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 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.

[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