



# Critical Issues for Intelligence Commanders

- Technical and Virtual Operations
- Preventing Terrorism and Targeted Violence
- Maintaining Access to Digital Evidence



MAJOR CITIES  
CHIEFS

## **Major Cities Chiefs- Board of Directors**

**Chief J. Thomas Manger**  
**President**  
Montgomery County

**Chief Art Acevedo**  
**1st Vice President**  
*Houston*

**Chief Jerry Dyer**  
**2nd Vice President**  
*Fresno*

**Chief Mike Brown**  
*Salt Lake City*

**Chief James A. Cervera**  
*Virginia Beach*

**Chief Jennifer Evans**  
*Peel Regional Police*

**Superintendent Michael S. Harrison**  
*New Orleans*

**Chief Kimberley Jacobs**  
*Columbus*

**Richard W. "Rick" Myers**  
*Executive Director*

**Chuck DeWitt**  
*Senior Associate Director*

**Patricia Williams**  
*Associate Director*



MAJOR CITIES  
CHIEFS

This project was supported by Grant No. 2014-DB-BX-K008 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

E-mail addresses, telephone numbers, and Internet references cited in this publication were valid as of the date of this publication. Given that URLs and websites are in constant flux, neither the authors nor the Bureau of Justice Assistance can vouch for their current validity.

#### Recommended Citations:

Major Cities Chiefs Association. 2018. Richardson, Tara. *Critical Issues for Intelligence Commanders: Preventing Terrorism and Targeted Violence and Maintaining Access to Digital Evidence*

Major Cities Chiefs Association. 2018. Koren, Dori. *Critical Issues for Intelligence Commanders: Technical and Virtual Operations*

## **Foreword**

### **Critical Issues for Intelligence Commanders**

Through the generous support of the Department of Justice Bureau of Justice Assistance, the Intelligence Commanders Group (ICG) of the Major Cities Chiefs Association (MCCA) and Major County Sheriffs of America (MCSA) had the opportunity to identify and examine in detail three issues that are of critical importance to local law enforcement agencies and their intelligence operations. The following three topics were selected by the leadership from MCCA, MCSA, and the ICG as current priorities that are expected to require continuing focus into the future:

- Technical and Virtual Operations
- Preventing Terrorism and Targeted Violence
- Maintaining Access to Digital Evidence

The final result of this project is this Critical Issues for Intelligence Commanders Series with three chapters that frame each of the above issues from the perspective of Intelligence Commanders and identifies recommendations for what MCCA and MCSA agencies can do to successfully confront them or what they need to have a greater impact.

Each chapter starts with an overview of the recommendations and needs across a few high-level categories, including Increasing Intelligence Commander information sharing and collaboration, advancing agency capabilities, intelligence and analysis, agency-wide training, federal collaboration, partner collaboration, and private sector collaboration. The topic of community outreach is also addressed, but only at a high-level since it is not the direct responsibility of Intelligence Commanders. Each chapter then delves into the detail of each recommendation and need, including any illustrative case examples, promising programs, or best practices. In addition to the detailed guidance on each topic, the following are some overall steps that can be taken to address all of the issues:

- ICG member agencies can help to move other agencies forward
  - Share example policies and practices
  - Spread word about available training and support
- Federal support would help to expand best practices and improve capabilities
  - Provide technology resources
  - Expand national training and technical assistance
  - Support identification and expansion of best practice programs
  - Direct resources to convene ICG Working Groups on specific priority issues

The content and findings of the Critical Issues Series are based on the work of three committees formed by members of the ICG. They met over multiple sessions independently and as a collective to address common components as a complete group. The committees ensured each issue was fully addressed and explored with the perspective and input of a broad range of agencies, pulling on the expertise already existing within the member agencies. Additionally, committee members were encouraged to share their agencies' individual promising practices to inform their discussions and include in the report.

The positive impact from this project has already been realized. It has become a strategic roadmap to guide the ICG on how it can best help its membership. Also, it has already resulted in agencies adopting best practices from other programs and it has increased offers of support and collaboration between member law enforcement agencies and from federal agency partners. All of these are positive and lasting steps that have made agencies more effective in their ultimate goal of protecting their communities.



**MAJOR CITIES  
CHIEFS**



## **The Intelligence Commanders Group**

The Intelligence Commanders Group (ICG) is a network comprised of the Intelligence Commander from every member of the *Major Cities Chiefs Association (MCCA)* and *Major County Sheriffs of America (MCSA)*. The ICG serve as a national forum for the discussion and analysis of intelligence related issues faced by the major cities and counties of the United States, including traditional criminal and homeland security related intelligence activities. It also identifies and examines common information sharing issues and proposes solutions for intelligence collection, analysis, and investigations, including identifying intelligence training needs and coordinating training opportunities for members.

Maintaining a national network of major city and county Intelligence Commanders allows for rapid information exchange in a diverse and very fluid threat environment. Accurate and timely information exchange is paramount in crime and terrorism prevention and includes the information sharing partnerships with federal intelligence agencies, fusion centers, and other organizations in the Intelligence Community. Prevention is the first line of defense for our nation against terrorism and targeted violence. Information exchange between federal, state and local law enforcement agencies and the Intelligence Community has reached a critical threshold of importance to keep our communities safe and secure from terrorist threats.

The Intelligence Commanders Group has led the way working to build advanced counter terrorism and intelligence capabilities. Their communities are home to many of the nation's most prominent terrorist targets, including those that are often mentioned in terrorist messaging and propaganda, which have driven them to find and adopt the most cutting-edge and effective strategies and capabilities and work with agencies across the United States and internationally to increase law enforcement's collective capabilities to continue to counter ever-evolving threats.

The continuing recent attacks experienced by MCCA and MCSA member agencies, whether the Las Vegas or Orlando nightclub shootings, the Chelsea Bombings, the Boston Bombing, the vehicle attacks around the country, or the hatchet attack against a New York Police Department officer, epitomizes the willingness of individuals to continue to take up arms against civilian populations and law enforcement. These events and others have forced member agencies to develop and refine their response capabilities after being the victims of some of our country's worst terrorist attacks and mass shootings. They are the country's preeminent experts in responding to mass shootings, bombings, vehicle attacks, and other complex attacks and the intelligence and information sharing operations that are needed to prevent these attacks.

Just as important is the safety and security of our communities negatively impacted by traditional criminal activity, including gang related activity and public health emergencies related to opioids. Strong partnerships between law enforcement and the communities they serve remain critical in the prevention of both crime and terrorism through identification and early intervention.

# Table of Contents

<b>Chapter One: Technical and Virtual Operations</b>	<b>1</b>
Executive Summary.....	1
Key Findings .....	2
Key Judgements .....	3
Key Recommendations .....	4
Introduction .....	5
Methodology.....	5
Survey and Research Results .....	5
Conclusion.....	15
Acknowledgements.....	16
<b>Chapter Two: Preventing Terrorism and Targeted Violence</b>	<b>17</b>
Executive Summary.....	18
Increasing Intelligence Commander Collaboration and Information Sharing .....	21
Advancing Agency Capabilities .....	23
Intelligence and Analysis.....	26
Agency-Wide Training.....	28
Federal Collaboration.....	30
Partner Collaboration .....	34
Private Sector Collaboration .....	36
Community Partnerships .....	37
Acknowledgements.....	40
<b>Chapter Three: Maintaining Access to Digital Evidence</b>	<b>41</b>
Executive Summary.....	42
Increasing Intelligence Commander Collaboration and Information Sharing .....	46
Advancing Agency Capabilities .....	47
Agency-Wide and Partner Training.....	48
Federal Collaboration.....	51
District Attorney Collaboration.....	53
Private Sector Collaboration .....	55
Community Partnerships .....	56
Acknowledgements.....	58

# **Critical Issues for Intelligence Commanders**

**Chapter One: Technical and Virtual Operations**



## Chapter One: Technical and Virtual Operations

### EXECUTIVE SUMMARY

The number of Internet users worldwide has increased over 20% in the last two years, reaching an estimated 3.8 billion as of 2018.<sup>1</sup> More importantly, the level to which people are living their lives online is unprecedented and rapidly rising. In fact, every second that passes marks another 3,000 Skype calls, 74,000 Google searches, and 2.7 million emails sent.<sup>2</sup> The numbers only tell half of the story though. The other half, which is more difficult to measure but certainly apparent, is the way in which people are increasingly turning to the Internet and social media applications for their education, employment, entertainment, and social well-being. This migration from the physical to the virtual world is occurring in every industry and affecting every aspect of life.<sup>3</sup>

Law enforcement and the manner in which society interacts with the criminal justice system is no exception. If anything, law enforcement agencies are quickly finding themselves on the verge of another major evolution in policing—this time revolving around the deployment of advanced technologies to combat crime and terrorism. Public safety cameras, license plate readers, cell phone tracking, and social media exploitation are already taken root in many large cities. Likewise, the path towards even more advanced technical operations is quickly becoming an emerging topic across the United States and Canada. Whether it be facial recognition and gunshot detection devices or video analytics and drones, there is no doubt the concept of virtual crime fighting will soon be the priority for many police chiefs and sheriffs.

As such, the Intelligence Commanders Group from the Major Cities Chiefs and Major County Sheriffs Associations recently embarked on a research project to shed more light on this topic and map-out part of the current landscape of technical and virtual intelligence operations in law enforcement. This report represents the findings of this effort to include the results from a survey of 52 of the largest law enforcement agencies in the United States and Canada.

*For the purpose of this report, technical or virtual intelligence operations are defined as the collection of intelligence information using electronic surveillance systems, social media, and other*



<sup>1</sup> Internet Live Stats, "Internet Live Stats."

<sup>2</sup> Internet Live Stats, "1 second."

<sup>3</sup> Koren, Dori. "Virtual HUMINT: Conducting human intelligence operations in the virtual environment." Naval Postgraduate School, 2015.



## KEY FINDINGS

- Nearly all of the agencies surveyed have a dedicated unit (52%) or some personnel (46%) designated to conduct technical or virtual intelligence operations. The average number of personnel an agency assigns to this specific mission is eight, while the agency with the largest number of personnel for this specific mission has 47.
- Over two thirds of the agencies surveyed have a unit dedicated to open source research (79%), social media analysis (75%), and/or technical surveillance operations (69%). Additionally, nearly half of the agencies surveyed have a Real-Time Crime Center (48%) and a little over a quarter have drone operators (29%).
- The most common purpose for conducting technical or virtual intelligence operations included support for criminal investigations, assessing threats to the public, and identifying crime and terrorism trends. The least common purpose was for identifying and tracking emergency management situations.
- The majority of the agencies surveyed use automated license plate readers, social network analysis, social media mining, remote surveillance, online undercover operations, and cell phone tracking to combat crime. While far less common, there are also some agencies that use drone operations and virtual Human Intelligence (HUMINT).
- The far majority of agencies surveyed are primarily using desktop computers (86%) instead of cell phones (14%) to conduct technical or virtual intelligence operations.
- Although the majority of agencies surveyed are conducting online undercover operations, only 42% have a deconfliction mechanism in place for these operations.
- The majority of the agencies surveyed use less than two paid services for conducting technical or virtual intelligence operations and nearly a quarter do not use any paid services. Additionally, the majority of the agencies surveyed use less than five free services for conducting technical or virtual intelligence operations.

### *This Report is Based on the Following Data Collection Effort*

*Survey Results from 52 of the Largest Law Enforcement Agencies in the U.S. and Canada*

*A Collection of Success Stories of Technical or Virtual Intel Operations in Law Enforcement*

*Research of Existing Literature and Coordination with Partner Associations*



## KEY CONSIDERATIONS

- The level of technical or virtual intelligence operations within major law enforcement agencies is high and likely to increase as new technologies become more affordable and widespread. This report is intended to serve as a foundation for further research and discussion on how law enforcement can better prepare for this new era of virtual crime fighting.
- The value of technical or virtual intelligence operations in combatting crime has proven quite promising in a short time. Nearly all of the agencies surveyed indicated a specific value in their overall effectiveness, but more importantly, many shared specific success stories where violence was prevented because of these technologies.
- Despite early success, funding continues to be a challenge for police agencies. In particular, programs that require homeland security grant funds to be divided across different mission areas (i.e., fire, police, and emergency management) continue to strain law enforcement's ability to combat crime and terrorism. Thus, a dedicated funding stream for police operations within homeland security continues to surface as a top priority.
- To be effective, law enforcement must remain current in deploying new technologies for preventing and addressing crime. A lack of innovation and adoption for whatever reason (cost, fear, perception, etc.) will give law enforcement a serious disadvantage in a world where even the newest technology quickly becomes accessible to the general public.
- Ensuring the protection of privacy, civil rights, and civil liberties must also continue as new technologies are explored in policing. In particular, it is essential for agencies to establish audit capabilities to ensure proper oversight and accountability for privacy and civil liberties protections. Such policies should be developed, implemented and enforced to ensure compliance and corrective actions for any violations. To the extent feasible, agencies should also continue to establish best practices with respect to the collection, use, dissemination, and maintenance of Personally Identifiable Information (PII).

## KEY RECOMMENDATIONS

- **Standardize and implement online undercover deconfliction mechanisms to avoid virtual blue-on-blue conflicts.** Eighty-eight percent of the agencies surveyed conduct online undercover operations, but only forty-two percent have deconfliction measures in place. The data did not specify whether those de-confliction measures were internal to the individual agency or external to outside agencies. In any case, the majority of online undercover operations are not effectively de-conflicted, which raises a number of potential issues for the future of online operations.
- **Increase the deployment of smartphones in law enforcement and expand the development of mobile software applications for police operations.** According to survey results, the vast majority of all agencies are primarily using desktop systems, while only ten percent are primarily using mobile platforms to conduct technical operations. Yet, eighty-seven percent of all surveyed agencies have Internet access in the field. Not only does this gap suggest that the use of mobile applications in law enforcement is feasible but it also highlights the fact that police agencies are still behind in matching the rapid migration to mobile platforms that is occurring in every industry. Simply put, the mobile phone is quickly becoming more important than the desktop and preparing for this transition will greatly enhance the use of technology within policing.
- **Establish an innovation network within MCCA and MCSA for enhancing virtual and technical operations in law enforcement.** The use of technology to combat crime and terrorism is quickly becoming the norm for most agencies and this is only likely to intensify in the coming years. Although there are numerous committees and think tanks that are exploring technology-related policy issues, there is not yet a formidable group that is focused specifically on innovation from within the law enforcement community. Such a network would allow for new ideas and solutions to be developed and driven by practitioners from within the police technical fields. The success stories within this white paper highlight the tremendous value in tapping into this knowledge base and interconnecting this research and development for the entire police community.



8

Average Number of Personnel Assigned to Conduct Technical or Virtual Intel Ops

47

Largest Number of Personnel Assigned to Conduct Technical or Virtual Intel Ops for a Single Agency

## INTRODUCTION

In August 2017, the Intelligence Commanders Group (ICG) of the Major Cities Chiefs and Major County Sheriffs Associations began exploring the topic of technical and virtual intelligence operations in law enforcement. The ICG formed a Technical and Virtual Intelligence Committee, supported by a grant from the Bureau of Justice Assistance, to conduct a survey and draft a white paper on this topic. The results of this survey and the effort as a whole are presented in this report.

Although this report contains original research and some unique insight into the current environment of technical and virtual intelligence operations, it is not intended to be comprehensive. The findings, success stories, and judgements are based solely on the participation of specific major city and county law enforcement agencies. Additionally, this report focuses exclusively on technical or virtual intelligence operations, which for this paper are defined as the collection of intelligence information using electronic surveillance systems, social media, and other computer-based sources or technologies. This general definition includes any form of legal intelligence collection that can be done virtually through the Internet (e.g., social media monitoring, open source analysis, online undercover operations) and/or remotely through an electronic device (e.g., drone surveillance, real-time camera monitoring).

Ultimately, this report is intended to provide police executives and law enforcement intelligence practitioners with some limited insight into the use of technical and virtual intelligence operations for combating crime and terrorism. There is a general assumption that the future of policing will increasingly become more technical and that perhaps someday, one cop behind a keyboard will prove to be more effective in identifying and preventing crime than three cops on the street. Whether or not this proves to be true, there is certainly an emerging need to prepare for what is likely become a new era of virtual crime fighting.

## METHODOLOGY

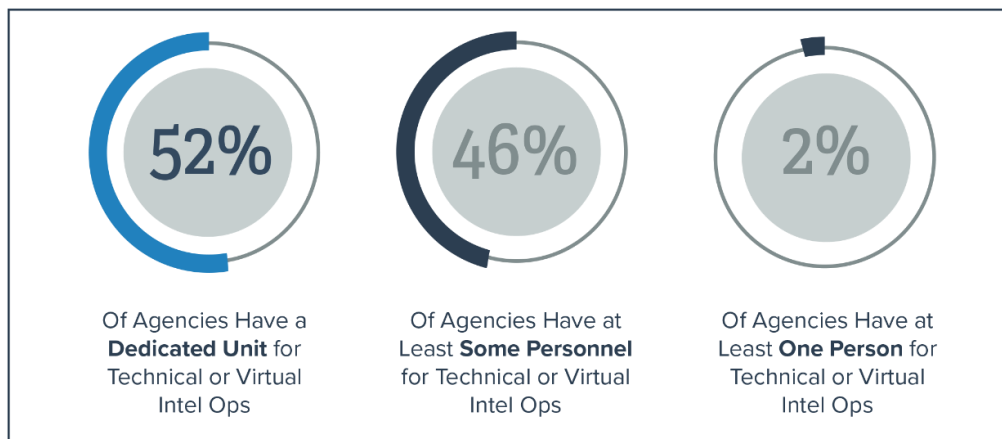
This report was developed using two data sets. The first data set is based on a twelve-question survey that was administered electronically to representatives from the intelligence sections of the Major Cities Chiefs and Major County Sheriffs Associations. This initial survey was designed to map out the current landscape of technical and virtual intelligence operations in law enforcement. Fifty-two agencies participated in this survey and provided complete answers to each question. The sample size and methodology used to collect this information was not designed to be scientific or representative of all law enforcement agencies. Instead, the survey was designed more as an inventory of current capabilities within the MCCA and MCSA environment.

The second data is based on success stories from MCCA and MCSA agencies that were collected from September to December 2017. 30 success stories were collected electronically from approximately 11 agencies. A limited selection of these success stories is presented in this report to provide a subjective view into the value of technical and virtual intelligence operations in law enforcement.

## SURVEY AND RESEARCH RESULTS

Nearly all of the participating agencies have a dedicated unit or some personnel assigned to the specific mission of technical or virtual intelligence operations. Only two percent, or one agency, responded that they only have one person in this type of assignment. The average number of personnel assigned to these units or

operations is eight, while the agency with the largest number of personnel assigned to this specific mission has 47. This initial measurement indicates a significant level of commitment to technical or virtual intelligence operations in law enforcement.



