whatever, and try to minimize the likelihood of those weapons being stolen.

Because those are the weapons that are hurting people, those that are being stolen, not from the guy who lives in my neighborhood or your neighborhood who goes down to the local gun shop and shows his identification and purchases a weapon either for protection or for recreation. It is those weapons that get away from us oftentimes and get into the wrong hands.

Mr. SENA. The comments I would like to add from the fusion center perspective.

Four years ago, when I started talking with the Terrorist Screening Center about the issue of known or suspected terrorist encounters that we were not being notified about, that was one of those encounters, groups. Reason being, they said, was the attorneys from TSC and the folks representing them.

They are fantastic partners, but they said, we can't share this with you, because the Second Amendment right that they can buy these, even if we know they have a belief from the law enforcement perspective that this person is a terrorist. I was just shocked, just dumbfounded.

Not having that information from a local officer or State officer that a person that we believe is engaged in criminal activity and under investigation and not know about it, it puts us in a bad position. Especially when we are talking about long guns. A long gun to a handgun is not a fair fight. Most law enforcement officers in America have handguns. They can't defend themselves against that.

Mr. HIGGINS. Mr. Chairman, just in closing, I would just say, first, thank you for your leadership. Thank you for your professionalism, your perspective on this issue. To me, it has massive street credibility.

We give fast track authority for trade deals; we should give law enforcement professionals and leaders fast track authority in devel-

oping common-sense, common-sense gun control, gun safety measures, because unless and until we do that, we are going to be back here year after year, and we are just going to be talking about the most recent mass shooting that occurred. Unfortunately, the further away you get from these incidents, these victims are forgotten.

So I will yield back.

Mr. KING. The gentleman yields back.

The gentleman from New York, Chairman Katko.

Mr. KATKO. Thank you, Mr. Chairman.

Thank you for your comments, gentlemen.

For 20 years I was a Federal prosecutor, and I had the great pleasure of working with State and local law enforcement on a regular basis in El Paso and in Puerto Rico and in up-State New York. I was always struck by the importance of having the State and local components on the Federal task forces.

Maybe the FBI didn't always agree with me, but I really felt that they were critically important. They brought a level of investigatory expertise that you don't always have. I mean, sometimes the local guys can just find that informant you need on the street or whatever to make your gang case or make your organized crime case. It is critically important.

So I have a fundamental understanding of task forces and the good and bad of them.

It is troubling to me to hear you say, Mr. Sena, that we still have this TS, Top Secret-think security clearance issue. So I wonder if you can expound on that for a minute.

Because it is frustrating to me, if you have State and local law enforcement that are willing to augment these task forces and are willing to put up bodies in this time of great budgetary constraints and in a time of a great pressure on the Federal law enforcement through the expansion of these ISIS investigations tenfold, maybe multi-times more than that, why has it taken so long, in your opinion, to get these clearances done? It makes no sense to me.

Mr. SENA. It has been painful. One manager in my office can't actually sit with the team that he manages for the past 8 months, because he is waiting for a clearance.

It makes it difficult for us to operate. Some of it is related to the violation into the systems for background checks that was done a few years back and their backlog. But it is a slow process.

The other complication of this is, DHS recently has gone to getting TS clearances for folks, but the SCI caveat has to be done by an organization such as the FBI to give up their information. So what we are running into, and this is the bizarre circumstance, we started out with getting secret clearances for our folks, and then they have to go through a whole new process to get a TS clearance from the FBI or SCI clearance.

It is a convoluted process. I know General Taylor over at DHS I&A has been very proactive in moving this forward to actually allow us for the first time for DHS to get TS clearances. But my clearance is through the FBI, and it was, back when it was done, a much smoother process. But we are still this time lag. If a person can't do their job for 8 months to a year and they are assigned to a task force, you are half a man down, basically.

Mr. KATKO. No, I understand that. We had the same problem, just my interns, in OCDETF cases, they couldn't even get access to the OCDETF information until halfway through the summer because they had to get a security clearances for a student intern. It is so frustrating.

Mr. SENA. Absolutely.

Mr. KATKO. Now, we understand the problem here. We did pass some legislation to hopefully address this. But what would you gentlemen suggest that we can do to get this going? I mean, is it just a matter of dollars and cents to get more bodies at FBI doing these background checks so we get them done in a more expedited manner or what is it?

Chief ALEXANDER. Well, I think that is a good question. I think that is something that the FBI wants just as much as we do, but the protocols that are set in place are set in place, so that may require some new changes in rules and policies and so forth.

