



September 8, 2016

State and Local Perspectives on Federal Information Sharing

Subcommittee on Counterterrorism and Intelligence, Committee on
Homeland Security, United States House of Representatives, One
Hundred Fourteenth Congress, Second Session

HEARING CONTENTS:

Member Statements

Rep. Peter T. King
Subcommittee Chairman

[\[View pdf\]](#)

Witnesses

Richard Beary
Immediate Past President
International Association of Chiefs of Police

[\[View pdf\]](#)

Mike Sena
President
National Fusion Center Association

[\[View pdf\]](#)

Cedric Alexander
National President
National Organization of Black Law Enforcement Executives (NOBLE)

[\[View pdf\]](#)

Available Webcast(s)*:

[\[Watch Full Hearing\]](#)

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

*This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.*



Compiled From*:

<https://homeland.house.gov/hearing/state-local-perspectives-federal-information-sharing/>

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

*This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.*



**Statement of Subcommittee Chairman Peter T. King (R-NY)
Counterterrorism and Intelligence Subcommittee**

*“State and Local Perspectives on Federal Information Sharing”
September 8, 2016*

Remarks as Prepared

Nearly nineteen 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 U.S. 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 five police officers in Dallas and seven 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 U.S.

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 U.S. 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.

###

**Statement of Chief Richard Beary
Immediate Past President of the International
Association of Chiefs of Police**

Subcommittee on Counterterrorism and Intelligence
Committee on Homeland Security
United States House of Representatives

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 three local hospitals. Now, three 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 issues 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 cybercrime 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 cybercrime, 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 cybercrime 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.



STATEMENT FOR THE RECORD

Mike Sena

President, National Fusion Center Association
Director, Northern California Regional Intelligence Center

United States House of Representatives
Committee on Homeland Security
Subcommittee on Counterterrorism and Intelligence
“State and Local Perspectives on Federal Information Sharing”

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 911. 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 underway 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 FY 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 weeklong 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 Ongoing 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 ongoing 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 cybercrimes. 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.

Testimony of Dr. Cedric Alexander
DeKalb County Deputy Chief Operating Officer-Department of Public Safety
Member of President Barack Obama’s Task Force on 21st Century Policing
Before the U.S. House Committee on Homeland Security, Subcommittee on
Counterterrorism and Intelligence
Hearing on “State and Local Perspectives on Federal Information Sharing”
September 8th, 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 be 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 \$90K, 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 cyberspace.

Classified information. 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 (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

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.

References

- [1] National Strategy for the National Network of Fusion Centers 2014 – 2017. Retrieved from [https://nfcusa.org/html/National Strategy for the National Network of Fusion Centers.pdf](https://nfcusa.org/html/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers.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.

- [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

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