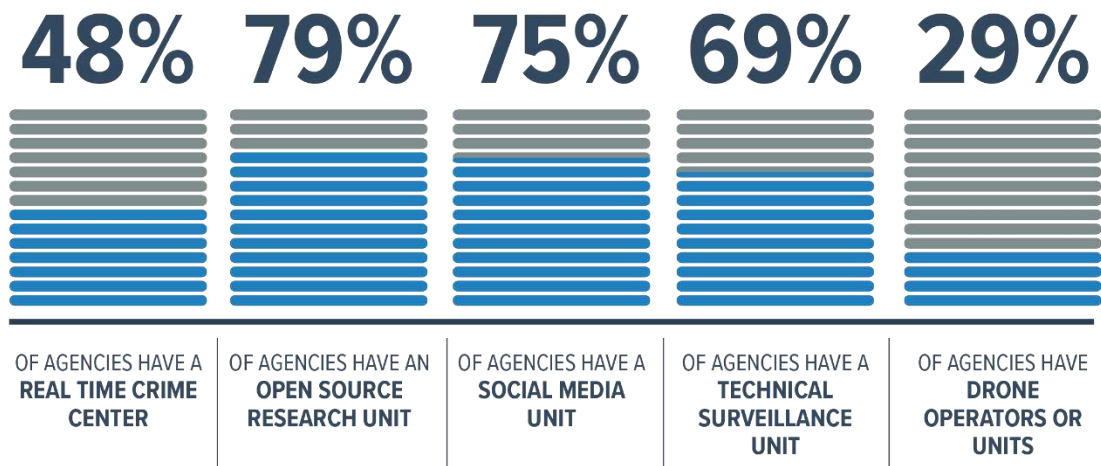
#### Success Story - Cell Phone Tracked to Arrest Kidnapping and Robbery Suspects

The Real Time Crime Center conducted investigative research to identify a phone for the suspect and then used GPS location information to further identify a possible location. The unit also leveraged online research tools to identify an escort advertisement that was connected to the suspect of the crime. The location and photo information were used to apprehend the suspects and recover a firearm. (Charlotte-Mecklenburg Police Department)

#### Success Story - Real Time Cameras Used to Arrest Robbery Suspect

Within three minutes of a robbery attempt, the Real Time Crime Center identified a subject matching the description using live surveillance cameras. This intelligence led officers to the suspect, who was arrested. (Louisville Metropolitan Police Department)

Over two thirds of the agencies surveyed have a unit dedicated to open source research, social media analysis, and/or technical surveillance operations. Additionally, nearly half of the agencies surveyed have a Real Time Crime Center and a little over a quarter have drone operators. This measurement indicates a particular focus on social media exploitation and online research in general, which is not surprising. However, the number of agencies with drone operations is noteworthy since this technology is fairly new in the law enforcement environment.



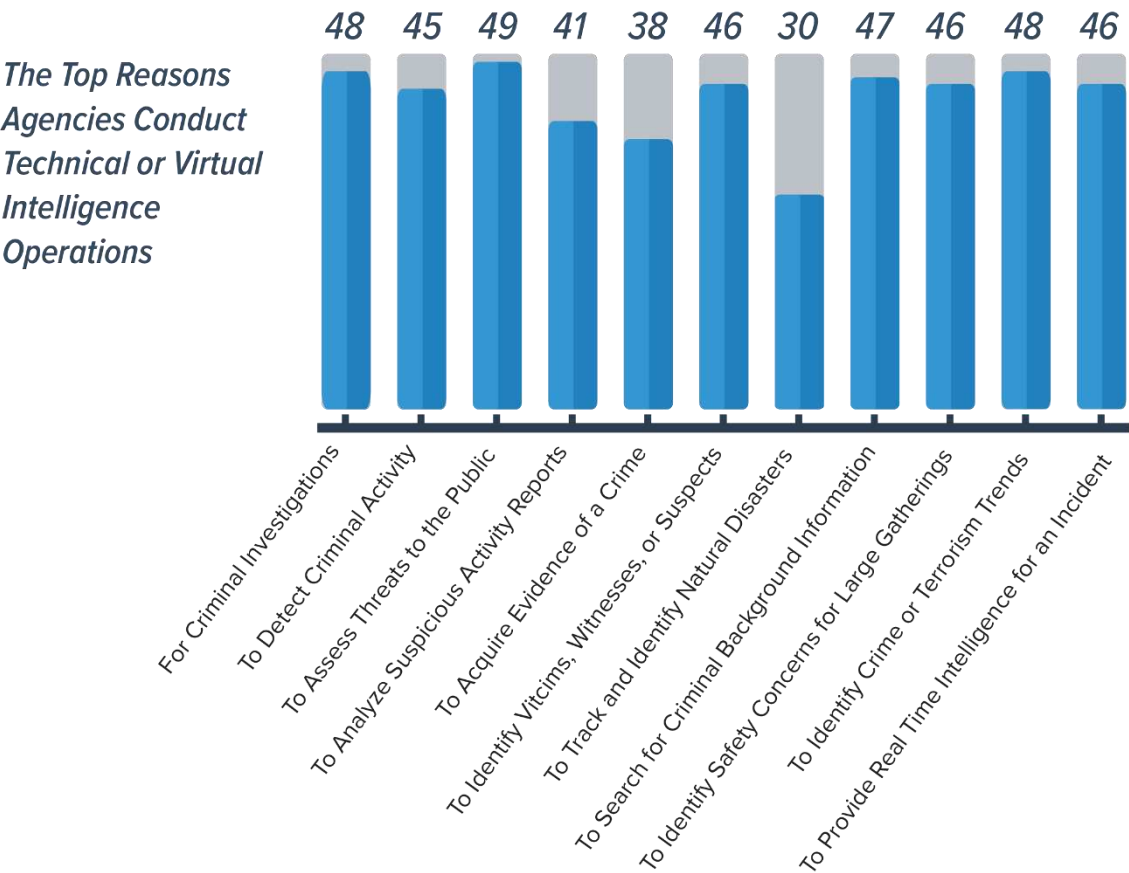
**Success Story - Real Time Cameras Used to Solve Home Invasion Case**

Officers arrived to a home invasion incident and quickly provided a description of the suspect to the Real Time Crime Center. The unit used this information to identify a subject matching the description in video surveillance and notified patrol of the location. Officers arrived on scene and took the suspect into custody within 15 minutes of the original crime. (Louisville Metropolitan Police Department)

**Success Story - Real Time Cameras Used to Prevent Violent Gun Crime**

The Technical Operations Section observed two suspicious persons standing in front of a convenience store while monitoring their real-time surveillance camera feeds. The camera operators zoomed in and watched one of the subjects retrieve a firearm from his waistband. The subject placed a magazine in the firearm and then appeared to insert a round. Patrol was notified in real-time and responded as the unit continued to provide intelligence. The subjects entered the store and then began looking out the window just as patrol was arriving in the area. The subjects then exited and tried walking away before they were apprehended. The subject with the firearm was arrested for possession of a stolen firearm before any possible violent crime could take place. (Las Vegas Metropolitan Police Department).

The most common reasons for conducting technical operations include supporting criminal investigations, assessing threats to the public, and identifying crime and terrorism trends. Additional categories that are also fairly common include providing real time intelligence during an incident and identifying victims and suspects. The least common purpose was for identifying and tracking natural disaster situations.

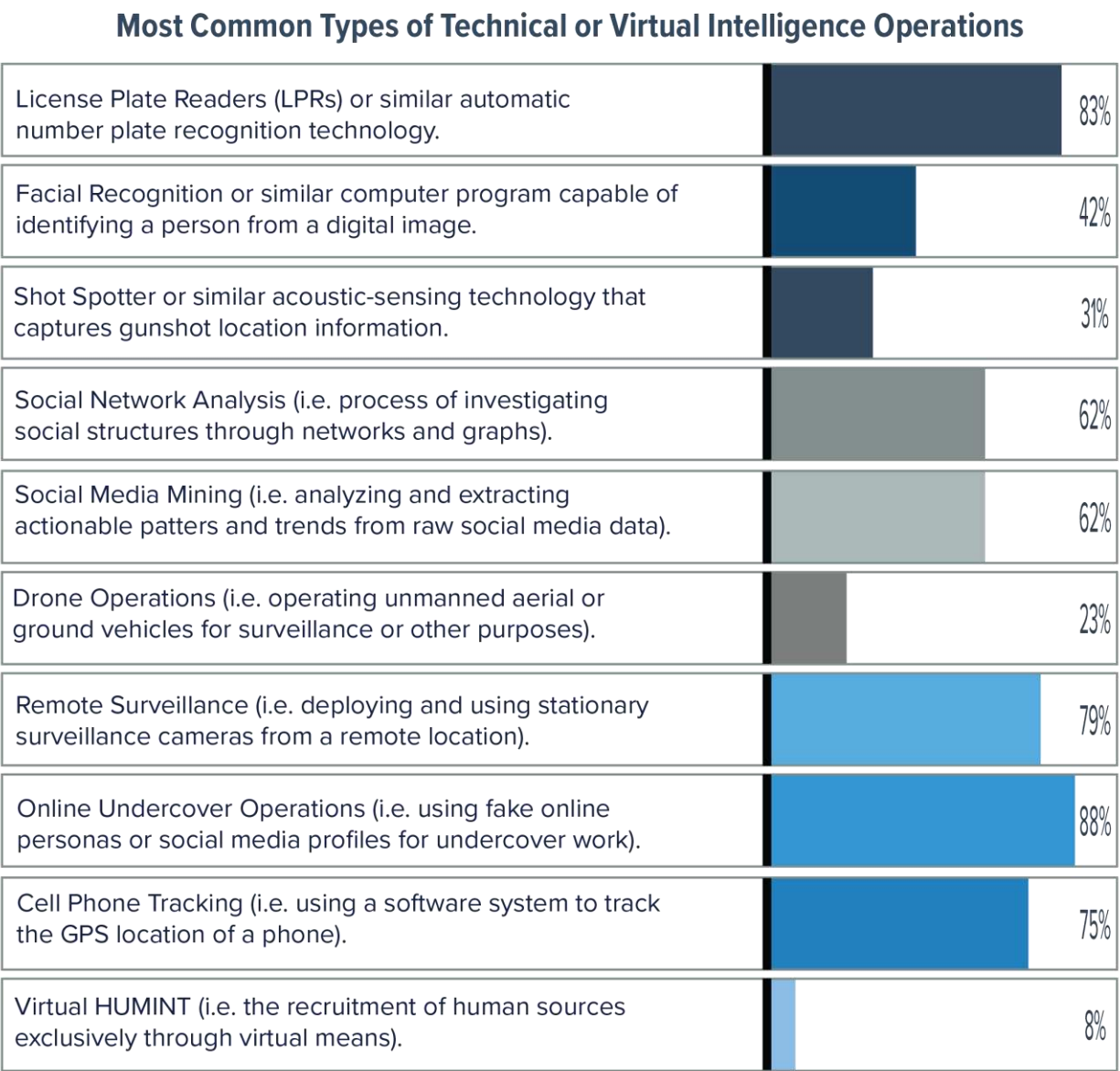


**Success Story - Prohibited Person Arrested Using Gunshot Detection Technology**

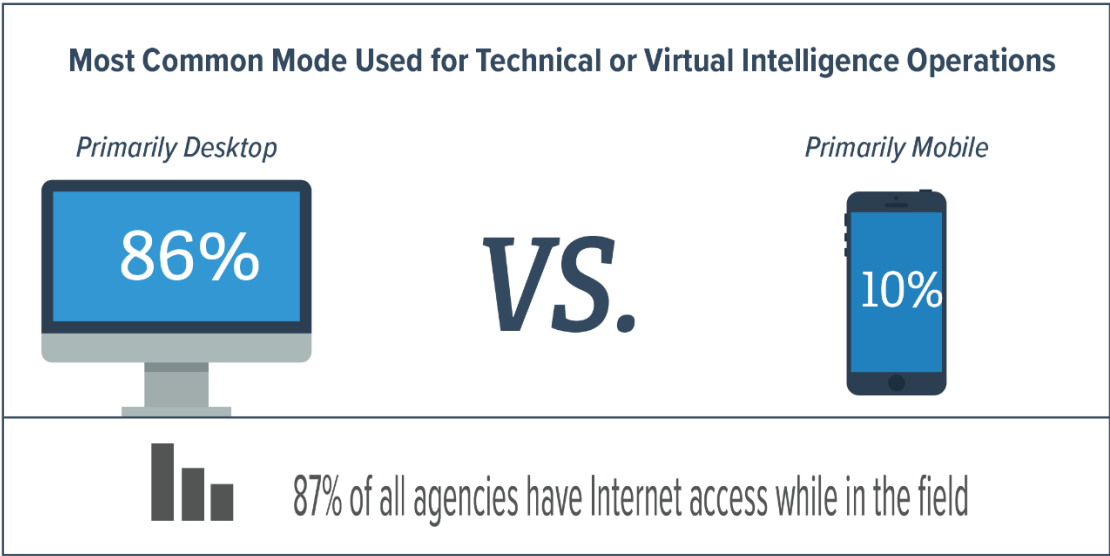
The Technical Operations Section used a gunshot detection technology to identify a shooting involving a single gunshot near an apartment complex. The shooting was not reported by any other means. The unit directed patrol to the exact location of the crime. Upon arrival, officers could not find any shell casings but did locate a witness that directed them to the suspect’s apartment. Patrol then gained a confession from the suspect, who admitted to shooting one round in the air. The suspect, who was on probation for selling narcotics, was arrested. The semi-automatic handgun used in the crime was recovered and impounded. (Las Vegas Metropolitan Police Department)



The majority of the agencies surveyed use license plate readers, social network analysis, social media mining, remote surveillance, online undercover operations, and cell phone tracking to combat crime. While far less common, some agencies also conduct drone operations and virtual Human Intelligence (HUMINT). Human intelligence is information gathered through human interaction, so virtual human intelligence is information gathered through human intelligence via digital communications.



The far majority of agencies surveyed are primarily using desktop computers instead of cell phones to conduct technical operations. While expected for the current environment, there is some indication this will rapidly change to more mobile use in the near future.



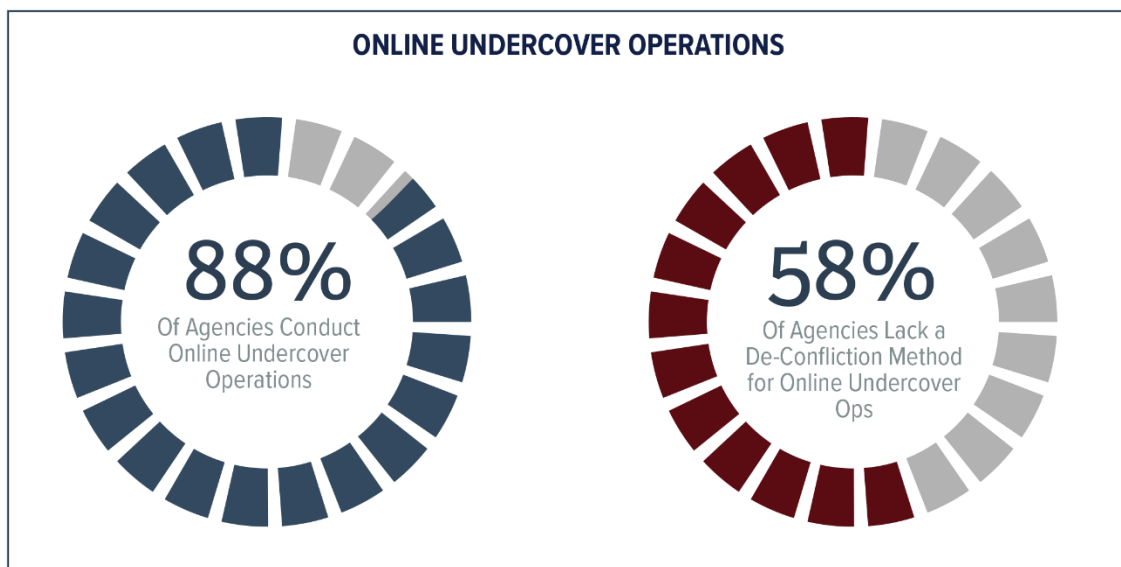
**Success Story - Triple Homicide Suspect Located Using Technical Surveillance**

The Technical Operations Section assisted on a triple homicide investigation, where the suspect was thought to have access to a cell phone device. A technical collection effort was conducted, which revealed a possible location for the suspect. This intelligence ultimately led to the apprehension of the suspect. (Las Vegas Metropolitan Police Department)

**Success Story - Open Source Research Solves Series of Armed Robberies**

During an investigation of multiple armed robberies, surveillance video and witnesses provided a description of the getaway vehicle and suspect. Knowing this vehicle was not incredibly common, analysts searched open sources and were able to locate the vehicle on a sales website. Analysts were able to use the photo of the vehicle and social media monitoring to locate the individual who submitted the post. An interview led to the identification of a suspect and charges filed. (Oklahoma City Police Department)

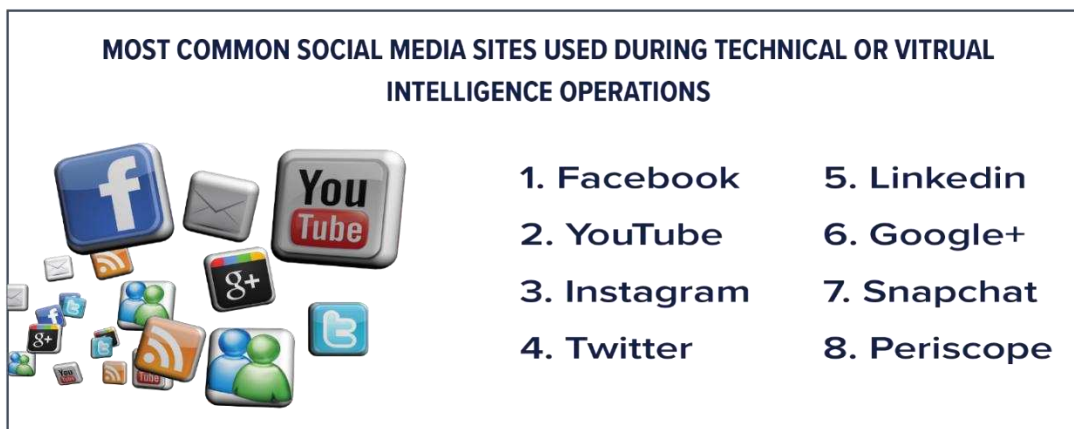
Although the far majority of agencies surveyed are conducting online undercover operations, only 42% have a de-confliction mechanism in place for these operations.



#### **Success Story - Social Network Analysis Used to Reduce Violent Crime**

In the second half of 2014, the City of Milwaukee experienced a 74% increase in motor vehicle thefts compared to the same period the previous year. An analysis of the trend revealed the crimes were committed by youthful offenders that would use the stolen vehicle to facilitate multiple thefts and robberies. In an effort to be proactive, crime analysts developed a predictive method that factored in a number of variables to assist in identifying the offenders. The variables included criminal history data, social network analysis, and threat assessments. One of the factors included reviewing open source information through social media platforms. The program was dubbed the Network of Criminals (NOC) program. and since its inception there has been a downward trend in the motor vehicle theft and robbery crime categories. The Milwaukee Police Department found that 62% of NOC offenders were arrested for a motor vehicle theft, robbery, or gun offense within 90 days of being highlighted by the NOC program. (Milwaukee Police Department)

The most common social media sites used in technical and virtual intelligence operations included Facebook, YouTube, Instagram, and Twitter. These results are not surprising since they match what are some of the most popular social media sites in the general public. However, the use of social media as an intelligence collection tool does come with limitations, especially when the information is based on protected speech. It is critically important that agencies conducting open source analysis of social media information must ensure they are doing so in a manner that protects privacy, civil rights, and civil liberties.<sup>4</sup>



#### **Success Story - Social Media Research Helps in Homicide Case**

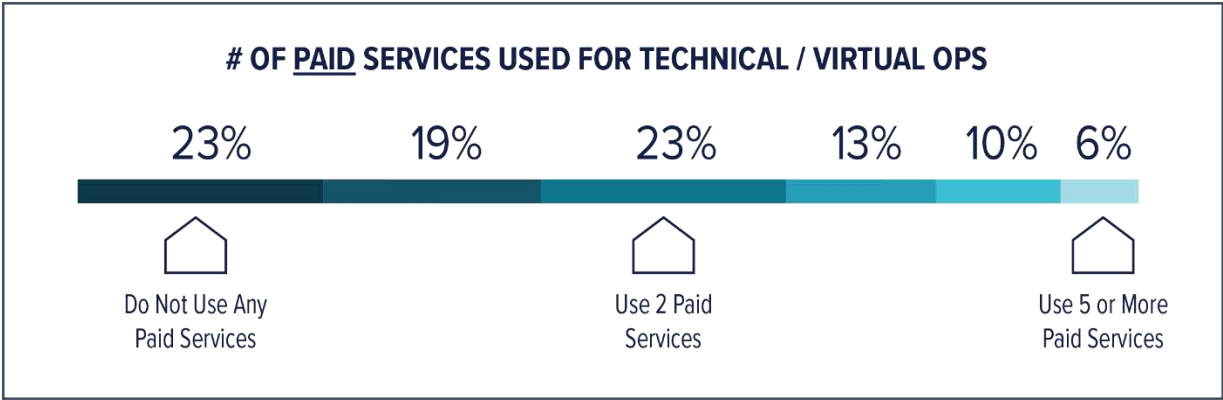
The Social Media Unit found a profile on Instagram for a homicide suspect, as well as a video he posted the night of the shooting that showed the same caliber firearm. This information helped the homicide detectives move forward with the case and arrest the suspect. (Baltimore Police Department)

#### **Success Story – Social Media Used to Prevent a Possible Attack**

In August 2015, two individuals planning to attend the Pokémon World Championship in Boston were engaging in online harassment and threats against another participant. Intelligence analysts evaluated social media messages that included photos of weapons and threatening statements. The information was shared with law enforcement and security, and the police were notified shortly thereafter that the two individuals were attempting to enter the event. The individuals were stopped and following a search warrant, police recovered a shotgun and an AR-15 rifle each with over 100 rounds of ammunition. (Boston Police Department / Boston Regional Intelligence Center)

<sup>4</sup> State, Local, and Federal Law Enforcement and Homeland Security Partners. (2017). Real-Time and Open Source Analysis (ROSA) Resource Guide. Bureau of Justice Assistance.