But the criticalness of it is in the here and now, because here is what we know about the threats that are out there and the threats that are emerging. These are local threats, sir, as you have indicated, that are actually coming from our communities. Because the threats, whether it is recruitment of young people in communities across this country, they are coming from the streets of America.

So if kids or young people or we have threats that have come into this country through other avenues, they are on the streets of this country. If they are going to be noticed, found, investigated, first someone knows. Someone is seeing something or hearing something that is very unusual. It starts from the local communities. It doesn't start up here. It starts from local communities.

Mr. KATKO. That is part of what we tried to address with the countering violent extremism, getting people into the communities to help intervene before they——

Chief ALEXANDER. Absolutely. Right. But to Mr. Sena's point, we have to have authorities and those in the law enforcement community who have immediate access to information and be able to share that information as quickly as we can, because so much is happening so fast.

Mr. KATKO. Right. That goes to my second question, really, accessing the databases, which is really frustrating to me to hear that. How the heck have you guys, if you get your security clearances, why are you having a hard time accessing these databases?

I know it is so frustrating for you, you probably want to scream. It is maddening to me. If the information is there and the guys with boots on the ground out on the street have those security clearances, why don't they have access to these databases?

Mr. SENA. Here is one of the hard issues that we have. So we have programs like the risk program that have been around for over 40 years for deconfliction services, watch center service, HIDTA program since 1988, fusion centers, a lot of them after 9/11. They are programs.

So when we go to get access to some services, they go: Well, you are a program, you are not an agency, and because of that, we cannot—you know, there is nothing written in CFRs, in the Code of Federal Regulations that defines our programs as having access to that type of data.

So they will say: Well, that one person in your organization, because they come from that police department or that agency, can have access, but the rest of you, if he is not there, you are on your own. That is what we are seeing in some locations.

Mr. KATKO. That is despite the fact that they all have the same security clearance?

Mr. SENA. Absolutely.

Mr. KATKO. That is madness to me. That is absolute madness.

Mr. SENA. Yes, sir.

Mr. KATKO. If you trust them to have the security clearance, you trust them to have access to information. Am I correct?

Mr. SENA. That is correct.

Mr. KATKO. So how can we fix that?

Mr. SENA. The only way I can see now, because we have tried through policy, we have tried through discussion with various organizations about how do we make this happen, and even then the ideas are, at best, half-baked. Well, we will get an agency to sponsor you. We will go to the chief's department and say: Can we get you to sponsor us?

Mr. KATKO. It sounds like there is a fundamental fix that we can do legislatively. So what I am going to do is I am going to have my staff contact you folks and get your input, and then let's work collaboratively to try and fix this.

Mr. SENA. That sounds great, sir.

Mr. KATKO. OK.

Mr. SENA. We would really appreciate that.

Mr. KATKO. All right.

Well, thank you all, gentlemen. My heart bleeds for Orlando, and anywhere in this country of ours where things like this are happening. But the cold, hard reality is in all 50 States in this great country, we have ISIS investigations, and we have big investigations. We have task forces that are getting stretched to the hilt.

To think that in this time of great stress that we can't even share the information with people who have the security clearances is maddening. So we have got to do our job, and we will.

So thank you all very much. I appreciate it.

Mr. SENA. Thank you, sir.

Mr. KING. Mr. Katko yields back.

Mr. Keating, the gentleman from Massachusetts.

Mr. KEATING. Thank you, Mr. Chairman.

Thank you for being here. This is a critical dialog that we are having. As a former DA myself, I worked a lot with the chiefs. In fact, I worked with your successor, Chief Beary, I think Terry Cunningham in Massachusetts. Those dialogs at that level were important. In fact, we met regularly.

So I would just say to all of you, at least individually and I think for the committee, if you have information that you think could be helpful to us, suggestions, not just after this hearing but on an ongoing basis, feel free to call my office and share that information. It is important information.

Then we will try and unravel so many roadblocks. I mean, how can the Federal agencies, for instance, share information, or the FBI share information that they don't have sometimes? After Orlando, Senator Nelson on the Senate side and myself on the House

side, we put in legislation so that the FBI, when they are investigating terrorists, and then they have to close the case because of the structure that is there, if that person later tries to purchase a weapon, at least they should be notified at the Federal level.

I would like you to comment on that legislation. Because if they don't have the information themselves, how can they share it?

Chief BEARY. Thank you, Congressman.