The majority of the agencies surveyed use less than two paid services for conducting technical or virtual intelligence operations and nearly a quarter do not use any paid services.



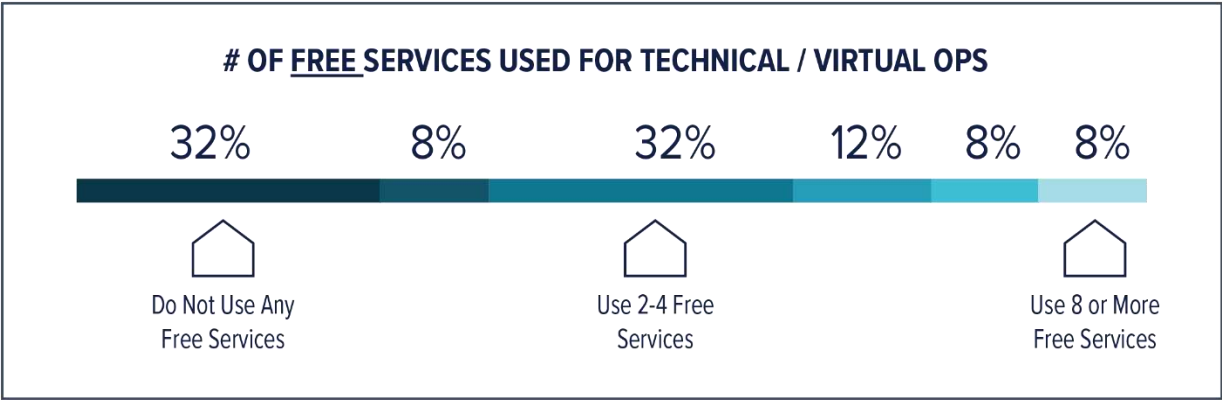
**Success Story - Social Media Research Leads to Wanted Suspect**

Detectives were attempting to locate a suspect who had a warrant. All of the possible addresses were checked but the suspect could not be located. A social media search revealed the suspect's Facebook account. The suspect posted a photo in front of an ordinary brown home. Analysts were able to identify the address of the home using Google Maps. The following day, the suspect posted a video on the porch of the home, allowing detectives to immediately make contact and arrest him. (Oklahoma City Police Department)

**Success Story - Serial Sexual Predator and Attempt Homicide Suspect Captured**

A suspect met a prostitute from a social media site and lured her into a vacant apartment, where he sexually assaulted her and slit her throat. The same suspect did the same thing a month prior. After the second event, the Technical Operations Section deployed a number of technical surveillance tools to help identify and locate the suspect. This technical collection effort was instrumental in capturing the suspect. (Las Vegas Metropolitan Police Department)

The majority of the agencies surveyed use less than five free services for conducting technical operations and a few agencies use eight or more free services.



**Success Story - Online Research Identifies a Homicide Suspect**

An analyst identified a robbery where a victim was shot in the face. The victim listed a moniker for the suspect online, which was used to identify his true name. The analyst was also able to identify location information using various online research tools. The suspect was later arrested and connected to multiple robberies, as well as another homicide. (Oklahoma City Police Department)

**Success Story - Social Media Research Strengthens a Criminal Prosecution**

In a 2017 conviction of a gang member on RICO charges, video found on social media was useful in proving gang membership and information about weapons and money. This helped to convince the jury that the activity was not just an act, as the defense had tried to establish. The larger RICO conspiracy in this case included murders committed by the gang members in furthering their enterprise. (Buffalo Police Department)

**Success Story - License Plate Reader Used to Locate Double Homicide Suspect**

The Real Time Crime Center received a license plate alert on a vehicle related to a wanted subject for a double homicide and child abduction. The center monitored the suspect vehicle via live feed from cameras and provided updates to responding units. Units located the suspect vehicle in a gas station and the driver was taken into custody. (Charlotte-Mecklenburg Police Department)

## CONCLUSION

As a whole, the research results of this preliminary report indicate a growing investment in technical and virtual intelligence operations within law enforcement. The data shows most agencies are already deploying fairly advanced technologies to identify and capture criminals. There are also some new technologies to include drones that are already being deployed within a limited number of agencies. Beyond the rising level of use, there is also demonstrated value in using technology to fight crime and terrorism. As demonstrated in the limited sampling of success stories, technical and virtual intelligence operations are proving quite effective in preventing violence before it occurs. These early successes reveal a tremendous amount of potential for the use of technology in law enforcement. Perhaps, more importantly, they also usher in a new era in policing that will likely be heavily dependent on virtual crime fighting strategies.

### **Success Story - Social Media Research and Cell Site Analysis Solves Serial Shooter Case**

Milwaukee police officers reported a gang house as being targeted and shot into on three different occasions. The casings at the scene were analyzed by National Incident Ballistics Identification Network (NIBIN) technicians and found to be highly probable that they were fired from the same handgun. In one incident, a named suspect was arrested. A review of social media revealed critical intelligence that assisted in obtaining the search warrant for the account. The NIBIN leads and technical collection efforts allowed investigators to: identify seven suspects, including the person previously mentioned as the common denominator in all cases; clear two non-fatal shootings; clear eight shots fired incidents; clear eight shots fired into a residence or auto; and clear two armed robberies. The associations made through social networking analysis allowed investigators to recover several handguns and key pieces of evidence before the information became stale. (Milwaukee Police Department)

### **Success Story - Online Research Tool Identifies Robbery Suspects**

Using the subject and vehicle descriptions provided by security cameras, multiple potential suspects were checked through the Law Enforcement Information Exchange (LinX). One of the suspects had a recent traffic stop by another agency and provided a local address during the encounter. Using additional databases along with open source searches that included social media, a positive match to the robbery suspect was confirmed. Within a matter of days of the robbery, the suspect was identified and, shortly thereafter, in custody. (Loudon County Sheriff's Office)



## ACKNOWLEDGEMENTS

The production of this chapter would not have been possible if not for the many partners and participants that contributed throughout the process. In particular, a special thanks to the Bureau of Justice Assistance (BJA), Major Cities Chiefs Association (MCCA), Major County Sheriffs of America (MCSA), the MCCA Homeland Security Committee, and the Intelligence Commanders Group.

### ICG TECHNICAL AND VIRTUAL OPERATIONS COMMITTEE

Deputy Chief Chris Jones (Chair)  
Las Vegas Metro Police Dept

Inspector Walt Smith  
Philadelphia Police Dept

Lieutenant Dori Koren  
Las Vegas Metro Police Dept

Tara Richardson  
Major Cities Chiefs Association

Assistant Chief John Sullivan  
Albuquerque Police Dept

Lieutenant Ron Maugans  
Charleston County Sheriff's Office

Captain David Salazar  
Milwaukee Police Dept

Sergeant Eric Schlapia  
Omaha Police Dept

Deputy Chief Jeff Matthews  
Arlington Police Dept

Ann Long  
St. Louis Police Dept

Captain Chris Wundrach  
Oakland County Sheriff's Office

Assistant Chief David Carabin  
Boston Police Department

Sergeant Chad Baker  
Orange County Sheriff's Dept

Lieutenant Kevin Armbruster  
Milwaukee Police Dept

### PARTICIPATING AGENCIES

Arapahoe County Sheriff's Office  
Arlington Police (Texas)  
Atlanta Police Dept  
Aurora, Colorado Police Dept  
Baltimore County Police  
Boston Police Dept  
Buffalo Police Dept  
Charleston County Sheriff's Office  
Charlotte-Mecklenburg Police Dept  
Dallas Police Dept  
Dane County Sheriff's Office  
Essex County Sheriff's Dept  
Hennepin County Sheriff's Office  
Honolulu Police Dept  
Houston Police Dept  
Jacksonville Sheriff's Office  
Jefferson County Sheriff's Office  
Kent County Sheriff

Kern County Sheriff's Office  
Lake County Sheriffs Office  
Las Vegas Metro Police Dept  
Long Beach Police Dept  
Los Angeles County Sheriff's Dept  
Los Angeles Police Dept  
Loudoun County Sheriff's office  
Louisville Metro Police Dept  
Memphis police Dept  
Miami-Dade Police Dept  
Milwaukee Police Dept  
Minneapolis Police Dept  
Montgomery County Dept of Police  
Montgomery County Sheriff's Office  
New Orleans Police Dept  
Oakland County Sheriff's Office  
Oklahoma City Police Dept  
Omaha Police Dept

Pinellas County Sheriff's Office  
Prince Gregory's County Police Dept  
Raleigh Police Dept  
Salt Lake City Police Dept  
San Antonio Police Dept  
San Bernardino County Sheriff's Dept  
San Diego Police Dept  
St. Louis Metro Police Dept  
Stanislaus County Sheriff's Dept  
Tampa Police Dept  
Toronto Police Service  
Tulsa Police Dept  
Vancouver Police Dept  
Venture County Sheriff's Office  
Virginia Beach Police Dept  
Washington DC Metro Police Dept

**For questions or comments about this report or the related research, please contact Lieutenant Dori Koren at [D9007K@lvmpd.com](mailto:D9007K@lvmpd.com).**

# **Critical Issues for Intelligence Commanders**

**Chapter Two: Preventing Terrorism and Targeted Violence**

## Chapter Two: Preventing Terrorism and Targeted Violence

### Executive Summary

It has often been said that local law enforcement agencies are likely to be the ones to detect the next terrorist threat or planned attack. Much has been discussed about the approaches for countering violent extremism through community outreach, but law enforcement Intelligence Commanders represent a different side of the coin. This white paper is an opportunity for Intelligence Commanders and the Intelligence Commanders Group to reaffirm their role in preventing terrorism and identify what is needed to make sure we have the best chance for preventing terrorism and targeted violence.

Preventing terrorism and targeted violence is a complicated responsibility. Not only are there endless ways and locations of carrying out these attacks, but there is no one type of person or set of indicators that will predictably lead to identifying a potential attacker. Additionally, the terrorist threat is no longer coming from just a centralized foreign terrorist organization, but there are the homegrown violent extremists that may not have any connection to a central terrorist organization and have just been inspired by and vulnerable to violent messaging. They also may be using tactics that require low technology and little advance preparation and planning and can be carried out by a single individual, making it all the more difficult to identify and prevent. This makes the Intelligence Commander role of prevention all the more vital. Because of the global view of these issues held by the Intelligence Commander they not only focus on their traditional role of intelligence collection and analysis, but they also look to make their own agency and community as educated and capable as possible since this is too large an issue to handle alone. It requires a complete set of partnership at the local, regional, federal, and international level.





There are much more detailed guides on how to operate, but this chapter is meant to identify the scope of the Intelligence Commander's primary and secondary responsibilities to most effectively combat the complex threat of terrorism and targeted violence. It also identifies high-priority areas where law enforcement agencies and Intelligence Commander operations need support or where there are opportunities for improvement that have the potential to make a large impact against the threat. While the list is long, it only scratches the surface. The critical role the Intelligence Commander plays across the organization for positively impacting crime and terrorism concerns cannot be overlooked.





A committee of Intelligence Commanders from the Intelligence Commanders Group convened a series of meetings to establish these priority needs and recommendations through a project that was made possible from a grant from the Department of Justice Bureau of Justice Assistance. This is just one example of the types of partnerships that are needed to build a complete prevention program. Law enforcement agencies already thrive and rely on partnerships. Whether that is with their communities, local public sector partners, the private sector, fusion centers, other law enforcement agencies or the federal government.

The Intelligence Commanders Group helps to bring this all together to support Intelligence Commanders in their role to prevent terrorism and targeted violence. The Intelligence Commanders fulfill a unique role in their agency and they maintain a unique connection among all of member agencies of the Intelligence Commanders Group across the country.

Please see the table that follows for a list of the recommendations and needs identified for this project. Also, please see the two other related white papers that are a part of this series related to Intelligence Commander Operations:

- Technical and Virtual Operations
- Maintaining Investigative Resources

	Recommendations and Needs	Federal Support Needed
 	<b>Increasing Intelligence Commander Collaboration and Information Sharing</b>	
	Increase support for the Intelligence Commanders Group	✓
	Reinforce the importance of the Intelligence Commander roles of establishing information needs, collection, and analysis to support agency operations and investigations	
	Improve real-time information sharing (steady state and emergency) among Intelligence Commanders	✓
	Collaborate on strategies to address common and migrating threats	✓
	Support the role of the Intelligence Commander and select candidates that will be good for role	
	Build Intelligence Commanders for the future	✓
	Build a formalized National Prevention Program	✓
	<b>Advancing Agency Capabilities</b>	
	Reinvigorate Terrorism Liaison Officer programs	✓
	Consider implementing a Field Intelligence Officer Program	✓
	Increase the number of in-house intelligence analysts	✓
	Establish international police agency partnerships	
	Continue to maintain special operation and human source capabilities	
	Identify additional justice system capabilities – state terror laws, injunctions	
	Follow-up on all Tips and Leads	
	<b>Intelligence and Analysis</b>	
	Support regular completion of agency and national threat assessments	✓
	Conduct year-to-year threat assessment analysis to better identify opportunities to collaborate against threats	✓
	Identify successful mitigation strategies and share with ICG membership	✓
	Embed analysts in fusion centers	
	Make technology investment a priority to improve collection and analysis	✓
	Foster technology innovation to improve collection and analysis	
	<b>Agency-Wide Training</b>	
	Provide training to investigators to increase their understanding of intelligence collection and analysis	✓
	Have agency leadership participate in training on intelligence and terrorism	✓
	Increase training opportunities for analysts	✓
	Take advantage of free training for analysts, leadership, and Intelligence Commanders through DHS and FBI	✓
	Continue to make training on source development a priority	
	Deliver Terrorism Liaison Officer training to all levels of an agency	
	Include officers, dispatch, and other government partners in awareness-level intelligence and counterterrorism training	

	<b>Federal Collaboration</b>	
	Need increased support through funding, personnel, training, and technology tools	✓
	Formalize a partnership with DHS, FBI, BJA, and other federal agencies to formalize an Intelligence Commander best practice program	✓
	Pair local and federal analysts - embed FBI analysts in local law enforcement agencies and local law enforcement agency analysts in JTTFs	✓
	Work closely with the FBI to follow-up on cases that do not rise to the level of a JTTF case	✓
	Work closely with DHS to share intelligence and best practice information	✓
	Work closely with Customs and Border Protection (CBP) to share intelligence and follow-up with identified individuals	✓
	Incorporate terrorism prevention activities into grant funding	✓
	Streamline federal information sharing systems	✓
	Build closer partnership with the Terrorist Screening Center and ensure guidelines are followed	✓
	Reinvigorate National Suspicious Activity Reporting Initiative (NSI)	✓
	Participate in federal task forces	✓
	<b>Partner Collaboration</b>	
	Partner with mental health, crisis response, and other social service groups to address people in crisis or at risk for using violence	✓
	Incorporate the use of behavior toolkits to inform assessments of whether a person is at risk for using violence	✓
	Turn partnerships into more formal off-ramp programs	✓
	<b>Private Sector Collaboration</b>	
	Establish a formal private sector outreach program	
	Educate, train, and inform private sector partners	
	Find opportunities for real-time and critical information sharing with private sector partners	
	Embed private security analysts in local law enforcement agency Intelligence Commander operations	
	Work with social media outlets to identify violent extremist content for removal	
	<b>Community Outreach (outside direct Intelligence Commander responsibility)</b>	
	Continue law enforcement agency outreach to all communities	
	Support community organizations working on violence prevention and resiliency programs	
	Increase public awareness of indicators of terrorism and violence and help them understand the importance of their tips	
	Increase public awareness of support resources that can provide an off-ramp alternative	✓
	Reinvigorate "See Something, Say Something" program to increase quality public reporting	✓

## Increasing Intelligence Commander Collaboration and Information Sharing

Working together to identify successful mitigation strategies and share information on current and evolving threats is the only way our communities and our nation will be able to prevent terrorism and targeted violence. This is the valuable role the Intelligence Commander and Intelligence Commander Group plays in the national security and Information Sharing Environment, which is why it is the first area addressed by this white paper.

### Recommendations and Needs

- Increase support for the Intelligence Commanders Group
- Reinforce the importance of the Intelligence Commander roles of establishing information needs, collection, and analysis to support agency operations and investigations
- Improve real-time information sharing (steady state and emergency) among Intelligence Commanders
- Collaborate on strategies to address common and migrating threats
- Support the role of the Intelligence Commander and select ideal candidates for role
- Build Intelligence Commanders for the future
- Build a formalized National Prevention Program

**Increase support for the Intelligence Commanders Group.** The value of the Intelligence Commanders Group to work together to prevent terrorism, targeted violence, and violent crime has been increasingly recognized among its member agencies and partners. It is the only national forum for the discussion and analysis of intelligence related issues, information sharing, and identification and sharing of best practices at the city and county level. Maintaining a national network of major city and county Intelligence Commanders allows for rapid information exchange in a diverse and very fluid threat environment. Accurate and timely information exchange is paramount in the prevention of terrorism and targeted violence. Prevention is the first line of defense for our nation against terrorism and other attacks. The Intelligence Commanders are the country's preeminent experts in information sharing operations that are needed to prevent these attacks and their insights and expertise needs to be harnessed as a collective for the greater good of the nation. *Local law enforcement agencies should continue to dedicate personnel and resources to participate in this group, and dedicated federal funding is needed to sustain this collaboration.*

**Reinforce the importance of the Intelligence Commander roles of establishing information needs, collection, and analysis to support agency operations and investigations.** While each department has a slightly different structure, the primary roles of the Intelligence Commanders are establishing information needs, collection, and analysis to support agency operations and investigations. They also provide the local context to national threat trends. With each incident and change in trends they reevaluate information needs and collection requirements that are then shared with the field. They come up with new and innovative methods for collecting information from the field, like through debriefing forms for officers to use in the field and are based on the idea that most terrorism begins with crime, so a few questions added to debriefing forms helps capture terrorist related information. This also serves to remind officers of the potential link between crime and terrorism and helps them remember the signs. They also improve collection through the development of sources, but source development has become more complicated. With there now being a criminal element in the gang world that has been radicalized, outreach to these groups can help identify extremist activity, especially homegrown violent extremists and can help with source development. As attacks become more and more difficult to detect as attackers use low tech methods, whether by using a steak knife, their own car, or a rental to carry out an attack, traditional methods of analyzing information and looking for links, indicators, and precursor events are harder to uncover. Also, with the loss of access to many sources of information because of the Going Dark issue, Intelligence Commanders are having to identify new sources, look for new indicators, and think about new ways of analyzing this information. Traditional means of collection and analysis are still important, like looking at financial transactions to identify precursor and monitoring communications from overseas, but these increasingly need to be augmented by additional capabilities. Tips and leads that come from the public and private sector also continue to be a valuable source for information that Intelligence Commander rely upon. *Local law enforcement agencies should continue to increase emphasis on this priority.*

**Improve real-time information sharing (steady state and emergency) among Intelligence Commanders.** This includes identifying a means for more easily communicating with individual agencies or the group as a whole and identifying a means for sending real-time alerts to all membership. Monthly conference calls with agency promising practice briefings is one solution. These calls would foster continuing participation and including a roundtable discussion has the potential to identify opportunities for collaboration against common threat issues. For emergency situations, including immediately after an attack, during an increased threat level, or when there is a suspected impending threat affecting one or multiple agencies there is also an opportunity for this group to provide increased support. They can enlist their analysts to support information requests, so they can focus on managing the incident. Ideas include developing a regional plan where each agency would have a regional partner identified as their support agency. There is also a need to identify ways to quickly push information to the entire membership when an affected agency has information they believe would be valuable for the collective. Ideas have included using an online portal to push information or having a regional partner push the information to the membership. Agencies could also be convened for immediate information sharing based on a more formalized plan for how to convene affected agencies to address an impending threat or response to an attack. An online communications portal that fosters ongoing communications and makes outreach and information sharing streamlined for the whole group is needed. *The ICG should make this a priority and other federal partners are needed to provide resources.*

**Collaborate on strategies to address common and migrating threats.** Closer communication will help Intelligence Commanders to identify opportunities and needs for collaborating against common and migrating threats. Regular gatherings, whether general in nature or to examine a specific topic, like was done with this project, results in exchanges of information and best practices that set the stage for closer collaboration on strategies against these threats. This might include a group of agencies working together to stop a known common threat or developing more proactive strategies across all member agencies for how to handle situations that do not meet the FBI's threshold for involvement, knowing that just because a situation does not rise to the level of the JTTF today does not mean it will not tomorrow. The ICG can also work to examine the written terrorism and targeted prevention strategies of each agency or support agencies to document their existing strategies to identify opportunities for building on existing strategies and where there might be opportunities for new approaches. The information sharing that resulted from this project provided a great starting point for identifying these strategies and now further targeted planning sessions can support agencies to move forward to collaborate on these coordinated strategies. *The ICG should make this a priority and other federal partners are needed to provide resources and coordination.*

## Increasing Collaboration Opportunities

**MCCA/MCSA Intelligence Commanders Group:** Intelligence Commanders from member agencies are encouraged to take advantage of the collaboration opportunities with this group. There is also great value in virtual communication, but it is still vital to maintain opportunities throughout the year to bring the group together or bring together sub groups around specific issues.

**Joint Terrorism Task Forces:** as the FBI's local arm of their counterterrorism efforts, Intelligence Commanders rely greatly on the quality of this partnership for increasing collaboration and information sharing. This is one of the most important partners for local agencies in their efforts to prevent terrorism and violent extremism and needs to be further fostered.

**Fusion Centers:** these are extremely valuable venues for collaboration with public safety in a region and with the local operations of federal agencies. Many law enforcement agencies manage their local fusion centers through their own operations, which increases their effectiveness for fostering collaboration and information sharing.

**Operation Sentry:** is a counterterrorism coalition operated by the NYPD with over 450 agencies participating from around the world. They work to monitor all events and share information with local, regional, and national partners. They also host an annual conference for all members. Participants are encouraged to share information and best practices with members to make all more prepared and capable to prevent future incidents.

**Criminal Intelligence Coordinating Council:** supports state and local law enforcement and homeland security agencies in their ability to develop and share criminal intelligence and information nationwide. The Intelligence Commanders Group participates in this vital forum.

**Regional Monthly Meetings:** if you live in a region with several law enforcement agencies, consider having monthly regional meetings with Intelligence Commanders from all agencies and including other partner agencies. Washington, DC holds regional meetings with all Intelligence Commanders from nearby law enforcement agencies and partner agencies to increase information sharing and collaboration. They also maintain an email distribution group for critical real-time sharing.



**Support the role of the Intelligence Commander and select ideal candidates for role.** It is important to ensure an Intelligence Commander is someone that is willing to work with everyone, since information sharing with many different groups is their role and is what makes them effective. Support from agency leadership is important as well to take the greatest advantage of the value this role brings to the entire organization. While the role of the Intelligence Commander may be a stepping stone to the next level of leadership in the department, there is value to the individual and the agency in minimizing the turnover in this position or at least having a strong organizational transition plan in place. Intelligence Commanders should build in time to provide regular updates to their Chief and leadership. This will help to continually demonstrate the value of the position, while also ensuring leadership has the most current information to inform agency priorities and resourcing. *Local law enforcement agencies should make this a priority.*



Oklahoma City man threatens mass shootings in Oklahoma City and San Antonio

#### **Field Examples: Increased Information Sharing and Collaboration**

The Oklahoma City Police Department was notified of a subject making threats to commit a mass shooting in San Antonio, Texas. The subject posted on social media that he was in Oklahoma City and was going to kill people there before driving to San Antonio to shoot people in a bar district. The Oklahoma City Police Department contacted the San Antonio Fusion Center who had also been made aware of the post. They worked together to locate the subject in Oklahoma City and take him into custody. He was ultimately charged in both jurisdictions for terroristic threats. It was a great example of multiple agencies working together and sharing information to interdict a possible mass shooting.

**Build Intelligence Commanders for the future.** Our member agencies have developed some tremendous Intelligence Commanders who are global leaders in preventing terrorism and targeted violence. Recognizing the critical and specialized role played by the Intelligence Commander it is important to examine what it takes to build the counterterrorism leaders of the future and identify guidelines agencies can use. *The ICG should make this a priority in conjunction with federal partners.*

**Build a formalized National Prevention Program.** Ultimately, a coordinated Prevention program is needed that looks at all aspects of the effort to prevent terrorism and targeted violence. Law enforcement and the Intelligence Commanders will be a significant part of that, but there are many federal, private, and community partners that are needed to develop this, direct resources to these areas, and implement it. A national framework could be built to address the capabilities and needs of multiple segments, like the Intelligence Commanders and local law enforcement, and then fuse them into a coordinated approach. This white paper can serve as a starting point for certain aspects of that program. *Local law enforcement agencies should work together to establish their components of a National Prevention Program and the federal government should support bringing together collective partners.*

## **Advancing Agency Capabilities**

Local law enforcement agencies have made great advancements in their intelligence and prevention efforts in both the criminal and terrorism realms. There continue to be new promising approaches worth integrating into existing operations, opportunities to improve existing efforts, and a need to reinvigorate valuable programs that may have declined without support.

#### Recommendations and Needs

- Reinvigorate Terrorism Liaison Officer programs
- Consider implementing a Field Intelligence Officer program
- Increase the number of in-house intelligence analysts
- Establish international law enforcement agency partnerships
- Continue to maintain special operation and human source capabilities
- Identify additional justice system capabilities – state terror laws, injunctions
- Follow-up on all Tips and Leads
- Maintain or establish a real-time crime center

**Reinvigorate Terrorism Liaison Officer programs.** Terrorism Liaison Officer (TLO) programs (also known as fusion liaison officers and intelligence liaison officers) were established by local law enforcement agencies and fusion centers to increase awareness of terrorism indicators and increase information reporting back to intelligence operations among all public safety disciplines. In many departments, these have lost momentum despite their value. These TLO programs need to be reinvigorated with fresh training to reflect the current threat environment and the appointment of a TLO Coordinator in each department. This goes hand-in-hand with the reinvigoration of the National Suspicious Activity Reporting Initiative (NSI) addressed in the Federal Collaboration Section. TLOs can also be good tool for encouraging closer collaboration with the local fusion center, since many fusion centers have embraced this program.

TLOs are basically officers on the street who have a heightened level of awareness of suspicious activities related to terrorism and targeted violence threats, know what to do when they come across those type of activities to maximize the information, and know where that information needs to be reported. The Intelligence Commander operations can then continue to take information from TLOs to inform their operations and drive information collection requirements back to the street level – all part of the intelligence cycle. Any member of any public safety or private sector organization (with a slightly different focus and training, please see the NYPD Shield program in the Private Sector Outreach section for more detailed information) can be trained as a TLO and they act as a force multiplier. The San Diego Police Department and others have had success integrating basic TLO training into their academy training for new recruits so that the whole agency receives this important initial training. *Federal support would be valuable to maintain training materials and technical assistance.*

**Consider implementing a Field Intelligence Officer (FIO) program.** The mission of this program, established by the New York Police Department, is to identify, collect, and disseminate accurate information and intelligence and to assist in the identification of individuals responsible for or associated with specific crimes for the purpose of crime reduction within New York City. The program has over 120 sergeants - one from each precinct – and has a tremendous success record. In 2017, the FIO program reached milestone accomplishments pertaining to intelligence driven policing: the program finished the year by recovering a total of 1,225 firearms based on information initiated by the FIOs. This was an increase of 4% over 2016. Also, in 2017, 38% of agency search warrants and 22.6% of guns seized by NYPD were initiated because of this program. The duties and responsibilities of a FIO remain fluid and are constantly changing to reflect the current crime trends throughout the city. Some other departments have started to implement elements of the program on a narrower basis. San Diego uses their gang unit and uniformed gang suppression team and Cleveland uses their vice officers to interview as many as possible after an arrest. *Federal support for documenting the programs practices and success factors would be valuable to help agencies implement the most important elements of this impactful program.*

**Increase the number of in-house intelligence analysts.** Many local law enforcement agencies still struggle to have and maintain a cadre of dedicated criminal intelligence analysts. A reduction in local law enforcement resources has made it

difficult to have the funding for these positions. The value of these analysts is that they can help to identify where the agency should focus limited resources and makes them more successful in those efforts. Even if an agency maintains a limited number of analysts, this will enable agencies to increase the benefit of analysts that may be embedded from federal agencies. In-house criminal intelligence analysts are the only ones who have the perspective of policing the local community. Some agencies have had success in taking motivated non-sworn personnel from within the department and giving them the training they need to become analysts. *Local governments and law enforcement agencies should make this a priority and federal grants should support funding these positions.*

**Establish international police agency partnerships.** Crime and terrorism have had an increasing international nexus. Additionally, there have also been instances where criminal activity and attack plots have been identified by foreign police agencies. These direct relationships can only help when a critical or time sensitive situation arises. Local agencies can connect with international police agencies through direct exchanges, conferences, or involvement in federal projects designed to support international police partnerships. Direct relationships should also be maintained with Interpol and with the State Department to coordinate international exchanges and formal information assistance requests relative to foreign nationals. *Local law enforcement agencies should make this a priority.*

**Continue to maintain special operation and human source capabilities.** These are still important and critical capabilities that must be maintained by law enforcement agencies. While technology and signals intelligence are vital sources of information, human intelligence still makes the difference. *Law enforcement agencies should continue to use this as a vital tool and ensure training is available to maintain these capabilities and skills for supervisors, operators, and analysts.*

**Identify additional justice system capabilities, including state terror laws and court injunctions.** The justice system in each state has different tools apply to terrorism. When states have terrorism laws, it provides the flexibility to pursue a case at the state and federal level to take the best approach to safeguard the community against a threat. Not all states have terrorism charges, but some are considering their addition. Arizona's Criminal Code § 13-2308.01 and New York's Penal Section 490.25 are examples. For gang activity, there are gang injunctions, for sex offenders there is an ability to limit their Internet access. Gang injunctions are a court-issued restraining order that can be put into effect during gang investigations to prohibit certain activities, including contacting other gang members. It is a civil injunction, but it violated, results in criminal charges. This can address gang problems before they reach the level of felony crime activity, but a similar tool could apply to terrorist activity. In other countries, like Canada, they have peace bonds that allow the court to apply conditions to individuals of concern for terrorist activity (e.g., no use of Internet), but there is a challenge to enforce them successfully. The court can authorize home entry by law enforcement to make sure people are respecting the conditions. *Law enforcement agencies should work together to understand these additional justice system tools in all states.*

**Follow-up on all Tips and Leads.** Agencies are prioritizing to follow up on every tip and lead and some have organized this effort into a separate unit. These leads might come in through the public, TLOs, or others within the organization. Some agencies have found that even those tips or leads that may have seemed like they only had a criminal element ended up having a terrorism nexus. Then there are even those that seem far-fetched which ended up having merit. This is an important step in making sure threats do not fall through the cracks and is one important way to identify individuals who may be in crisis and in need of support. *Local law enforcement agencies should make this a priority.*



Arizona man convicted  
on Arizona state terror  
charges

### Field Examples: State Terrorism Charges

An 18-year-old Arizona man of Pakistani descent was convicted on Arizona state terrorism charges for plotting to attack government locations. He had also expressed an interest in attacking religious locations. When states have terrorism laws, it provides the flexibility to pursue a case at the state and federal level to take the best approach to safeguard the community against a threat. Not all states have terrorism charges and this should be something available as a tool in all states. Arizona's Criminal Code § 13-2308.01 and New York's Penal Section 490.25 are examples.

**Maintain or establish a real-time crime center.** Local law enforcement agencies can establish a centralized technology hub to identify patterns, stop emerging crime, and provide instant information to field officers and detectives to guide their daily priorities. This can also be the hub for most of the activity of the intelligence analysts and can be a space for collaboration between the intelligence analysts and operators. *Local governments and law enforcement agencies should make this a priority and federal grants should support funding these positions.*

## Intelligence and Analysis

Intelligence and analysis is the cornerstone of Intelligence Commander operations. To be able to effectively carry out these roles, Intelligence Commanders need a variety of tools to ensure the highest quality information is collected and that the volume and complexity of the data can be effectively analyzed to result in actionable intelligence to guide field operations.

### Recommendations and Needs

- Support regular completion of agency and national threat assessments
- Conduct year-to-year threat assessment analysis to better identify opportunities to collaborate against threats
- Identify successful mitigation strategies and share with ICG membership
- Embed analysts in fusion centers
- Make technology investment a priority to improve collection and analysis
- Foster technology innovation to improve collection and analysis

**Support regular completion of agency and national threat assessments.** The ICG established a standardized annual domain threat assessment (DTA) process that enables each agency to better identify, measure, and counter their priority threat groups and threat issues. Conducting a DTA helps agencies determine if they are focused on the right criminal threats and provides data to substantiate intelligence collection efforts. Providing intelligence personnel with focus and direction, establishing data that supports intelligence collection, and ensuring an agency is operating against the threat groups and issues that pose the greatest concerns are key elements of a successful intelligence unit. Agencies can only expect to be effective, appropriate, and efficient in their intelligence mission when they evaluate priorities and use a strategy to guide operations. The Threat Assessment Cycle depicted in Figure 1 marries with the traditional intelligence cycle and is the basis for the comprehensive threat assessment approach used by the ICG. Consistently completing assessments at least every year also helps to increase awareness and understanding throughout the agency, which has the effect of exposing a wider set of personnel to the threats they may not have realized were active in their areas. This then continues to improve information collection throughout the entire agency. Each year is a learning process. An automated online toolkit could help agencies conduct this online process, analyze the information, and serve as a pointer system for identifying other agencies confronting similar issues. *Local law enforcement agencies should continue to conduct comprehensive threat assessments on at least an annual basis, and federal funding is needed to enable the ICG to fulfill this important function.*

**Figure 1: Threat Assessment Cycle**



Conduct year-to-year threat assessment analysis to better identify opportunities to collaborate against threats. Completing the threat assessments on an annual basis provides an opportunity to analyze the collective member agency submissions on a yearly basis to detect national trends and migrations of threats. This will help to identify promising practices that might be driving down threats and develop collective strategies to counter the threat groups and issues. This will also help to increase awareness of common threats and increase information sharing between local agencies. *Local law enforcement agencies should continue to support annual national trend analysis, and federal support is needed to harness this collective knowledge.*

**Identify successful mitigation strategies and share with ICG membership.** When strategies have been identified to

mitigate threats, it is important to quickly identify, document, and share the approaches with other local law enforcement agencies. Not only will this increase awareness for possible strategies to adopt, but if multiple agencies exhibit success using similar methods, it will help to verify their status as best practices. The challenge has been that agencies do not have a dedicated team to do this and there has been no systematic way for documenting these, sharing with other agencies, and providing support to agencies trying to replicate the models. A dedicated ICG team would be ideal for documenting these practices and identifying the elements that made them successful, so that each agency can find the best way to implement. *Federal resources are needed to support a dedicated ICG team to document and share these approaches and provide technical assistance to agencies to implement.*

**Embed analysts in fusion centers:** Local law enforcement agencies have found great value in embedding analysts in fusion centers, even if on a part-time basis. Law enforcement agencies that already operate their local fusion center will have an easier time making this happen. *Local law enforcement agencies should make this a priority.*

**Make technology investment a priority to improve collection and analysis.** Information collection and analysis can no longer be done effectively without strong technology solutions. Not only is there too much information to analyze, but the volume of digital sources to reach is too vast for the usually small number of analysts local law enforcement agencies are able to maintain. Additionally, the increasing loss of law enforcement access to public sources because of multiple aspects of the Going Dark issue (please see the other white paper in this series for more information on how the Going Dark issue is affecting local law enforcement agency access to investigative resources) requires continuing investment in new technologies. It is harder and harder to access the information needed to protect people. *Local law enforcement agencies need to prioritize these investments and have a long-term plan for maintaining the investment, but they would benefit from federal grant language that allows for the use of grant funding to fund certain technologies, like what has been done for body worn cameras. Additionally, federal agencies could develop a program to provide access to a suite of tools across local law enforcement agencies.*

**Foster technology innovation to improve collection and analysis.** Many agencies use field intelligence cards to guide officers and dispatch on intelligence collection needs or how to conduct an interview related to a specific type of incident or circumstance. Because there are so many different field interview cards, each with their own set of questions, it may be hard to remember what questions that need to be asked. Critical situations also make it difficult to take the time to pull out a card and read through each question. As a result, opportunities for collecting valuable information, and being able to identify a high-threat situation are lost, ultimately putting officer safety and public safety at risk. Through the combination of artificial intelligence, voice recognition, and mobile technologies these could be brought to the next level, so that conversations of officers and dispatch would be monitored through their desktop or mobile devices and when

certain lines of discussion are identified alerts would be pushed with questions pushed to a video display or earpiece. This would allow the individual to continue to focus on handling the incident and would help to increase targeted information collection. The artificial intelligence cues could be maintained to stay current with ever-changing collection needs.

Much has also been discussed about the importance of the partnership between operators and analysts. While this can be fostered by collocating these individuals, that connection is still usually diminished when the operator is in the field. Mobile technology has allowed somewhat of a connection to be maintained, but further maintaining this close connection in the field would allow the analyst to better inform the operator relative to each situation. They could push them information to help them focus on the most important aspects of a situation and better inform their lines of questioning. Along this line, mobile technology can also better provide that information at the fingertips of the officers or other operators to help them target their questioning of witnesses or subjects to improve the likelihood of gathering better information. Mobile officer programs can do this when they are enabled with analysis apps that have instant access to all relevant databases and systems (e.g., license plate readers, arrest records, known associates, live surveillance video feeds) and do basic analysis. There is also a continuing need for new technologies that provide signals and electronic intelligence. (Please see the other white paper in this series for more information on what law enforcement agencies are doing to conduct virtual and technical policing operations). These are just a couple of examples of where technology and innovation can help to improve both information collection and analysis. *Local law enforcement agencies can partner with the private sector to encourage innovation that truly meets the needs of law enforcement.*

## Agency-Wide Training

Many of these recommendations are interrelated, but it is important to specifically call out the different parts of an agency that may have unique training needs, existing resources that may be able to be used to address multiple audiences, and more specialized training that may be needed for specific skilled positions.