You bring up one of the fallacies of the system. When it comes to firearms purchases, that is another whole—as I talked about, some of the challenges that are there. I can't get my head around, as a police chief, that you can be on the terrorist watch list and legally purchase a weapon. I mean, if we can't fix that, I am not sure where we are going with the rest of it.

But again, I am not sure what the fix is of that, but I would certainly hope that there has got to be some kind of communication on the Federal level, and then through our joint terrorism task forces it would get down to us on the local level. I certainly hope that happens.

But again, if we can't fix the watch list, I think that one is glaring and we should jump on that first, and then we will go from there.

Mr. KEATING. This doesn't even stop the purchase of the gun. It just gives the authorities the information that is being done, information that if they had that information as they are doing an investigation, could have made a great difference.

Chief BEARY. Correct. I think would have made an incredible difference. Based on those people that I know at the FBI that we work with on a daily basis and those personnel that we have assigned to the joint terrorism task forces, I think it would have made an incredible difference. I believe that.

Mr. KEATING. I also think from the bottom up having access. I just want to follow up regarding the clearance issue, too. I mean, what is the expense on the local departments? How are you getting some of the money for that as well as just the roadblocks that are there administratively? Is that an issue too? Do you need more resources to do that?

Mr. SENA. As far as the clearances themselves, the process goes through, for us, mainly, FBI and Department of Homeland Security. So they take care of the processing piece. It is just it takes so long right now for those clearances often to come through. You will have some that will take 90 days. You will have some that will take a year. No real rhyme or reason. But I always feel like it is a lack of resources and the ability to do these clearances that need to get done.

Mr. KEATING. Beyond the local and county law enforcement people getting clearance, do you want to comment too? We have had testimony before on the data analysts at the fusion centers having clearance. How important is that? Because if they are working with that data all the time, they don't have clearance.

Mr. SENA. Absolutely, that is critical. If they don't have the clearance, we can't tell them the context that what they are working on could potentially have. It is very painful.

The other piece of that is we have struggled over the years, we have worked tremendously with the FBI Office of Partner Engage-

ment, Kerry Sleeper's team, to try to figure out, how do we get the analysts the data from FBINet? A lot of the holdings that are about terrorism are in that system.

So we can get a task officer, so it is a sworn law enforcement officer, we can get him FBINet access, but we have yet to figure out how can we get the analysts who need the data more often than the officers, to give them the information to do their job in the field. It has really been heartbreaking for us to struggle so long.

We had an initiative, the National mission cell initiative, which has actually turned into the enhanced engagement initiative, which the primary goal of that was to figure out how do we get access to the analysts of those systems and how we get them the training. To date, over a year, we haven't gotten to that point yet.

Mr. KEATING. It is not a new issue.

The other thing I want to just highlight as an issue and get your comments, I hope, is the fact that the effectiveness of the CVE, for lack of a better term, that training, how helpful that is. But also, I know we are trying to do this in my home State and around the country, but just to get a sense in terms of reaching out to communities, reaching out to the Muslim community, reaching out and making them more empowered to be a partner in sharing information, that is critical at the root level. There has to be a trust that is built. But that trust is important. Also the access is going to mostly come from local law enforcement building those bridges.

Can you tell us of some of the progress, some of roadblocks, how you are doing across the country? Because without that, we are shutting off an important source of information and a dialog that has to be continued.

Mr. SENA. Absolutely. If my colleagues don't mind me taking that first.

Chief BEARY. No, go on.

Chief ALEXANDER. No, go right ahead.

Mr. SENA. The CVE, it starts for us with Building Communities of Trust, which was a DHS and Department of Justice, Bureau of Justice-assisted program, where we actually went out to the communities and start trying to build those relationships. I have to tell you, the first meeting we had was probably about the roughest experience I have had in my life. Folks with no trust for law enforcement. Trust was not even talked about. It was: We don't trust you from the start, from the beginning of this meeting.

That has kind of flourished to the point where today, this afternoon actually, we are doing a seminar with groups that probably have never been given a voice in our public safety community, from the Council on American-Islamic Relations to the Islamic Networks Group to the Muslim public advocacy committee. These groups are now going to do a presentation to law enforcement on what they see CVE, what they see Islamophobia, and what they see as ISIS from their perspective.

We do a lot of things in government from the top end. That doesn't work. We have to engage the community and hear their voice and what their concerns are. One of the things that they had a concern about is hate crimes. So we added onto our website portal and our ability on a mobile application that they could click on "hate crimes," so they can take that application out and give it to

their community so they can report things. We tell them first make sure you call your local law enforcement, but we are good with secondary reporting or if you have a fear of reporting, just click on that application to tell us.

Right next to that is our suspicious activity reporting. So that way if someone in their community sees something that fits the characteristics of a suspicious behavior, they can report that too. It is a huge leap for us, enormous. But it has been slow. It has taken us several years to do this.

But here is the problem we hear across the country. The communities that we are trying to talk to about CVE don't want to talk to us about CVE. They want to talk about the crimes they see. They want to talk about the hate crimes. They want to talk about the issues they have in their community. They want to talk about law enforcement and violence in their community.

Those are their issues, and we need to address those in order to get that conversation going about how to identify violence in their communities.

Mr. KEATING. That is a great point.

Doctor.

Chief ALEXANDER. Yes, sir, it becomes hugely important, with all the negative anti-Muslim rhetoric that we have heard over recent years, to engage our Muslim community. In DeKalb County, we have well over 700,000 residents, and we have an extremely large Muslim community in and around DeKalb County.

So what we did, and what is critically important in bridging these relationships, even though oftentimes we think of doing them after something happens, what is really important, that people feel a sense that you are really genuine in what you are asking in terms of building that relationship.

So for us, right after San Bernardino, it came to mind for me to bring in the Muslim community in DeKalb County, to sit down and talk with their leadership. I ended up, through one imam, ended up having about a dozen imams throughout the whole Atlanta metro community that showed up, along with my staff and a number of other chiefs that are in my county as well too, where we have a number of small cities in our county.

So it provided an opportunity to them to talk about their fears and the threats they had been receiving, their children had been receiving post-San Bernardino event. So it gave us an opportunity to share with them our commitment to their safety as we would any other American citizen, and they also committed to us that if they hear something or see something, that they would call us.

True to form, not long after that meeting, they began to share information with us that we gave to the FBI for their follow-up, and I think that is what we are trying to do here. But it has to be done in a very genuine way, and it has to be done in a way that people don't feel where you are just reaching out to me being nice because this occurred and you want to know if something happening in your back yard.

Mr. KEATING. I think that, last, I am over my time, but it is my own experience, what you are saying is so important. We did, in our county, when I was DA, we did civil rights training for law en-

forcement, but we did it regularly. We didn't do it just after a crisis.

I want to say this, because it is my experience as well, I come from a police family. The willingness of local police to participate and be part of this was just so strong, and I think it should be said publicly, given all that is occurring and the rhetoric around the country, this is something that if it is there and they can participate, police want to do this. It is for their own safety, but they are committed to the safety of their community.

So I just couldn't agree with you more that let's just not do these things in the wake of a tragedy, let's do it on an on-going basis. I think you have the willingness of the public and these community groups as well as the police to make it successful.

Thank you for what you are doing. Thank you.

Mr. HURD [presiding]. I would like to thank my friend and the distinguished gentleman from Massachusetts for his questions and his years of commitment to this issue.

I am now going to recognize myself for 5 minutes.

Gentlemen, good to see you all again. I think last time we were here, we were talking about overclassification. It seems that this issue has not been resolved. This is something that has to be resolved to make sure we get the right information in the right hands.

I think what your brothers and sisters in arms have to deal with, whether it is an active shooter—we are dealing with one possibly right now in Alpine, Texas, a small town in west Texas that I represent—is difficult. I want to make sure that your brothers and sisters in arms have all the information that they need.

Earlier, in some of you all's testimony, you were talking about a lack of cyber preparedness, and I think everybody hit on that. I am curious, can we dig a little deeper in what should happen, what kind of information are you all looking for, and where do you think that can come from?

Let's start with you, Chief Beary.

Chief BEARY. Thank you, sir.

What I found is good leadership delegates, and I would delegate that to Mr. Sena. I think he is in a unique position from the fusion center network to talk about a more global aspect.

Mr. HURD. Mr. Sena.

Mr. SENA. Thank you, Congressman Hurd.

When we started looking at the issues of cyber we drew back on kind-of what we looked at in our approach to suspicious activity reporting and how we create a unified message, that if you see something suspicious, say something, call someone, call local law enforcement, local law enforcement will pass that information to the FBI and JTTF and to their fusion centers.

When we look at the world of, "Who do you report a cyber threat to?", the closest thing we get has 5 different people on it that you need to contact. That makes it a little difficult, although there is a lot more cross-communication between those 5 different areas that you could potentially call, depending on what type of event it is, but we still need to have more of a unified process around the country of how an attack, how an incident is reported.