### Recommendations and Needs

- Provide training to investigators to increase their understanding of intelligence collection and analysis
- Have agency leadership participate in training on intelligence and terrorism
- Increase training opportunities for analysts
- Take advantage of free training for analysts, leadership, and Intelligence Commanders through DHS and FBI
- Continue to make training on source development a priority
- Deliver Terrorism Liaison Officer training to all levels of an agency
- Include officers, dispatch, and other government partners in awareness-level intelligence and counterterrorism training

**Provide training to investigators to increase their understanding of intelligence collection and analysis.** Agencies are increasingly pairing investigators and analysts more closely to improve understanding for each other's roles and foster real-time collaboration. Marrying analysts and investigators also helps to identify intelligence gaps that both can start driving to fulfill together more effectively. While some agencies may be starting this early in their careers, it may not be a practice that can be carried throughout the organization. Agencies can deliver their own training and might integrate it into their TLO training or take advantage of many sources of federal training made available free of cost. *Local law enforcement agencies should make this a priority and federal agencies should continue to provide support for this type of training.*

**Have agency leadership participate in training on intelligence and terrorism.** There is frequent rotation and advancement of agency leadership, including among Intelligence Commanders. The Intelligence Commander position is often one of the positions on the rotation for leadership advancement, so there can be wonderfully capable leaders put in place that have not had much exposure to intelligence, analysis, and counterterrorism. They would benefit from training focused for leadership to ensure they have the perspective needed to supervise the intelligence process. It will also help to emphasize



the importance role and value of intelligence to the decisions law enforcement leaders must make. *Local law enforcement agencies should make this a priority and federal agencies should continue to provide support for this type of training.*

**Increase training opportunities for analysts.** The quality and standardization of law enforcement intelligence analyst training has increased in the last decade. Basic analyst training now ensures analysts have a greater grasp of the complex thought process required to be an effective analyst, while still providing a thorough review of the varied crime and threat environments law enforcement addresses and how they have continued to evolve and become ever-more complex. Since there is no formal certification for analysts and since analysts often come from various backgrounds. Law enforcement agencies need the support of strong training programs to prepare even the most inexperienced and continue to advance their knowledge, perspective, and capabilities.

An agency may also have multiple types of analysts (e.g., strategic and tactical) that require different types of training. Additionally, analysts may also become increasingly more specialized (e.g., social media, cyber crime) and will need more advanced training. While analysts may focus on more specific topic areas, they must still maintain a wide enough breadth of knowledge that they can still recognize connections across crime and terrorism threats. As an example, a crime analyst in a real-time crime center should still have exposure to indicators of foreign terrorist and transnational criminal organization activity, including criminal activities that may be going towards funding terrorist activities (e.g., cigarettes, baby formula, counterfeit items). Regardless of what type of an analyst, they all need to have training on how to be able to take the best advantage of available technologies. *Local law enforcement agencies should make this a priority and federal agencies should continue to provide support for this type of training.*

**Take advantage of free training for analysts, leadership, and Intelligence Commanders through DHS and FBI.** Much of the intelligence and analysis training an agency needs is now accessible free of charge through the FBI and DHS. These are good quality training offerings at both the basic and more advanced levels and can even meet the specific needs of new Intelligence Commanders or other law enforcement leaders (please see page 14 for a list of some of the available training). *Local law enforcement agencies should make this a priority and federal agencies should continue to provide support for this type of training.*

**Continue to make training on source development a priority.** Human sources and informants are still a valuable source of information for local law enforcement agencies and for fulfilling information collection needs. *Local law enforcement agencies need to make sure they continue to make this a priority.*

## Supporting Training for Intelligence Commander Analysis and Operations

Analysis and intelligence analysts are the backbone of Intelligence Commander operations. Many existing training resources can support increasing the capabilities of law enforcement analysts. While not an exhaustive list, the below resources are some of the ones commonly used by law enforcement agencies.

**Federal Bureau of Investigation:** The FBI provides law enforcement agencies an opportunity to participate in some of their analyst training at Quantico and other locations. They also provide more targeted course offerings like the Introduction to Intelligence Theory & Applications for Law Enforcement Supervisors that is delivered periodically to help supervisors and commanders understand the intelligence process for use in managing intelligence led policing.

**Foundations in Intelligence Analysis Training (FIAT):** this five-day training offered by the International Association of Law Enforcement Intelligence Analysts (IALEIA) has become the accepted starting point for many analysts to receive their basic training. IALEIA also offers other training and professional advancement offerings.

**Department of Homeland Security:** the DHS Office of Intelligence and Analysis hosts a Specialized Analytic Seminar Series (SASS) on current topics to advance analytic capabilities.

**Defense Intelligence Agency:** while they do not have a formal program for local law enforcement analysts, some agencies have been able to have their analysts benefit from training made available on a limited basis.

**Domestic Preparedness Consortium:** they are a DHS and FEMA training partner that can be leveraged for basic and advanced capabilities. Their online course catalog can be sorted to find training for law enforcement related to intelligence and analysis.

**Center for Domestic Preparedness:** some of their in-residence training addresses incident management for many of the types of scenarios Intelligence Commanders might be responsible for addressing.

**Deliver Terrorism Liaison Officer training to all levels of an agency.** Agencies that already have a TLO program can use the existing TLO as a resource to provide at least basic awareness-level training throughout an agency. *Local law enforcement agencies can use this existing resource to reach their entire organization.*

**Include officers, dispatch, public safety, and other government partners in awareness-level intelligence and counterterrorism training.** Agencies need as much support in countering terrorism and targeted violence they can get. The best way to ensure other public safety and government partners can recognize concerning activities and know how to take action and report the information is to include them in at least awareness-level intelligence and counterterrorism training. There are some specific benefits for officers and dispatch. Agencies have been doing a good job of making their officers aware of what to look for, but regular updates are important, especially as new priorities, indicators, and collection requirements arise. San Diego has FBI analysts and supervisors teach their class with local law enforcement investigators which helps demonstrate their partnership. Dispatch may still need a better understanding of what rises to the level of being suspicious and needs follow-up. It's better to pass on the information than turn it away. *Local law enforcement agencies need to make sure they continue to make this a priority.*

## Federal Collaboration

Local law enforcement agencies and federal agencies have worked hard to increase collaboration and support for each other's operations and priorities. These partnerships are the only way to make sure both local and federal law enforcement have the information and capabilities they need to prevent attacks. Local agencies could use the federal government's support to help them in their efforts to identify and expand best practices. Local agencies also want to work with federal partners on charting a path forward for continuing to improve existing national efforts and for developing new frameworks for greater information sharing and collaboration.

### Recommendations and Needs

- Need increased support through funding, personnel, training, and technology tools
- Formalize a partnership with DHS, FBI, BJA, and other federal agencies to formalize an Intelligence Commander best practice program
- Pair local and federal analysts - embed FBI analysts in local law enforcement agencies and local law enforcement agency analysts in JTTFs
- Work closely with the FBI to follow-up on cases that do not rise to the level of a JTTF case
- Work closely with DHS to share intelligence and best practice information
- Work closely with CBP to share intelligence and follow-up with identified individuals
- Incorporate terrorism prevention activities into grant funding
- Streamline federal information sharing systems
- Build closer partnership with the Terrorist Screening Center and ensure guidelines are followed
- Reinvigorate National Suspicious Activity Reporting Initiative (NSI)
- Participate in federal task forces

**Need increased federal support through funding, personnel, training, and technology tools.** While local law enforcement increasingly plays a larger role in the prevention of terrorism and targeted violence, in many cases their resources and personnel have been reduced. Local personnel will always be important since they know their communities better than anyone else, putting them in the best position to identify a local threat. While federal analysts embedded in local agencies provide tremendous value, there is no replacement for having personnel with firsthand knowledge of the local environment. Local governments should also make funding of their law enforcement agencies a top priority, but the federal government has an opportunity to provide resources that may not otherwise be attainable. The federal government is already doing a lot to develop and deliver training, but as threats evolve and best practices emerge there are continuing needs for new, updated training and technical assistance to keep agencies at the highest possible level of capability. Technology is another area that is not only hard for local agencies to afford but is hard to maintain the most current capabilities as technology advances. Exploring the possibility of federal agencies providing access to specialized technological tools might be one solution. *Federal resources are needed to increase local capabilities.*



**Formalize a partnership with DHS, FBI, BJA, and other federal agencies to formalize an Intelligence Commander best practice program.** The ICG would like to find the best way to partner with DHS, FBI, BJA, and other federal agencies as part of a national program to identify and spread best practices to other local agencies and increase information sharing between local agencies and with federal partners. Programs like the NYPD Field Intelligence Officer (FIO) program or mental health and crisis response frameworks with law enforcement partnerships are best practices that may just be implemented in a few agencies but could increase the capabilities of all agencies if there was a dedicated program for identifying, documenting, and expanding these programs. *Federal resources are needed to increase local capabilities.*



Ft. Lauderdale Airport  
shooter

#### **Field Examples: FBI Handoff to Local Law Enforcement Agencies**

The recent collection of Florida shootings, including the Fort Lauderdale Airport and the Orlando Pulse nightclub, are examples where shooters had been on the FBI's radar, but there was not enough information for the FBI to continue to pursue. These individuals were not raised as concerns to local authorities, so they could help maintain awareness. Local law enforcement agencies could have helped to monitor the wellness of the individuals and possible indicators of turning violent.

**Pair local and federal analysts - embed FBI and DHS analysts in local law enforcement agencies and local agency analysts in JTTFs.** This addresses one of the most important partnerships for Intelligence Commanders. Inclusion of federal analysts in real time crime centers or fusion centers or local analysts embedded in JTTFs and other local federal offices has been established as a valuable practice that helps to establish and maintain a pipeline of collaboration and information sharing. Federal analysts embedded in local agencies who have access to both federal systems and local law enforcement systems can help to identify connections that might not otherwise be possible. In turn, this also helps the federal agencies to gain better context on threats they may have identified. It is a mutually beneficial arrangement and increases the effectiveness of existing resources. This practice should also apply to specialized capabilities, including airports, harbors, and sporting venues. *Local law enforcement and federal agencies should continue to make this a priority.*

**Work closely with the FBI to follow-up on cases that do not rise to the level of a JTTF case.** There are federal constraints on when or how long an investigation can be conducted. Once they are required to be closed, it does not mean they are not still a threat. There should be a better way to close that gap and capture information on a potential threat that can then be shared with local law enforcement officials for continuing follow-up and monitoring. Local offices of the FBI need to continue to increase information sharing on situations

or individuals that present a concern. Establishing a regular meeting of all local law enforcement intelligence units in the area with the FBI to review the information and make the handoff is one practice being used to make sure no information falls through the cracks. The FBI Threat Squad is a group that is particularly helpful to work with that involves a good level of information sharing and planning for intervention where needed. The FBI is working to get local law enforcement

#### **The eGuardian System**

"The eGuardian system was developed to help meet the challenges of collecting and sharing terrorism-related activities amongst law enforcement agencies across various jurisdictions. The eGuardian system is a sensitive but unclassified (SBU) information-sharing platform hosted by the FBI's Criminal Justice Information Services (CJIS) Division as a service on the Law Enforcement Enterprise Portal (LEEP). The eGuardian system allows law enforcement agencies to combine new suspicious activity reports (SARs) of incidents like these with existing (legacy) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel and analysts directly supporting law enforcement. The information captured in eGuardian is also migrated to the FBI's internal Guardian system, where it is assigned to the appropriate Joint Terrorism Task Force (JTTF) for any further investigative action." (eGuardian website)

agencies involved earlier in an identified area of concern. The eGuardian system is a primary information tool to support this (please see page 16 for an overview of the eGuardian system) but cannot substitute for the in-person information sharing through these more regularly scheduled meetings or through embedded analysts. These interactions will help to ensure the information is input into the eGuardian system. (Please see Figure 2 for a chart depicting how the FBI and local agencies can work together to manage concerning individuals combined with an overlay of partnerships with community services.) *Local law enforcement and federal agencies should continue to make this a priority.*

**Work closely with DHS to share intelligence and best practice information.** In addition to the information sharing with the FBI, DHS is working hard to share more than ever before to try to help keep local agencies abreast of the latest information on a broad set of specialized topics. DHS is also helping to share local products more widely to help local agencies to be able to better identify connections between geographic areas. Additionally, there are efforts to share real-time information between local and federal partners on incident boards. Additional access to DHS information systems, whether direct access or through analysts embedded in local agencies would also be helpful for ongoing access to critical information. *DHS should continue to make this a priority.*

**Work closely with CBP to share intelligence and follow-up with identified individuals.** CBP publishes very accurate threshold targeting reports they will share with local law enforcement agencies on concerning individuals who are flying in or out of an area. Local agencies and local offices of CBP should establish a formal chain for sharing these reports. Local law enforcement agencies are working with CBP to then make a visit with the concerning individual to touch bases two to three weeks after they are identified. There is hope this interaction will make the individual think twice about taking any action. *Local law enforcement and CBP should continue to make this a priority.*

**Incorporate terrorism prevention activities into grant funding.** Need targeted grant funding that includes careful wording to continue to support intelligence operations and prevention activities. Many federal terrorism-related grants are focused on the response to terrorism, rather than the prevention of terrorism. This grant funding should be administered by a federal agency that has responsibility for preventing a terrorist attack. *Federal agencies should continue to make this a priority.*

**Streamline federal information sharing systems.** In this digital age, the public has a sense that law enforcement can enter the name of a suspicious person and find out any related concerns that have

## Great Support from Federal Partners

**Bureau of Justice Assistance (BJA):** their many programs, including grants, training, technical assistance, coordinating bodies, and policy efforts provide great support to local law enforcement.

**Fellowships with NCTC, DHS, and FBI:** local law enforcement agencies have opportunities to send their leaders to formal fellowship programs in these federal agencies to improve mutual understanding and capabilities. They help to create a lasting and productive partnership between the federal government and local law enforcement.

**Training from DHS, FBI, and BJA:** local law enforcement agencies depend on the training and training resources provided by many different federal agencies. The federal government often covers all the costs of training and can either bring the training to an agency or region or send law enforcement personnel to the training. Local law enforcement agencies can continue to inform what new training is needed to meet new threat issues or how existing training can be updated.

**FBI Best Practice Meetings:** these meetings with both local law enforcement agencies and FBI field offices have helped to identify best practices worth spreading and opportunities for new collaboration.

**DHS Best Practice Expansion Programs:** since its inception, DHS has supported the expansion of best practice models to help local agencies integrate new capabilities or improve existing operations.

**FBI Violent Crime Drivers Meetings:** these meetings have helped bring Intelligence Commanders together to identify trends and possible drivers of violent crime. These then identify opportunities to work together to reduce violent crime.

**ATF National Integrated Ballistics Information Network:** this has been a tremendous resource to integrate ballistic information into Intelligence Commander units to quickly inform investigations.

**Embedded Analysts:** the practice of embedding federal analysts in local agencies and local analysts in both local and national offices of federal agencies is extremely valuable for all involved.

**Local Field Offices of Federal Government:** DEA, FBI, DHS, ATF, CBP are just a few of the many agencies that are vital federal partners for the Intelligence Commander operations in local agencies.

been reported throughout the country to other federal, state, or local agencies. There is also the impression that there are automatic systems that are continuously scanning all of these seemingly connected databases of information to identify patterns of concerning activity. We know that just is not the case and that it is hindering the ability to identify concerning individuals and patterns of activity. Analysts from each agency can only access their own systems. At a minimum, all federal information should be in one clearing house that cuts across violent crime and violent extremism concerns. In theory, DHS and FBI databases should be touching each other and should at least notify each other when there are similarities. These streamlined and connected systems with an automated analytical overlay is desperately needed. *Local law enforcement agencies can work with federal agencies to help chart a plan for how this could be most useful for all agencies.*

**Build closer partnership with the Terrorist Screening Center and ensure guidelines are followed.** The Terrorist Screening Center (TSC) is a valuable federal information sharing partner for local law enforcement, including Intelligence Commanders and the ICG. The Terrorist Screening Database (TSDB) maintained by the TSC is one of the most straightforward examples of information sharing between federal and local law enforcement having the potential to make a direct impact against a terrorist plot. The TSC has made a tremendous effort in recent years to improve training and outreach on what local officers and dispatch need to do when they receive a “hit” on the TSDB. Since they are already a valuable partner with the ICG, this provides the basis for continuing the outreach with major city and county Intelligence Commanders and their agencies directly. There is also an opportunity to continue to address in information sharing to ensure individuals on the TSDB do not slip through the cracks. Agencies may not be aware that they request a report of TSC activities that have taken place in their area on a monthly or annual basis. The important role local law enforcement plays with the TSC, the need for officers to report their interactions with individuals on the TSDB, and the TSC procedures to follow can continue to be emphasized through this partnership. *Local law enforcement agencies and TSC can increase collaboration on training and outreach and revisit policies and procedures to identify opportunities for local agencies to play a larger role in safeguarding their communities relative to local hits on the TSDB.*



Private security  
guard threatened  
attack

#### **Field Examples: Importance of Private Sector Partnerships**

A subject on the TSDB was employed as a private security guard at a major entertainment event in Ventura County. Investigators used various techniques (LPR trailers, stationary video surveillance camera, and partnership with local federal investigators) to help prevent an incident from happening.

**Reinvigorate National Suspicious Activity Reporting Initiative (NSI).** The NSI is a tremendous program partnered with the “See Something, Say Something” initiative to increase and document tips and leads from law enforcement and the public. The program could use a fresh push to reinforce the important role local agencies and the public can play in preventing terrorism and targeted violence. They need to know not only what to look for, but they need to feel compelled to take action and know where to report the information. A part of the “See Something, Say Something” messaging can also be more effective if it makes the public more comfortable that if they report their concerns about family and friends early enough, there are support resources that could be brought to help the individual in crisis and that an arrest is not the only possible outcome. Local law enforcement agencies might also consider how they follow up on each tip and lead to see if there is more they can do. *Local law enforcement agencies can work with federal agencies to help chart a plan for reinvigorating the valuable NSI program.*

**Participate in federal task forces.** Law enforcement agencies continue to emphasize the importance of participating in federal task forces to improve a mutual understanding of priorities, threats, and strategies. *Local law enforcement agencies and federal agencies should continue to make this a priority.*

## Partner Collaboration

Law enforcement should look for partners outside of their law enforcement circles to enlist additional means for protecting their communities. This gets at the heart of the need for developing a prevention program. Addressing mental health needs is a very important part of addressing these threats and can be best addressed through a collection of partners to collaborate and provide wrap-around treatment to those in crisis or at risk for using violence. Intervention and stabilization are two different things. Law enforcement's interest is in stopping an attack and while intervention by law enforcement must be applied when a crime has been committed, social services can address the stabilization and support element to help prevent a crime.