Mr. HURD. Honestly, we have tried to address that issue with the Cybersecurity Act of 2015, making the Department of Homeland Security the bellybutton for this level of cooperation. If you have the fortunate opportunity to be at a fusion center you could be able to still go to the Bureau and sometimes Secret Service, depending on the information, and we don't want to prevent the existing lines of cooperation that may already be happening, but where there is none, Department of Homeland Security is supposed to be the bellybutton.

We are also working, when it comes to the reorganization of the entity within the Department of Homeland Security that deals with cybersecurity, making it an operational unit. It already is, let's be frank, but we have to make sure that they have the proper structure to do that and to ensure that there are individuals there that are working with State and local folks on this level of cooperation.

But we can't just talk about sharing between the Federal Government and local law enforcement, we need to be talking about private sector as well, because they are the ones that are seeing a bulk of these attacks. We can be learning from them, and these are potential analysts that local law enforcement and State entities could be using.

So has there been talk of the integration of private-sector entities within some of these fusion centers when it comes to cyber information sharing?

Mr. SENA. Actually there has been. We have centers where there are folks in the private sector that have come in with this type of expertise. Virtual collaboration, we have a Cyber Intelligence Network that we have created, analysts from around the country that can get on-line, use a HSIN Cyber Intelligence Network tool that we have, and that way they can exchange information in real time of what threats they are seeing.

Because you are absolutely right, the people that are more able to see the threat are oftentimes the private sector. By the time that a law enforcement agency sees the threat, their computer is already locked up and everything has become a brick. At that point, it is too late.

But what we want to be able to do is, when somebody sees a threat, share that information with others, but also the hygiene part is incredibly important. The fact that someone within an organization, and it just takes the weakest link, clicks on whatever spear phishing that may be out there, somebody send you an email going, "Hey, I am your long lost brother, I am going to send you some money," or whatever it may be, clicks on that link and infects the entire computer.

We recently had that where it took out an entire agency, and not a large agency, it took out their dispatch services. That is happening across America.

Mr. HURD. One of the things that is important for me specifically is, when you all have specific examples where the information sharing works and when it is a problem, understanding those specific examples. Because if we can solve that problem for that individual instance, then we can figure out how to solve it in the future. But in this case, we need to have granular understanding. I

am deep in the weeds on this issue. So you all's feedback, positive and negative, going forward would be helpful.

There are two issues I want to address in the time I do not have, and one is this issue about suspicious activity and suspicious behavior. If we use the example of the Orlando shooter—Orlando killer, excuse me—he cased a number of locations that had private security there.

Are private-security folks, are they trained to detect suspicious activity? Are they filling out suspicious activity reports? If a private-sector security service has a suspicious activity, where does it go? Does local law enforcement see that? Because the reality is, I think, when dealing with these lone-wolf attacks of folks that have never been on the radar before, the way that we are going to figure it out is disrupt them when they are doing the casing operations. Guess who is going to disrupt it? The two of you all, the folks that you all represent.

So is that process on-going? How does that get integrated into the fusion center? Because I would describe these as micro intelligence networks, that we are gathering this information on the ground, and then how do we connect it to some of the National intelligence?

Maybe, Dr. Alexander, have you go first, and then Chief Beary, and then, Mr. Sena, you wrap it up.

Chief ALEXANDER. I think that is a great question, Congressman. Maybe Chief Beary has a different perspective on it. My perspective is, in a lot of these establishments, such as the Pulse nightclub for an example, we have thousands of those across this country, hundreds of them in some communities across this country as well, and they all have security at the front door, if you will. So if you were to ask are they trained to detect certain behaviors and so forth, no, they probably are not.

So even where you have police officers who may be working off-duty jobs at some of these establishments, they have a little bit better insight because of the training that they have, but if they are not careful and become very lax in that very social kind of environment, they themselves can find themselves very much at risk.

But to your question, I think it is something to really think about on a National perspective, is how do we train such establishments, if you will, how do we help them train or how do we train, whether we do it locally through JTTF or some law enforcement agency, to train security personnel that may be at nightclubs. If you are going to do it for nightclubs, now you have to do it for restaurants, you have to do it for theaters, you have to do it for——

Mr. HURD. Malls, grocery stores.