### Recommendations and Needs

- Partner with mental health, crisis response, and other social service groups to address people in crisis or at risk for using violence
- Incorporate the use of behavior toolkits to inform assessments of whether a person is at risk for using violence
- Turn partnerships into more formal off-ramp programs

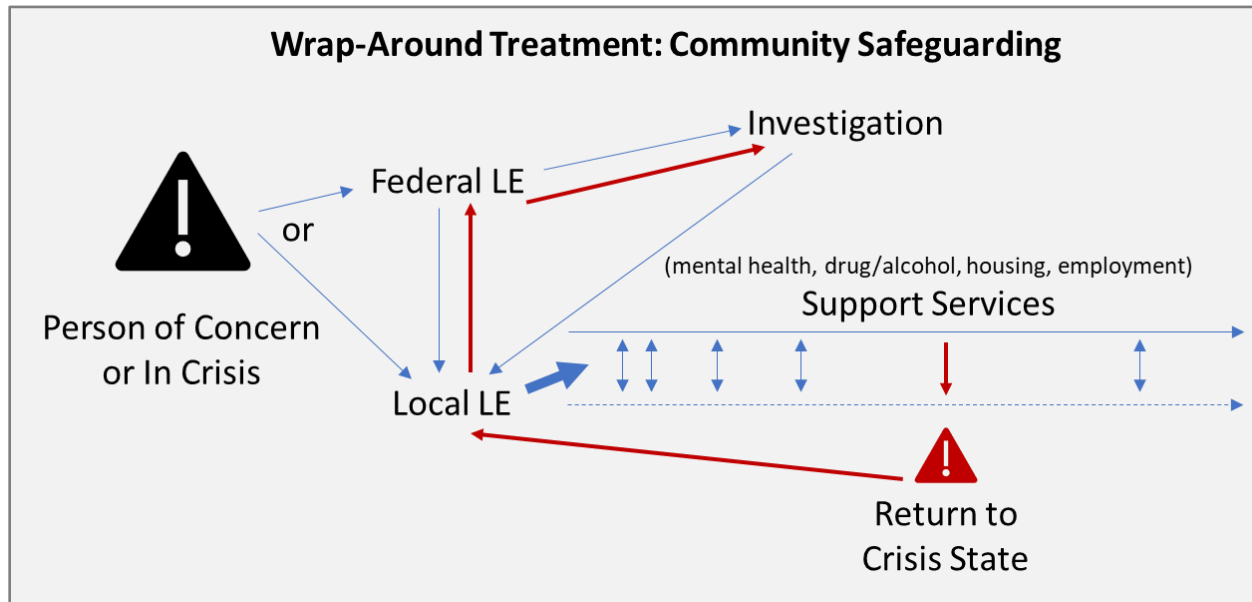
**Partner with mental health, crisis response, and other social service groups to address people in crisis or at risk for using violence.** This will help to provide options for supporting individuals while still maintaining law enforcement awareness of their status. Part of the challenge is that these mental health and other partners have limited resources themselves but working together to develop plans for how to support individuals of concern might help to best use limited resources. Radicalization can happen so quickly, especially for those with mental health issues, so these concerns need to be addressed with focused and persistent action. Since there are similarities between gang and terrorism recruitment, the partner resources used to address gang recruitment might be a good place to start. Many local law enforcement programs are also working to partner mental health clinicians with officers in the field through psychiatric emergency response teams and other programs. They also bring the added benefit of having greater power to apply an involuntary hold on an individual where needed, can ensure any guns are removed, and they are prohibited from purchasing guns. In many agencies, these are existing mental health and crisis response units that are now being applied to preventing terrorism and targeted violence.

Consider this as a wrap-around treatment to safeguard communities. This can apply to all individuals in crisis or for those at risk for using violence, including when the FBI has turned over a case to local law enforcement. If an individual is identified to have a mental health issue, they can be connected with a mental health worker who can advise law enforcement on whether they are at risk for using violence. Also, law enforcement can continue to stay in contact with the mental health support team to know when a person is becoming more of a concern. The mental health partner could continue to make sure the individual continues their mental health appointments or takes their medication. At any point the individual becomes more of a concern a different law enforcement course of action can be taken, including elevating it back up to the level of the FBI and JTTF. *Local law enforcement agencies should make this a priority and federal resources are needed to document best practices and increase local capabilities.*

**Incorporate the use of behavior toolkits to inform assessments of whether a person is at risk for using violence.** There are a variety of behavior evaluation tools law enforcement can use in partnership with clinicians trained in these tools to help determine if someone possesses indicators that might put them at risk of becoming violent or being vulnerable to violent messaging. This helps to ensure assessments are based on behavior indicators and the partnership with the clinicians helps to protect the privacy of individuals. These can help to focus limited resources on those identified to have the highest risk for using violence or the highest level of vulnerability to being recruited to use violence. It is important that only trained individuals apply these tools to ensure they are used most effectively. The Structured Interview for Violence Risk Assessment (SIVAR) tool is one example.<sup>5</sup> *Local law enforcement agencies should partner with federal agencies to identify validated tools and train local personnel to use them in conjunction with mental health partners.*

<sup>5</sup> National Behavioral Intervention Team Association, <https://nabita.org/resources/sivra-35/>

Figure 2: Local Law Enforcement and Partner Approach



Turn partnerships into more formal off-ramp programs. Once partnerships are established they can be turned into more formal off-ramp programs that are most effective if they can be applied before a person turns to violence, which is good community policing for all at-risk communities. We can point them to our social service partners. These programs can leverage existing protocols as the basis of an off-ramp methodology to provide treatment options. These might include involuntary hospitalization, counseling, mentorship, job training, housing, drug and alcohol treatment, and other social services. These then provide the opportunity for law enforcement to maintain some visibility of individuals at risk for using violence. Local off-ramp programs could also partner with the FBI to provide this as an early intervention option to get individuals off the path towards radicalization or violence, rather than wait to see if they act. A mental health and crisis response framework can be applied as a means to improve prevention, maintain law enforcement awareness of those considering violence, and to increase public's comfort with reporting concerns about friends and family. *Local law enforcement agencies should make this a priority and work with the FBI to apply it to their local concerns where possible.*

#### Growing Community Safeguarding and Off-Ramp Programs

Local law enforcement agencies are increasingly taking programs that support individuals with mental health concerns that may have been in place for decades and applying them to individuals that might be going down the path towards violent extremism.

**Los Angeles:** their existing mental health protocol has been in place for over 20 years to address targeted violence (workplace and school violence and threats against the mayor) and is well respected in the community and a welcome resource. Their assessment tool looks at behaviors that might lead to violence, including those related to violent extremism. They have a long-term management unit that is well established and checks in with individuals regularly. There are more off-ramp options available if the person has not committed a crime, but they can also work with them on the back end if a crime has been committed to provide support. They are working to better connect mental health and counterterrorism teams.

**Seattle:** working with mental health professionals, treatment plans for specific individuals are developed that are made available throughout the department and among treatment partners. That way, when anyone comes across this individual, they know what action to take in the field and for continuing support.

**Houston:** the crisis response unit in the Houston Police Department uses its existing and traditional approaches to support individuals with mental health concerns and is working closely with the Houston Regional CVE Steering Committee to apply these practices to those vulnerable to violent extremism in a more coordinated community-wide approach.



## Private Sector Collaboration

Private sector outreach is an extension of other community outreach. Private sector venues are often the target of attacks, so they have the responsibility and opportunity to play a large part in preventing attacks.

### Recommendations and Needs

- Establish a formal private sector outreach program
- Educate, train, and inform private sector partners
- Find opportunities for real-time and critical information sharing with private sector partners
- Embed private security analysts in local law enforcement agency Intelligence Commander operations
- Work with social media outlets to identify violent extremist content for removal

**Establish a formal private sector outreach program.** An outreach program specifically targeted at the private sector and private security increases the eyes and ears of law enforcement to safeguard critical infrastructure and high-profile and high-density locations. The New York Police Department Shield program is an example of this. The NYPD Shield and iWatch programs provide materials for how to get a program started and share all training, documents, and videos so other agencies can use them as is or adapt to their own situation. The NYPD Shield program emphasizes that any agency can get started with their own program with just one person who focuses on getting information sharing started. The Shield program has begun to build out a network of Shield programs across the United States and internationally to improve information sharing in a global threat environment.

San Diego County through their fusion center, the San Diego Law Enforcement Coordination Center (SD-LECC), has an Infrastructure Liaison Officer (ILO) Program that coordinates all outreach, training, and exercises in partnership with the San Diego InfraGard Chapter to private sector partners. Infragard is an FBI program that provides a vehicle for seamless public-private collaboration that supports information sharing and promotes mutual learning for the protection of critical infrastructure. It has thousands of vetted members nationally and is a preexisting program that would benefit other departments who can be more involved with their local fusion centers. *Local law enforcement agencies should make working with the private sector on this a priority.*

**Educate, train, and inform private sector partners.** Existing awareness-level training, like that used for TLO programs, can be adapted to use as training materials for private sector audiences. Recipients of the training can include a variety of private sector partners, including hotels, utility companies, and cable companies, which are those who are invited into homes or hotel rooms regularly. Other types of industries can be included as well to include those who might sell items that could be used to make bombs, like with farm supply stores for fertilizers, pool or beauty supply stores for other chemicals like hydrogen peroxide or chlorine, or places where extremist groups/individuals might go to train (e.g., paintball, airsoft). Training and education materials should show them what to look for, so they can be the eyes and ears for helping to protect their community and become a force multiplier. They might be the one to see pre-attack surveillance. More advanced training can help them understand what to do in an active shooter scenario or what specific indicators might be unique to their sector. *Law enforcement agencies should make working with the private sector on this a priority.*

**Find opportunities for real-time and critical information sharing with private sector partners.** Since private sector venues, whether critical infrastructure or large gathering places, are often the targets of attacks, local law enforcement agencies should look for ways to tailor information sharing products to the private sector. Building relationships with these organizations is a starting point that could serve as the basis for building an information sharing approach. This might include generating an email list of local public sector partners to receive informational bulletins and a real-time information sharing approach. While real-time information sharing could just help to keep businesses informed, it could also provide the information necessary to prevent the next incident or identify an attacker. An example of real-time information sharing from the NYPD Shield program is sending information to banks when there is a bank robbery since there can be strings of robberies that might be prevented. *Local law enforcement agencies should make working with the private sector on this a priority.*

**Embed private security analysts in local law enforcement agency Intelligence Commander operations.** The private sector can have resources to dedicate to this important effort and their well-trained analysts are worth leveraging for analysis support, to gain improved understanding between local law enforcement and the private sector, and to foster real-time information sharing. *Local law enforcement agencies should make working with the private sector on this a priority.*

**Work with social media outlets to identify violent extremist content for removal.** Local law enforcement agencies can reach out to social media companies to develop a partnership that focuses on protecting vulnerable communities from violent extremist messaging. Some social media companies are already doing this and could use additional information identified by local agency analysts to identify and pull down terrorist and violent extremist social media content. Working with the private sector, local law enforcement agencies could identify a standardized and streamlined way of submitting this information to social media companies. *Local law enforcement agencies should make working with the private sector on this a priority.*

**Domestic Security Alliance Council (DSAC) and Overseas Security Advisory Council (OSAC)**

The Domestic Security Alliance Council (DSAC) is a partnership between the United States government and the United States private sector to improve communication and information sharing on security and intelligence issues. The Overseas Security Advisory Council (OSAC) is located in the FBI and was established to “promote security cooperation between American private sector interests worldwide and the U.S. Department of State.” Local law enforcement agencies can reach out to these agencies to develop an information sharing partnership.

**Community Partnerships**

Community outreach is usually not the direct responsibility of an agency’s Intelligence Commander operations, so is not the focus of this document, but the continuing importance of community outreach cannot be overstated. Many local law enforcement agencies have specific units that reach out to ethnic, immigrant, and other specific populations to meet their unique needs. These units also partner closely with other community organizations and often take their lead on outreach.

**Recommendations and Needs**

- Continue local law enforcement agency outreach to all communities
- Support community organizations working on violence prevention and resiliency programs
- Increase public awareness of indicators of terrorism and violence and help them understand the importance of their tips
- Increase public awareness of support resources that can provide an off-ramp alternative
- Reinvigorate “See Something, Say Something” program to increase quality public reporting

**Continue local law enforcement agency outreach to all communities.** While agencies may have specialized units to organize their outreach to more specific communities to better meet their needs, this community policing approach is the basis for all local agency operations. This includes continuing to maintain connections with schools, which might include placement of local law enforcement agency school resource officers. Communities and school staff may be the first to see signs of changes in behavior. *Local law enforcement agencies should continue to make this a priority.*

**Support community organizations working on violence prevention and resiliency programs.** Many community organizations already have a history of trying to prevent violence in their communities and there are new models being used to prevent terrorism recruitment and radicalization. Mothers’ groups like which have been seen in Hennepin County, Minnesota and the United Kingdom to prevent terrorism recruitment is one example of a community effort to harness the will of mothers to protect their children. Supporting these efforts helps communities to be able to counter that narrative themselves rather than solely relying on government. *Local law enforcement agencies should continue to make this a priority.*

**Increase public awareness of indicators of terrorism and violence and help them understand the importance of their tips.** Make training available to community groups to make them aware of signs of terrorism and potential use of violence, how to report the information, and the importance of reporting the information to keep their community safe. Incorporating this awareness information into youth programs may also help to keep vulnerable audiences more empowered to resist these threats. *Local law enforcement agencies should continue to make this a priority.*



#### **Field Examples: Importance of Tips and Leads**

A large majority of incidents involve someone, whether a friend, family member, teacher, neighbor, or someone else knowing that there is concerning activity or behavior before someone has carried out an attack. Whether it is the San Bernardino shooter or one of the recent high school shooters, there are people around them that need to understand the importance of reporting the information to authorities. The Los Angeles Police Department, like many agencies, shared that through their community outreach and terrorism indicators training, community members have reported on several occasions individuals that were exhibiting behaviors that were consistent with terrorism.

**Increase public awareness of support resources that can provide an off-ramp alternative.** Having off-ramp alternatives increases the likelihood that family, friends, and community members will report suspicious activities, knowing there might be a way to support the radicalizing or at-risk individual rather than just arresting them. The support has the goal of stopping an individual before they move any further down the path to radicalization and the use of violence and before they have committed a crime. Knowing these support resources exist might help inspire someone to call in a report earlier than they might have otherwise, which could make it more likely an attack is prevented. *Local law enforcement agencies should continue to make this a priority and continue to work with the federal government to incorporate into national awareness programs.*

**Reinvigorate “See Something, Say Something” program to increase quality public reporting.** A renewed public awareness campaign could increase the likelihood of the public to take action to report information. The messaging could present compelling examples of how the public was able to stop attacks or stop someone from going down the path of violence thanks to available support resources. It should also make people feel a need to report the information. The renewed messaging should also be more action oriented so that rather than just asking them to say something, they are being asked to take action by reporting information to authorities. They could be told exactly where and how to report their information. Additionally, the campaign could make the public more aware of the types of behaviors, actions, and warning signs that should be considered as concerning. This messaging also needs to be distributed through many outlets, to many different audiences, and it needs to be repeated and kept current. *Local law enforcement agencies should continue to make this a priority and continue to work with the federal government to incorporate into national awareness programs.*



**Figure 3: Innovative Programs to Expand**

NYPD Field Intelligence Officer Program	Unit of senior investigators to debrief majority of arrested individuals to identify additional important information <ul style="list-style-type: none"><li>• NYPD Guidebook available to help other agencies establish their own program.</li></ul>
Mental Health/Crisis Response Units	Applying behavior assessment practices to identify violent extremism <ul style="list-style-type: none"><li>• Seattle, Los Angeles (PATHE), Houston</li></ul>
Private Sector Collaboration	Private Sector Outreach/Training <ul style="list-style-type: none"><li>• NYPD Shield Toolkit available to help establish program in any agency, part of national Shield network</li><li>• San Diego County Infrastructure Liaison Officer (ILO) program</li></ul>
iWatch	Community Outreach and Tip Reporting/ Public Sector Outreach <ul style="list-style-type: none"><li>• LAPD iWatch app and materials available to establish program in agency</li><li>• Other programs include Dallas and San Diego Harbor Police</li></ul>

## ACKNOWLEDGEMENTS

The production of this chapter would not have been possible if not for the many partners and participants that contributed throughout the process. In particular, a special thanks to the Bureau of Justice Assistance (BJA), Major Cities Chiefs Association (MCCA), Major County Sheriffs of America (MCSA), the MCCA Homeland Security Committee, and the Intelligence Commanders Group (ICG).

### PREVENTING TERRORISM AND TARGETED VIOLENCE COMMITTEE

Deputy Chief Horace Frank (Committee Chair) Los Angeles Police Department	Inspector Walt Smith (Chair, ICG) Philadelphia Police Dept	Captain Chris Wundrach (Vice Chair, ICG) Oakland County Sheriff's Office
Lieutenant William Wickers Phoenix Police Department	Captain Milton "Wyatt" Martin Houston Police Department	Captain James Boggess Oklahoma City Police Dept
Lieutenant Ryan Hallahan San Diego Police Department	Captain Paul Liquorie Montgomery County Police Dept	Chief Thomas Galati New York Police Department
Commander John Stedman Los Angeles County Sheriff's Dept	Deputy Chief Harold Pretel Cleveland Police Department	Commander Adam Plugge Kern County Sheriff's Dept
Captain Kevin Kelley Kent County Sheriff's Dept	Director David Carabin Boston Police Department	Director Larry Kraus Pasco County Sheriff's Office
Lieutenant Jeff Kendrick Salt Lake City Police Dept	Deputy Chief Shawn Anderson Las Vegas Police Department	Bobby Wyche Los Angeles County Sheriff's Dept
Major David Danzig Pinellas County Sheriff's Office	Captain Michael Ward Montgomery County Police Dept	Sergeant Eric Schlapia Omaha Police Department
Sergeant Chad Baker Orange County Sheriff's Dept	Commander Hank Turner San Diego Sheriff's Department	Lieutenant Kurt Pierce Dane County Sheriff's Office
Major Zachary O'Lare Prince George's County Police Dept	Captain Mark Timpf Tucson Police Department	Lieutenant Dori Koren Las Vegas Police Department
Captain Alejandro Vargas Los Angeles Police Department	Tara Richardson Major Cities Chiefs Association	Chief Mark Stainbrook San Diego Harbor Police

# **Critical Issues for Intelligence Commanders**

**Chapter Three: Maintaining Access to Digital Evidence**

## Chapter Three: Maintaining Access to Digital Evidence

### Executive Summary

With the advent of new encryption methods for communications devices, American law enforcement is rapidly losing the capability to lawfully obtain information necessary to protect the public from crime and violence. Moreover, advocates for enhanced privacy now seek to impose further barriers and restrictions that prevent law enforcement from obtaining historically lawfully accessible information, even when it's needed to stop violent criminals and to save lives. Encryption is just one facet of access to digital evidence and barriers, whether in terms of service provider response, intentional jurisdictional ambiguity, or procedural opaqueness have added to the burden placed on law enforcement leaders, investigators, analysts and Intelligence Commanders. The balance between public safety and privacy has tilted so far out of line that law enforcement leaders are compelled to speak out for crime victims and the public we are sworn to protect.

### Encryption and Privacy

Law enforcement leaders embrace encryption and respect privacy rights. Law enforcement agencies have themselves been the victim of unlawful intrusions, cyber-attacks, and the theft of sensitive data. To protect privacy and unreasonable searches, law enforcement is trained to follow strict procedures and required by law to obtain court orders when obtaining evidence that is protected. These established laws and procedures have served Americans well, and represent the balance between individual rights and protection of the public. New measures designed to safeguard data security and privacy have thrown off the balance and have had an unintended result – they prevent local emergency responders from helping persons in danger and apprehending subjects who pose a threat to the public we serve. Both encryption technologies, proposed privacy measures and company procedures have crossed over the point of balance and go to such extremes that police and sheriffs are prevented from discharging our most fundamental duty – protection of the public.

### Protecting Public Safety

When police and sheriffs have a court approved warrant or there is an immediate threat of grave harm, service providers should respond with urgency, but that is not the reality. The public may not realize that law enforcement routinely faces delays and roadblocks when attempting to obtain information from service providers and cellular device manufacturers – even when that information is needed to save lives and has been directed to be provided through legal demand.

Practices of the United States federal intelligence agencies have provoked controversy among the public, but reactions to those programs should not be extended to state and local law enforcement agencies with differing roles and responsibilities. Mass

### Fully Understanding the Issue: Encryption and Response Challenges

Law enforcement's difficulties with accessing digital evidence comes from both the encryption of data and devices and a lack of response from manufacturers, developers, and providers. Data might be found on a device, app, communication platform, or other digital system. Additional considerations for understanding the access challenges are included below.

**Data in Motion:** this is information moving across networks that may have originated from or end up on a device, communication platform, app, or other means.

**Data at Rest:** data that is stored in any digital form in a device, database, server, cloud service, app, or other location.

**Apps:** many apps have now incorporated end-to-end encryption. Messaging apps with this type of encryption are commonly used by criminals and terrorists and their communications can no longer be accessed.

**Devices:** whether it's an iPhone, hard drive, thumb drive, or other device with digital data, these are often encrypted. Criminals and terrorists use many of these devices for their planning and communications.

**Manufacturers, Developers, and Service Providers:** manufacturers and developers are increasingly incorporating encryption into their devices, apps, and other supporting data services. Service providers include communications and data storage services, like cell phones and cloud storage services. Any of these may not respond to lawful legal demand, intentionally limit relevant content, or may not respond in time to save people from harm. Another complication is that if companies or their data is based internationally they may not be bound by United States court orders.

email intercept operations are not conducted by law enforcement. Emerging encryption capabilities and proposed privacy restrictions are reactions to revelations about practices by national security agencies, but new technologies and proposed privacy measures unintentionally or otherwise, block law enforcement from accessing historically and legally available information necessary to protect the public.