Chief ALEXANDER. Yes, you have to do it everywhere. So it has to be a training that is across the board that heightens everyone's awareness to the environment that we live in today that we all need to be very thoughtful, very mindful, and very watchful of our environment, but do it in a way where we don't hamper the democracy of people who like to move through a free society such as we do, but do it in training in a way in which we all are very thoughtful, because this is a new way of doing business in this country when it comes to that.

The other piece I want to back up, if you would allow me, sir, for a moment, you were talking about the investment of our corporations or private industry being involved in this whole security piece. The private sector has a huge investment in making sure that our Nation's security remains safe. They are the infrastructure of this Nation. Oftentimes, when we have had to call on them in the State of Georgia, for an example, the Southern Company, Georgia Power, we call on them for support or for information or provide us with support so that we don't have access to, they have been very willing to do so.

So the point is, I think, if we ask more of our private industry partners in our communities to take part in this whole enforcement piece, watchful eye of things that are going on, and being able to work with us through our intelligence gathering, and sharing what is intelligence that would be relevant for them as civilians, I think is going to strengthen this country as a whole. So I certainly do support that wholeheartedly.

Mr. HURD. Thank you, sir.

Chief.

Chief BEARY. Thanks, Congressman.

In particular with the Pulse killer, it is still an active investigation, so I need to kind of dance around some of what I am going to say. But it is very clear from what I know that this individual had cased other locations, and it was because of a change in a security footprint in those locations that that individual probably moved to another target. So changing your security stance occasionally is a good thing. Of course, at the university setting, we do that regularly with football and large-scale events. So we know that works.

In Orlando, we have ILOs, intelligence liaison officers, and those ILOs are not just law enforcement officers, they are people that work for those private corporations that are vetted, and they feed that information into our Central Florida Intelligence Exchange. So we do have that network. We have had it in place for many years. It is not just private sector. It is on the fire side. We have expanded that out.

Is there incredibly renewed interest? Absolutely. Then we get into that whole challenge, which we have talked about before, it is funding for our intel centers, our fusion centers, and then those clearances that those people need.

So there are systems in place, and they do work, and we know they work. But again, I agree with Dr. Alexander, we probably need to come up with some kind of standard training that is vetted so it is proper and that we don't violate people's Constitutional rights, and share that with more private-sector companies that are looking at enhancing their security operations.

Mr. HURD. Thank you, Chief.

Mr. Sena, in your response, I am going to add another question to you. If an outside entity is willing to pay for the security investigation to get clearances, shouldn't that speed the process? What is the barrier that is preventing that from happening?

Mr. SENA. To start it off on the security question, there is right now no real mechanism to allow the FBI or DHS to accept money from a private entity, and that is probably one of the bigger prob-

lems that they have. If they were going to pay for play and I get a quicker investigation if I pay, there is nothing like that that exists right now, and I don't even know if it would ever be possible to do that.

Mr. HURD. Well, there is a program called the 559 program on the border. It is really hard, I have learned in my 20 months in Congress, it is really hard to give something for free to the Federal Government, and there have been examples where we do that on infrastructure along the border, and I think there is a model for that public-private partnership.

Who is the entity, who is the person that makes that decision?

Mr. SENA. Well, that would be FBI and DHS security that would make that decision.

Mr. HURD. Gotcha.

Any final thoughts?

Mr. SENA. I did want to add to that question on the liaison officer piece and how you engage the critical infrastructure, and it is that piece. The ILOs, give them that direction.

The one thing that we have gotten a lot of good press on, I should say, and it is unfortunate that the way we get it is every time there is an attack, they put it on the news, they say, hey, this is how you submit a SAR. If you are critical infrastructure folks, this is how you push the button, and you can put the information in or call right away.

But that is the key. There has got to be some place, some easy mechanism for those people in private security forces to pass that information to us. They do daily. We have about 1,000 people.

But the other part of that is we need to be able to push data to them as well. So there has to be the ability from the Federal Government, from fusion centers, to send that. We are doing that to 1,000 people that are really the directors of and managers of the private security forces.

Mr. HURD. Well, gentlemen, I could sit here for another 15 or 30 minutes and continue this conversation. I just want to end with thank you all for what you do. Please thank your Members and the people that you represent. You have an incredibly difficult job, and thanks for keeping us safe. Again, I appreciate your valuable testimony and the Members for their questions.

Members of the subcommittee may have some additional questions for the witnesses, and we will ask for you to respond to these in writing. Pursuant to Committee Rule VII(E), the hearing record will be held open for 10 days.

Without objection, the subcommittee stands adjourned. Thank you.

[Whereupon, at 11:26 a.m., the subcommittee was adjourned.]