### **The Way Forward**

Privacy and encryption advocates now champion harmful technology that blocks law enforcement from protecting the public. State and local law enforcement officials have joined the FBI find ways for industry to comply with lawful requests to recover data that is essential for protection of the public from harm- the most fundamental duty of government – protection of the public.

Even industry giants must obey the law and comply with lawful legal demand. The public should still be protected, while allowing for innovation and respecting both privacy rights and proprietary technology. Service providers and manufacturers should comply with lawful requests from law enforcement and the courts. The National Domestic Communications Assistance Center (NDCAC) is a tremendously valuable resource, since it is not practical or possible for every one of the thousands state and local law enforcement agencies across the country to have, within their own department, adequate access to resources and expertise; federal assistance is needed to supplement the efforts of their local partners.

Victims and the public need to be protected so defiance of court orders no longer allows criminals, their enterprises and terrorists to operate in the shadows. Moreover, access to digital evidence that exonerates the innocent is just as important as preventing and prosecuting criminals.








### **Chapter Three**

There are much more detailed guides on how to operate, but this chapter is meant to identify the scope of the Intelligence Commander's primary and secondary responsibilities to most effectively use digital evidence to combat crime and terrorism. It also identifies high-priority areas where law enforcement agencies and Intelligence Commander operations need support or where there are opportunities for improvement that have the potential to make a large impact against criminal and terrorist elements and to ultimately protect the community. While the list is long, it only scratches the surface. The critical role the Intelligence Commander plays across the organization for positively impacting crime and terrorism concerns cannot be overlooked.

A committee of Intelligence Commanders from the Intelligence Commanders Group (ICG) convened a series of meetings to establish these priority needs and recommendations through a project that was made possible from a grant from the Department of Justice Bureau of Justice Assistance. This is just one example of the types of partnerships that are needed to operate an effective law enforcement agency.

Please see the table that follows for a list of the recommendations and needs identified for this project. Also, please see two other related white papers that are a part of the Critical Issues for Intelligence Commanders Series:

- Law Enforcement Technical and Virtual Operations
- Preventing Terrorism and Targeted Violence

	Recommendations and Needs	Federal Support Needed
	<b>Increasing Intelligence Commander Collaboration and Information Sharing</b>	
	Establish a “Maintaining Access to Digital Evidence” standing committee within ICG	✓
	Develop a template of agency policies and communications for member agency reference	✓
	Continue to impress upon agencies the importance of this issue and its potential exponential negative impact if not addressed now	✓
	<b>Advancing Agency Capabilities</b>	
	Establish agency policies for steps required to access digital evidence	✓
	Maintain a guidebook of best practices and court document templates	✓
	Create a digital evidence submission form that is required for each device and information source	✓
	<b>Agency-Wide and Partner Training</b>	
	Take advantage of NDCAC free training for law enforcement agencies and investigators	✓
	Support continued training for investigators and digital forensics team	✓
	Update training annually as technology and issues change	✓
	Multiple training modules are needed to address capabilities throughout the agency and for partners (e.g., judicial, baseline, basic handling, executives)	
	<b>Federal Collaboration</b>	
	Support the NDCAC, NW3C, and NCFI programs	✓
	Make all law enforcement agencies aware of the example policies and templates and training and technical assistance available through NDCAC	✓
	Take advantage of all NDCAC services	✓
	Work to establish a more structured partnership between NDCAC and law enforcement agencies through the ICG Maintaining Access to Digital Evidence committee	✓
	Consider becoming a trainer for NDCAC by participating in their train-the-trainer programs	✓
	Continue data collection with FBI to better understand diminished access to digital evidence	✓
	<b>District Attorney Collaboration</b>	
	Create closer relationships between law enforcement technology divisions and District Attorney’s office to professionalize process	
	Continue working closely with the National District Attorneys Association	✓
	Develop an onboarding package for new District Attorneys	✓
	<b>Private Sector Collaboration</b>	
	Develop closer relationships with private sector to improve cooperation against crime and for victims	
	Invite the private sector and media to spend time with law enforcement departments and Intelligence Commanders	
	Find common ground with the private sector on ways to protect communities	
	Embed private security analysts in law enforcement agency Intelligence Commander operations	
	<b>Community Outreach (outside direct Intelligence Commander responsibility)</b>	
	Create partnerships with victim groups to give their stories a voice	✓
	Hold press conferences to share success stories and tragedies	✓
	Increase public awareness of impacts of loss of access to digital evidence to community safety	✓



## National Domestic Communications Assistance Center (NDCAC)

The National Domestic Communications Assistance Center (NDCAC) provides a tremendous collection of services to local law enforcement. Not only is the support free of charge, but in many cases, they will cover all travel costs and attendance at their center for training and other support services. They also will come out to deliver training and services to individual agencies or a regional grouping of agencies depending on the request. NDCAC is a hub for technical knowledge management within the Department of Justice (DOJ) that shares solutions and capabilities with local law enforcement agencies. They also work to strengthen law enforcement relationships with the communications industry. Any local law enforcement agency can request their assistance in a variety of areas. They can even be a continuing resource for ad hoc and immediate expertise and guidance.

You must work for a law enforcement agency (e.g., police officer, investigator, crime analyst) in order to access NDCAC's secure website and take advantage of the numerous resources and tools that it provides. There is no limit to the number of representatives per agency. **To register send a request to: [askndcac@ic.fbi.gov](mailto:askndcac@ic.fbi.gov)**

**Technical Resource Group/ Help Desk:** This is the single point of contact within NDCAC for requesting services and support. It operates 24/7, 365 days a year. The group develops and maintains knowledge of industry-developed and law enforcement technical solutions and best practices. They also identify and address issues related to industry-developed and law enforcement technical solutions and best practices around subpoena and court order compliance. This information is used to provide technical assistance to local law enforcement on lawful intercept and electronic evidence collection methods and best practices. They have also established a secure forum to facilitate communication and collaboration among partnered law enforcement agencies.

**Training:** NDCAC provides a comprehensive curriculum to educate law enforcement on new and emerging services and technologies. They also leverage the training capabilities of local law enforcement agencies through regional sessions or train-the-trainer programs to benefit a larger portion of the community. The curriculum is also used to educate industry and courts on law enforcement methodology and processes. All expenses are covered by NDCAC for local law enforcement to travel to their facilities for training. A sampling of courses includes:

- Best practices for collection/seizure of mobile devices for investigations (3 days)
- Evidence preservation: theory and practical application with a mock crime scene to perform activities (1 day)
- Train-the-trainer course on handling digital evidence
- Overview training: Understanding Investigating Techniques for Modern Telecommunications

**Technology Sharing:** NDCAC is also a resource center for sharing industry-developed and law enforcement technical solutions, technical tools, and applications. They share best practices already in place within the law enforcement community and continuously assess new and updated solutions and modify best practice and guidance to always stay on the forefront. This is bolstered by working with local law enforcement to leverage their research and development efforts. They also identify and share best practices relating to industry-developed and law enforcement lawful intercept and electronic evidence collection equipment, methods, and techniques.

**Industry Relations:** An important component of NDCAC's work is to develop and maintain relationships with industry to ensure law enforcement's understanding of new services and technologies. They provide a venue to exchange information, streamline processes, and facilitate more efficient interaction between law enforcement and industry, including identifying mutual concerns and conveying law enforcement needs. This collaboration is improved by educating industry on law enforcement's evidentiary and other processes and how private industry can facilitate law enforcement's ability to protect communities. There is also technical collaboration to verify law enforcement's understanding of technical solutions and how they work. This program is designed to complement an individual agency's industry outreach and coordination and address issues that rise to a national level.

**Legal Resources:** Law enforcement can access a repository of legal information relative to accessing digital evidence, including templates and guidance on successful practices of law enforcement agencies with court requests.

## Increasing Intelligence Commander Collaboration and Information Sharing

The only way law enforcement agencies will be able to protect our communities and bring justice to victims in this challenging environment is by working together to identify current and emerging successful practices for accessing digital evidence. The Intelligence Commanders Group has a responsibility to play this role between its member agencies since the information Intelligence Commanders require often come from digital and encrypted sources.

### Recommendations and Needs

- Establish a “Maintaining Access to Digital Evidence” standing committee within Intelligence Commanders Group
- Develop a template of agency policies and communications for member agency reference
- Continue to impress upon agencies the importance of this issue and its potential exponential negative impact if not addressed now

### Establish a “Maintaining Access to Digital Evidence” standing committee within Intelligence Commanders Group.

Technology and corporate policies of technology companies and communications providers change so fast that an established venue for regularly scheduled information sharing is needed. This group would not only share their technical practices for accessing digital evidence, but also address successful practices with courts and the private sector for improving response to court filings or other information requests. They can also exchange information on best practices for agency policies, operations, and organization. This group can also call upon outside resources as needed for the latest technology updates or other expertise, guidance, or information. *Local law enforcement agencies should continue to dedicate personnel and resources to participate in this group and federal partners are needed for collaboration.*

**Develop a template of agency policies and communications for member agency reference.** Many agencies already have written policies and templates that work for managing digital evidence or for submitting court requests. These could be compiled into one guide and a supporting repository of existing agency resources could be maintained for ICG member agency reference. This would also be shared with other partners, like NDCAC, that work frequently with law enforcement and compared with their resources to ensure each group has the most effective set of resources. *The ICG should make this a priority and federal partners are needed for collaboration.*

### Field Examples: The Importance of Cell Phone Data in Assisting Human Trafficking Investigation

During a large-scale human trafficking investigation by the Ventura County Sheriff’s Office, numerous cell phones were seized and suspected of containing evidence. Most of the phones were encrypted. Using many techniques, the encryption was defeated and evidence was gained to assist the investigation to stop the exploitation of human trafficking victims. As illustrated in this case, access to digital evidence is key and the burden placed on law enforcement to access evidence is onerous and often untenable for smaller and underfunded agencies.

**Continue to impress upon agencies the importance of this issue and its potential exponential negative impact if not addressed now.** While agencies and agency leadership generally understand the importance of maintaining access to digital evidence, the true impact to the future of law enforcement may not be appreciated throughout an agency. The immediate impact is certainly understood to investigators, officers, Intelligence Commanders, and analysts, but the importance of following protocols and procedures, no matter how arduous and sometimes fruitless, is crucial for ensuring law enforcement maintains its lawful ability to access evidence. What currently may be deceiving, is that law enforcement continues to be able to solve crimes, find missing people, and arrest criminals, because talented law enforcement professionals have found means to overcome criminals who take advantage of these spaces to stay outside the reach of lawful access. Intelligence Commanders can continue to reinforce this message with their agency leadership and spread this important message throughout their agency. Part of this can be accomplished by establishing policies and practices to ensure digital sources of evidence are not abandoned just because private sector practices increasingly create challenges. Law enforcement continues to have the same lawful precedence for access and needs to continue to emphasize this. *Law enforcement agencies and the ICG should make this a priority and support from federal partners is needed.*



## Advancing Agency Capabilities

There continue to be new promising approaches worth integrating into existing operations, opportunities to improve existing efforts, and basic capabilities to spread throughout an agency. Roles, responsibilities, policies, and practices will need to be clearly understood and followed, so that no opportunity to gain digital evidence will be lost. These will need to be continually revisited and any updates will need to be clearly and promptly communicated and understood throughout the agency with the frequent changes in technology.

### Recommendations and Needs

- Establish agency policies for steps required to access digital evidence
- Maintain a guidebook of best practices and court document templates
- Create a digital evidence submission form/checklist that is required for each device and information source
- Clearly outline digital evidence responsibilities within an agency and collaboration practices

**Establish agency policies for steps required to access digital evidence.** Agencies need to establish clear policies on what steps must be followed when digital evidence is a factor in a case, which in this era is becoming more and more prevalent.<sup>6</sup> This is key to improve the likelihood of access and the maintenance of law enforcement's precedence for access. This might include handling instructions to improve the preservation and likelihood of accessing digital evidence, logging of the asset details in a case file or centralized tracking system, submission of court requests to access the information (even if it not likely to be successfully accessed because of encryption technology), the logging of successful and unsuccessful access attempts for statistical tracking, and regular submission of tracking data to NDCAC and inquiries to determine additional possible paths to access. As investigators and officers have come to understand that their attempts to access this information may be time consuming and highly impossible, they may not be going through the traditional steps to gain access. Establishing clear policies will ensure these critical steps are still taken. It will help to then have these policies clearly communicated by agency leadership with an emphasis that these are required steps by everyone in an agency and that following these will be part of each individual's performance assessment. *Law enforcement agencies should make this a priority with the support of the ICG and federal partners.*

**Maintain a guidebook of best practices and court document templates.** The NDCAC maintains a current repository of templates for requesting warrants and other requests of courts and the private sector and the most current and technical details on accessing and handling digital evidence. Agencies should also maintain a clear guidebook of what is adopted by their agency for use, including specific requirements to fulfill for their local courts. *Law enforcement agencies should make this a priority with the support of the NDCAC and federal partners.*

**Create a digital evidence submission form/checklist that is required for each device and information source.** Create a device submission form/checklist (paper or digital) required to be completed and would be rejected without complete information. This will help to ensure that the proper procedures are followed, that an agency can track their success, and that there is a complete understanding of the impact of digital evidence to cases, especially where digital evidence cannot be accessed. *Law enforcement agencies should make this a priority with the support of the ICG and federal partners.*

**Clearly outline digital evidence responsibilities within an agency and collaboration practices.** Since this issue encompasses multiple elements (e.g., devices, applications, carrier/developer requests), agencies should map out which parts of their agency addresses what and consider a streamlined process for establishing processes and communicating everyone's activities on a regular basis to ensure improved coordination and success. It needs to be very clear what each unit does and how they communicate with the other divisions, so everyone has a common understanding of the lines of responsibility and the status of any efforts to access digital evidence, including how urgent needs are addressed. *Law enforcement agencies should make this a priority.*

<sup>6</sup> Technical and Virtual Operations, Critical Issues for Intelligence Commanders Series, Summer 2018

## Agency-Wide and Partner Training

Many of these recommendations are interrelated, but it is important to specifically call out the different parts of an agency that may have unique training needs, existing resources that may be able to be used to address multiple audiences, and more specialized training that may be needed for specific skilled positions or to use with partners. Agencies have been doing a good job of making their officers aware of digital evidence procedures, but regular updates are important, especially as new priorities, practices, and technologies arise. It is better to equip an entire organization to address this challenge to improve outcomes.

### Recommendations and Needs

- Take advantage of NDCAC free training for law enforcement agencies and investigators
- Support continuing training for investigators and digital forensics team
- Update training annually as technology and issues change
- Multiple training modules are needed to address capabilities throughout the agency and for partners (e.g., judicial, baseline, basic handling, executives)

**Take advantage of NDCAC free training for law enforcement agencies and investigators.** One of the vital services provided by NDCAC is training for local law enforcement, including offerings suitable for Intelligence Commanders, analysts, law enforcement leaders, investigators, and others. They can adjust their standard offerings to meet the needs of a specific agency or region. They are also interested in delivering train-the-trainer sessions so the information can be carried more widely to meet the true need for this content in law enforcement agencies. Much of their training is provided at their center in Virginia, but if there is enough demand NDCAC can travel to deliver the training to a large number within an agency or among a group of agencies. Regardless, the training and travel costs are entirely covered by NDCAC for local law enforcement attendees. They maintain the most current knowledge about technology and private sector practices to be able to help law enforcement personnel follow the best practices for accessing digital evidence on devices or through apps or service providers. *Law enforcement agencies should make this a priority and federal agencies should continue to provide support for this type of training.*

### Field Examples: Common Encryption Challenges

The scenarios below demonstrate the common encryption challenges for public safety in a variety of technologies.

**Voice:** Detectives present a signed court order to intercept calls between persons engaged in human trafficking. Trying to find where the victims are to be taken and held, detectives cannot learn anything because voice communications are encrypted on the devices used by the cartel. Even when detectives recover phones during an arrest, the encrypted data cannot be recovered.

**Text Messages:** Domestic terrorists are under surveillance by a local task force and have disclosed to undercover agents that they intend to commit violent crimes. Court authorized intercepts of unencrypted communications confirm that an attack has been planned, but even with a warrant, investigators cannot intercept their encrypted text messages and the attack goes forward.

**Email:** Investigators have a warrant for email from a child pornography suspect – a previously convicted pedophile. When police try to read the email to his next victim, it is encrypted and they cannot respond before he has lured the victim to a planned meeting place.

**Support continued training for investigators and digital forensics team.** Investigators and digital forensics teams that may operate within the Intelligence Commander operations or in partnership with them are often the individuals who conduct the detailed work to access and extract digital evidence. This is the group that needs the detailed training not only on the technology and how to technically access the information, but also the agency practices that must be followed and the best practices for gaining court orders to obtain the information. With the variety of technologies and devices that might be sources of digital evidence and the growing numbers this training will need to be ongoing to maintain the spectrum of capabilities within an agency. Depending on the size of an agency or the proximity of other partner agencies, it might be possible to have individuals develop specialties. However, they should still have a breadth of capabilities so that an agency is not dependent on just one person to be able to carry out the job. NDCAC will be one important source for this training (please see page 10 for additional training resources). *Law enforcement agencies should make this a priority and federal agencies should continue to provide support for this type of training.*

**Update training annually as technology and issues change.** Since technology changes so quickly, the guidance that may have been recently recommended may now cause a device to be rendered completely inaccessible. More formal training can be updated annually, with roll call training to cover any critical changes applicable to officers in the field. *Law enforcement agencies should make this a priority and federal agencies should continue to provide support for this type of training.*

**Multiple training modules are needed to address capabilities throughout the agency and for partners (e.g., judicial, baseline, basic handling, executives).** A variety of training topics are needed to maintain an agency's core capabilities.

- **Judicial:** How to write successful subpoenas, warrants, and other court documents and how to testify on digital evidence and the procedures used to gain access.
- **Baseline Understanding:** This would be the initial training, likely in an academy or continuing education setting, that would provide some basic understanding of the importance of digital evidence and some of the challenges for gaining access. This will make all new agency personnel aware of issues and required agency processes from the beginning.
- **Basic Handling:** This would likely be delivered in partnership with the Baseline Understanding training and would address what to do and not do when seizing or trying to access a device to ensure the best possibility for data recovery. This is likely for officers on the street who may be the first to come in contact with a digital device. The guidance on what to do with a device can change frequently, so roll call training may need to supplement the basic training with current updates and to provide frequent reminders of required practices.

#### **Supporting Training for Accessing Digital Evidence**

Many existing training resources can support increasing the capabilities of law enforcement agencies. While not an exhaustive list, the below resources are some of the ones commonly used by law enforcement agencies.

**National Domestic Communications Assistance Center (NDCAC):** They provide a variety of free training and other technical expertise to local law enforcement agencies. Please see page 9 for a more complete overview of their services.

**National Computer Forensics Institute (NCFI):** is run by the United States Secret Service's Criminal Investigative Division and the Alabama Office of Prosecution Services to provide instruction on digital evidence and cyber-crime investigations and prosecutorial and judicial challenges. The free education is available to state and local law enforcement, legal and judicial professionals.

**Federal Law Enforcement Training Center (FLETC):** offers a variety of courses on a digital evidence from the introductory to the advanced levels.

**National White Collar Crime Center (NW3C):** nonprofit, membership-affiliated organization for law enforcement and prosecutorial and regulatory agencies. They provide training in computer forensics, cyber and financial crime investigations and intelligence analysis.

**National Technical Investigators Association (NATIA):** offers online and in-person training and certification program.

**International Association for Computer Investigative Specialists:** offers in-person training and certification program.

**Private Companies:** some of the companies that help law enforcement access devices and digital evidence also offer training.

- Executive: This would help law enforcement leaders better understand the importance of digital evidence and the issues related to gaining access. It would also cover the types of practices and policies that help an agency to most successful at continuing to be able to gain access.
- Courts: This would help courts understand the importance of digital evidence for law enforcement and would help them understand law enforcement's current challenges. Going through training together and having instructors from both sides would also help to build a closer partnership.

*Local law enforcement agencies should continue to make this a priority, so the entire organization and partners are reached.*

#### **Field Examples: Extreme Costs Prevent Access to Digital Evidence Needed to Solve Crimes**

State and local law enforcement agencies have many devices from cases that are believed to have valuable information to help solve crimes, however they are locked and encrypted. While there are companies and services that may have the ability to unlock some of these devices to access the critical information, the high costs of these services make them cost prohibitive to use. State and local law enforcement agencies are unable to complete the investigation because they cannot afford to pay the high costs every time they need to get into a phone, which is becoming more often.

## Federal Collaboration

Local law enforcement agencies and federal agencies have worked hard to increase collaboration and support for each other's operations and priorities. These partnerships are the only way to make sure both local and federal law enforcement have the information and capabilities they need to address crime and terrorism. State and local agencies could use the federal government's support to help them in their efforts to identify and expand best practices. Local agencies also want to work with federal partners on charting a path forward for continuing to improve existing national efforts and for developing new frameworks for greater collaboration and increasing each other's capabilities.

### Recommendations and Needs

- Support the NDCAC program
- Make all law enforcement agencies aware of the example policies and templates and training and technical assistance available through NDCAC
- Take advantage of all NDCAC services
- Work to establish a more structured partnership between NDCAC and police agencies through the ICG Maintaining Access to Digital Evidence committee
- Consider becoming a trainer for NDCAC by participating in their train-the-trainer programs
- Continue data collection with the FBI to better understand law enforcement diminished access to digital evidence

**Support the NDCAC, NW3C, and NCFI programs.** These programs are a tremendous resource for local law enforcement. Their expertise, training, and other services are one of the main ways that local law enforcement can maintain the capabilities and knowledge needed to continue to gain access to digital evidence. As local law enforcement becomes more aware of their offerings, these groups will need additional resources to continue maintaining the same level of support. Since there are very few other organizations providing this type of information and support to local law enforcement agencies, it is even more critical they receive the support it needs to meet the volume and breadth of needs. *These types of services for state and local law enforcement should continue to be supported.*

**Make all law enforcement agencies aware of the example policies and templates and training and technical assistance available through NDCAC.** Local law enforcement is still becoming aware of NDCAC's offerings. As digital evidence is increasingly a factor in a majority of cases, having the in-house capabilities to access digital evidence is critical and NDCAC can support this need. *The ICG will continue to make this a priority and the federal government should also work to make agencies aware.*

### Field Examples: NDCAC Assistance Helps Solve Homicide

The Oklahoma City Police Department is working with NDCAC on accessing a locked cell phone which should contain evidence to directly connect a homicide suspect to setting up a meeting with the victim at the location of the homicide.

**Take advantage of all NDCAC services.** While law enforcement agencies may have taken advantage of NDCAC's training, they should also make an effort to gain a better understanding of the other services they can provide (please see page 9 for a more complete list of their offerings). NDCAC can be a continuing resource for ad hoc and immediate expertise and guidance. Reach out to NDCAC to gain a better understanding for their complete set of offerings. State and *local law enforcement agencies should make this a priority.*

**Work to establish a more structured partnership between NDCAC and police agencies through the ICG Maintaining Access to Digital Evidence committee.** To create a more direct line of communication between local law enforcement and NDCAC, the ICG and its Maintaining Access to Digital Evidence committee will provide regular updates to the membership on NDCAC offerings and any updates in recommended practices. It will also work to identify opportunities to increase

interactions between NDCAC and local law enforcement. State and local law enforcement and federal agencies should continue to support this as a priority.

**Consider becoming a trainer for NDCAC by participating in their train-the-trainer programs.** As NDCAC's offerings are in greater demand, one of the limiting factors will be having enough trainers to support all of the training requests from law enforcement. Since local law enforcement agencies are developing their own cadre of experts, they may be in the best position to become trainers for NDCAC offerings. Ideal trainers will already have much of the expertise needed and will simply need to participate in one of NDCAC's train-the-trainer sessions before they can start increasing the capabilities of other agencies. *The federal government should provide resources to support this effort and law enforcement agencies should participate.*

**Continue data collection with the FBI to better understand law enforcement diminished access to digital evidence.** Participation is needed from all local law enforcement agencies, which will require each agency to maintain their own repository of information. For an agency to amass this collection of data will likely require establishing policies for how to collect digital evidence and how to document the details. Personnel performance evaluations should also be tied to following these requirements, which will require training to ensure personnel know the detailed information required and where to report it, so it can be entered into a central repository to be compiled with other agencies. This will require a high level of discipline from individuals and agencies. Developing this collection of data is the only way local law enforcement, combined with federal law enforcement agencies, will be able to truly understand the current landscape and provide the background to support any legislative changes. Local agencies should work together with federal agencies to identify what data is of greatest importance to collect to limit the burden on local agencies. *Local police agencies should continue to make this a priority with the support of federal agencies.*

## Non-Technological Barriers to Access

In addition to technological barriers to access such as encryption, law enforcement remains hampered by non-technological barriers to access due to a lack of service provider compliance standards. At a time when the nation expects measures to provide for public safety, these conditions continue to worsen.

**No Federal Compliance Requirements:** There are no mandatory requirement upon carriers to comply with law enforcement requests, even when lives are in danger.

**No Penalties for Failure to Comply:** When providers refuse to obey a lawful request for assistance, including a warrant, there is no federal penalty or remedy.

**No Consistent Procedures or Policies:** The federal government has failed to establish a standard submission system for law enforcement to serve warrants and process on common carriers and Internet service providers.

**No Emergency or Exigent Provisions:** While courts have held that law enforcement need not obtain a search warrant when exigent circumstances demand immediate police actions, advocates would require a warrant in all cases, without regard to emergency conditions.

**No Evidence Procedures:** Lacking any standards or legal requirements, carriers often damage the chain of custody and integrity of evidence.

**No Retention Requirements:** There are no standardized retention schedules for digital information. Critical evidence may not be there when law enforcement needs it most to ensure justice and public safety.

**No Required Technology Standards for Public Safety Access:** There are no technology standards that require viable entry for public safety to access critical information in the event of an emergency and with a court order.



## District Attorney Collaboration

Law enforcement works with District Attorneys on a daily basis to prevent crime and carry out justice and accessing digital evidence is one increasing component of this partnership. With this comes a need for a mutual understanding of the value of digital evidence and the best practices for working together.

### Recommendations and Needs

- Create closer relationships between law enforcement technology divisions and District Attorney's office to professionalize process
- Continue working closely with the National District Attorneys Association
- Develop an onboarding package for new District Attorneys

**Create closer relationships between law enforcement technology divisions and District Attorney's office to professionalize process.** Work to understand each other's needs and how to work together to serve the needs of victims and prevent crime and terrorism. Law enforcement will want to understand in as much detail as possible what information and documentation the District Attorney and court will require to submit requests and issue warrants and subpoenas and build strong cases for prosecution. With this understanding law enforcement can follow through to gather the necessary details to submit formal requests for access to all digital evidence that requires a formal request. As discussed in the Advancing Agency Capabilities section on page 7, agencies may have reduced the number of formal requests they are making for digital evidence because they know there will be technical or other challenges to finally gaining access to the information, even if a court order is issued. When agencies follow through to make these requests with every instance, it makes all partners aware of the volume of need and the prevalence of the issue. This may help to set the stage to develop a process or other strategy for improving outcomes and an ongoing dialog for continuing to make adjustments as technologies and needs evolve. *Local police agencies should make this a priority.*

**Continue working closely with the National District Attorneys Association.** The National District Attorneys Association has been a close partner with the ICG, MCCA, and MCSA in the Encryption Coalition, which is a group of federal agencies, local agencies, and associations working together to ensure continuing access to digital evidence to protect communities, serve the needs of victims, and prevent crime and terrorism. This is a valuable partnership to ensure continuing access to digital evidence and to continue to identify where national legislative changes are needed. *The ICG, MCCA, MCSA, law enforcement agencies, and federal partners should continue to make this a priority.*

**Develop an onboarding package for new District Attorneys.** Local law enforcement agencies reported that it is often the new attorneys in the District Attorney offices who are assigned to handle the warrants for access to devices, applications, and communications. Since these new attorneys may not be as knowledgeable on the issue or the specific details of the process, it would help to create an onboarding package to help them in their new role. *Federal partners can help to make resources available to the ICG to establish a template that can be customized by each member agency.*

### Field Examples: Encrypted Communications App Prevent Prosecution of Mexican Mafia

During a wire-tap investigation into the Mexican Mafia by the Ventura County Sheriff's Office, an attempt was made to intercept communications from a Mexican Mafia member who was using a cellular telephone while in custody in state prison. The Mexican Mafia member was using a cellular phone application called WhatsApp to communicate with other Mexican Mafia members and associates in and out of custody. Due to the WhatsApp design, it is not possible to intercept communications, so the Sheriff's office was unable to prosecute the Mexican Mafia member.

### Is Technology Above the Law?

When lives are in danger and violent offenders seek to prey upon the public, industry should not be permitted to ignore court orders – no entity is above the law and no business model purposefully crafted to thwart criminal investigations should be lauded. It is corporate practice among some technology companies to defy court orders, even when public safety is at risk because it might “tarnish”<sup>7</sup> their corporate brand.

- **Public Safety Emergencies:** encryption prevents police and rescue personnel from finding a missing person, a lost hiker, an Alzheimer’s patient, or a heart attack victim.
- **Criminal Investigations:** encryption blocks law enforcement from finding an abducted child, apprehending a murderer, stopping a drug trafficker, or locating victims of human trafficking.
- **Service Provider Response:** service providers routinely withhold valuable content from law enforcement. The lack of transparency on how their systems are configured to allow for tailored court orders leaves law enforcement having to guess the magic word, even in emergency situations.

Corporations are taking additional steps to make it harder for law enforcement to access critical information. One example is the recent Apple software update that will disable the phone’s charging and data port an hour after the phone is locked. This disables one of the means law enforcement can use to access important data after recovering a device of a criminal or victim.<sup>8</sup>

While corporations are on the one hand indicating they are working to protect privacy, they continue to gather and sell private information. The selling of location information<sup>9</sup> and tracking movement<sup>10</sup> and other activities are just a few examples of technology companies using the information we are forced to provide to them through exhaustive user agreements people are required to accept.

#### Field Examples: When Time Is of the Essence, Lives are at Risk When the Private Sector Does Not Assist

In December 2017, an exigent case involved a missing 13-year-old Texas girl who was recovered in Mexico with FBI assistance, despite Google refusing to release the contents of an email address citing there was no evidence there. The girl allegedly went to Mexico to meet up with a man with whom she had been corresponding with a for a year. Authorities confirmed the presence of evidence in the Google account once a search warrant was completed and responsive data was received which was after the girl had been rescued. Missing persons cases are especially time sensitive and when the private sector does not assist they put lives at risk.

11

<sup>7</sup> Court Filing on behalf of Apple; Ken Dreifach: <https://www.documentcloud.org/documents/2465705-apple-brief-10192015.html>

<sup>8</sup> Nicas, Jack, New York Times, June 13, 2018, “Apple to Close iPhone Security Hole That Law Enforcement Uses to Crack Devices”

<sup>9</sup> Website Flaw Exposes Real-Time Locations of US Cellphones, Associated Press, May 18, 2018

<sup>10</sup> 'It Knows When I Got Out of the Car!': Tucker's Special Report on How Google's Tracking You, Tucker Carlson Tonight, Fox News, February 7, 2018

<sup>11</sup> Young Texas Teen Found Safe in Mexico, CBS News, December 4, 2017



## Private Sector Collaboration

The private sector has been a critical partner in responding to in-progress crimes which has led to people being saved and protected from further harm. They also have been a critical partner in bringing justice to victims and preventing crime and terrorism. This is the same type of partnership law enforcement is looking to build on with technology companies. While there may be areas where many private sector organizations have made a commitment to help law enforcement to have lawful access to digital evidence, there is a small segment of technology and communications companies that defy court orders and do not respond in a timely way when there are urgent needs.

### Recommendations and Needs

- Develop closer relationships with the private sector to improve cooperation against crime and support for victims
- Invite the private sector and media to spend time with law enforcement departments and Intelligence Commanders
- Find common ground with the private sector on ways to protect communities
- Embed private security analysts in law enforcement agency Intelligence Commander operations

**Develop closer relationships with the private sector to improve cooperation against crime and support for victims.** Work to develop closer relationships with manufacturers, developers, and providers to establish open communication lines to improve cooperation against crime and support for victims. Private sector information sharing and awareness programs that have been established in some agencies may primarily be established to help prevent terrorism, but these also help to develop closer relationships with the private sector and the communications and technology industries can be added as a specific segment. Some members of the private sector have gone so far as to embed their own analysts in police agency analysis operations. *Law enforcement agencies should make working with the private sector on this a priority.*

**Invite the private sector to spend time with law enforcement departments and Intelligence Commanders.** Citizen academies or similar programs that invite the media to participate in law enforcement training with simulations of real-world incidents and are exposed to other aspects of law enforcement operations could be used or adapted for a private sector audience. Content that demonstrates the need to access digital evidence and the challenges in gaining access could also be added. This would show the perspective of law enforcement and how they use digital evidence to protect the community, which can include exonerating people suspected of crimes. *Law enforcement agencies should make working with the private sector on this a priority.*

**Find common ground with the private sector on ways to protect communities.** The private sector is already a valued partner with law enforcement. Law enforcement, the private sector, and communities all want the same thing – they want safe communities. That is common ground from which all can come together to find the best ways to maintain access to digital evidence to protect communities while still protecting privacy and individual rights. *Law enforcement agencies should make working with the private sector on this a priority.*

**Embed private security analysts in law enforcement agency Intelligence Commander operations.** There are many reasons this makes sense, especially to collaborate against crime and terrorism, but it also helps to increase understanding between law enforcement and the private sector on digital evidence issues. *Law enforcement agencies should make working with the private sector on this a priority.*

### Hampering Criminal Defense

The discovery process in criminal cases requires all exculpatory evidence to be released by law enforcement and prosecutors. With encryption, neither investigators nor the accused will be able to see or read what may exonerate the defendant.

- If manufacturers do not have keys to decrypt data, defendants will be unable to use communications content in their defense.
- If text messages are not retained by service providers, defendants cannot subpoena the content for their own defense.

## Community Partnerships

Community outreach is usually not the direct responsibility of an agency's Intelligence Commander operations, so is not the focus of this document, but the continuing importance of community outreach cannot be overstated. The public does not realize how often police turn to digital technology to locate both victims and criminals. Whether to find a lost camper or a kidnap victim, police rely upon carriers to provide location data. When police have lawful access to digital cell phones and other sources, information will lead rescuers to persons in danger and to the criminals who would do them harm.

### Recommendations and Needs

- Create partnerships with victim groups to give their stories a voice
- Hold press conferences to share success stories and tragedies
- Increase public awareness of potential impacts of loss of access to digital evidence to community safety

**Create partnerships with victim groups to give their stories a voice.** During every hour of every day, law enforcement uses digital evidence, whether encrypted or not, to save lives, protect their communities, and solve crimes to bring justice to victims.

Victims groups know the tragedy and pain of terrible crimes all too well, but they also know the relief that comes from solving the crime that hurt them or their loved ones and serving justice on the offender and the satisfaction that comes bringing light to an issue where they prevent someone else from becoming a victim. Work with local and national groups to incorporate them in outreach and media events to give them an opportunity to share their stories and where digital information did or could have made a difference. *Law enforcement agencies should continue to make this a priority with federal and other partners.*

**Hold press conferences to share success stories and tragedies.** One way to effectively convey to communities the challenges for accessing digital evidence and the need for ensuring private sector cooperation and legislative protections is for Police Chiefs, Sheriffs, and agency leadership to share information at press conferences. These press conferences could be set up specifically to share success stories where quick access to digital evidence meant the difference between life and death or where justice was served for a victim. These could also bring to light the tragedies that result from access to digital evidence being blocked or not provided quickly when time matters. Additionally, this continuing challenge could be mentioned as a part of all press and outreach efforts. *Law enforcement agencies should continue to make this a priority with federal and other partners.*

**Increase public awareness of potential impacts of loss of access to digital evidence to community safety.** The long-term impacts of continuing to lose access are dire. While law enforcement may be working harder to be able to find needed information, they are left without the full picture and they are losing more and more of that picture without legislative protections. Law enforcement needs to find better ways to educate the public on these issues and the impact to their safety. Not only will criminals go without being identified or prosecuted, but in-progress events where children have been kidnapped, a person is lost, or where someone's life or well-being is known to be in imminent danger will go without there being a way to access the digital information that could make the difference between life and death. *Police agencies should continue to make this a priority with federal and other partners.*

### Justice for Victims

Losing access to digital evidence means that crime victims will be further harmed. Digital data represents the evidence of crimes - to which victims have a right.

**Victims of Human/Sex Trafficking:** where photographs and communications content are required, victims will be unable to get justice when key evidence is beyond the reach of the court.

**Victims of Child Predators:** and other criminals who document their horrific crimes will be able to use encryption to their advantage. Without lawful access for law enforcement, key evidence will be hidden.

**Murder and Kidnapping Victims:** The current voluntary response posture allowed for service providers permits destruction of evidence while law enforcement waits for release of the data.

Many other types of victims are at risk for not having justice served.

**Field Examples: Sources for Help for Law Enforcement Agencies**

Law enforcement agencies are finding support for accessing digital evidence from a variety of sources outside their own operations:

- Department of Homeland Security and Customs and Border Patrol: the Tucson Police Department has an excellent collaboration with other agencies to help gain access to digital evidence, especially the Department of Homeland Security and the Border Patrol because of their proximity to the southern border.
- Intermountain West Regional Computer Forensic Lab: this is a lab affiliated with the FBI that is used by the Salt Lake City Police Department and other agencies.
- San Diego FBI Regional Computer Forensics Laboratory: the San Diego Police Department uses this resource.
- Southern California High Technology Crime Task Force: the Ventura County Sheriff's Office uses this resource when they have technical difficulties they cannot easily handle in-house.
- United States Secret Service: many agencies are using their full set of support resources.
- National Domestic Communications Assistance Center (NDCAC): many agencies are using their full set of support services.

## ACKNOWLEDGEMENTS

The production of this chapter would not have been possible if not for the many partners and participants that contributed throughout the process. In particular, a special thanks to the Bureau of Justice Assistance (BJA), Major Cities Chiefs Association (MCCA), Major County Sheriffs of America (MCSA), the MCCA Homeland Security Committee, and the Intelligence Commanders Group (ICG).

### MAINTAINING ACCESS TO DIGITAL EVIDENCE COMMITTEE

First Dep. Commissioner Kevin Smith  
(Committee Chair)  
Nassau County Police Department

Inspector Walt Smith  
(Chair, ICG)  
Philadelphia Police Dept

Captain Chris Wundrach  
(Vice Chair, ICG)  
Oakland County Sheriff's Office

Detective Lieutenant Devin Ross  
Nassau County Police Department

Captain Milton "Wyatt" Martin  
Houston Police Department

Captain James Boggess  
Oklahoma City Police Dept

Captain Scott Canter  
Baltimore County Police Dept

Major David Danzig  
Pinellas County Sheriff's Office

Commander Harold Turner  
San Diego Sheriff's Department

Captain Mark Timpf  
Tucson Police Department

Director David Carabin  
Boston Police Department

Lieutenant Ryan Hallahan  
San Diego Police Department

Sergeant Eric Schlapia  
Omaha Police Department

Lieutenant Dori Koren  
Las Vegas Police Department

Lieutenant Jeff Kendrick  
Salt Lake City Police Dept

Tara Richardson  
Major Cities Chiefs Association

Laura Cooper  
Major County Sheriffs of America