IACP Deliverables

Be sure to work with your IACP Member Engagement Team staff liaison to move these products through the appropriate review and approval process prior to publishing.

Police Chief Magazine

Police Chief magazine is the official publication of the IACP. Articles can be considered for publication in the online or print versions of the magazine. There are also several columns accepting submissions, including:

- Research in Brief
- Technology Talk
- Traffic Safety
- The Informer
- Spotlight
- The Brief
- Officer Wellness
- Chief's Counsel

IN THE FIELD Traffic Safety Initiatives

Automated Vehicles and State Law Enforcement Summit

BY Mark Savage, Deputy Chief, Colorado State Patrol, and Gina Espinosa-Salcedo, Region 8 Administrator, National Highway Traffic Safety Administration

AUTOMATED VEHICLE TECHNOLOGIES ARE INCREASINGLY MORE PREVALENT ON THE ROADWAYS. FROM AUTOMATIC EMERGENCY BRAKING AND AUTOMATIC PARALLEL PARKING TO FULLY AUTONOMOUS TECHNOLOGIES THAT ALLOW A VEHICLE TO OPERATE WITHOUT A HUMAN BEHIND THE WHEEL, AUTOMATED TECHNOLOGY IS INCREASINGLY GUIDING TRANSPORTATION SYSTEMS.

Whether it be driver-assist technology or fully autonomous vehicles, these technologies will forever alter the relationship between driver and vehicle. Eventually, these technologies could eliminate the need for humans to drive at all. While these features promise to save lives and reduce injuries, numerous public safety issues and considerations remain. Law enforcement agencies are increasingly tasked with ensuring that the convenience of automation does not come at the cost of safety. Accordingly, there must be recognition by policy makers at all levels that law enforcement has a significant role and needs to be included in the discussions surrounding automated vehicles.

The growing ubiquity of automated vehicles has generated new responsibilities for law enforcement. Task forces or study groups have been created to manage the implications of automated vehicles, with state and local law enforcement occasionally having a seat at the table.

In some states, state law enforcement actually oversees the testing of highly automated vehicles on public roads. In some of these cases, agencies have had to swiftly evolve to confront the challenges of automated vehicles with few resources or peer relationships to help guide them. To help those already engaged with these issues and to start the conversation on how to best address the coming changes, the Colorado State Patrol (CSP) hosted a two-day summit in September 2019 on Automated Vehicles and Law Enforcement. As one of the first state law enforcement agencies involved with these activities, the CSP was interested in convening a summit for law enforcement agency executives to share information, experiences, ideas, and lessons learned.

The agenda was designed to be beneficial for both newcomers and experienced users alike, including an overview of automated vehicle technology, lessons learned from states where automated vehicles were already in testing or use, and an opportunity to hear from manufacturers.

The regional office of the National Highway Traffic Safety Administration (NHTSA) worked in support of the CSP to host the summit. NHTSA Region 8 and CSP collaborated in the planning, logistics, and execution of the meeting.

States represented by attendees at the Automated Vehicles and Law Enforcement Summit:

- California
- Colorado
- Idaho
- Kansas
- Maryland
- Mississippi
- Missouri
- Montana
- Nebraska
- New Mexico
- New York
- North Dakota
- Ohio
- South Dakota
- Texas
- Utah
- Washington
- Wyoming

Colorado State Patrol Chief Matt Packard provides welcoming remarks.

20 POLICE CHIEF ★ JUNE 2020

policechiefmagazine.org

TECHNOLOGY Tech Talk

A Quick Guide on Mobile Drone Detection

Things to Consider When Evaluating Technologies

Center for The Study of The Drone at Bard College, in March 2020, 1,103 law enforcement agencies were using drones in some capacity. This is 70 percent of the total use by law enforcement, fire and rescue, and emergency management combined.

Drones have practical uses within many industries, not just law enforcement. Most notably, drones are used for videography, real estate, infrastructure inspections, and crop and field management. It is important to differentiate between beneficial, clueless or careless, and criminal drone use.

It's no secret that any commercial drone pilot in the United States is required to follow federal and state regulations, and law enforcement agencies must stay abreast of any changes in drone laws or regulations. The hobbyist pilots who are still clueless or careless are the ones to worry about. Just to name a few of many examples, hobbyists have unintentionally disrupted first responder

policechiefmagazine.org

"The short duration of the attacks highlights the importance of preventing these tragedies before they occur."

took place with greater frequency in the weeks following the summer and winter breaks. In addition, 17 incidents occurred within the attacker's first week back to school following other breaks in attendance, such as absences due to truancy, illness, or suspension. Several attacks took place on the first day after a scheduled school holiday, including three that occurred on the first day of school following the summer, fall, and winter holidays.

CASE EXAMPLE

A 15-year-old student shot and wounded a peer in the cafeteria on the first day of school. He had spent the last week of his summer break planning the attack. Four hours before the shooting, he shared a message on social media: "First day of school, last day of my life."

Nearly half of the attacks were over within one minute. As seen in targeted school attacks and other acts of targeted violence, many victims may be harmed or killed before law enforcement even has the opportunity to respond. The short duration of the attacks highlights the importance of preventing these tragedies before they occur.

FIGURE 1. DURATION OF ATTACKS

Percentages do not total 100 due to rounding.

OVERVIEW OF U.S. SCHOOL ATTACKS FROM 2008 TO 2017

The 41 school attacks analyzed in the NTAC study included at least one attack in every year of the study period, showing no pattern of increasing or decreasing in the years from 2008 to 2017. Attacks happened in every month except July and every day of the week but Sunday. The majority of the incidents took place in the morning, with one-quarter occurring before school and half taking place during morning class hours. A third of the attacks were carried out outside of classroom hours, indicating that schools and law enforcement should prepare for the possibility of violence before and after school, during lunch, and at other times when students are not in class. For example, 1 of the 41 attacks occurred during a Saturday prom.

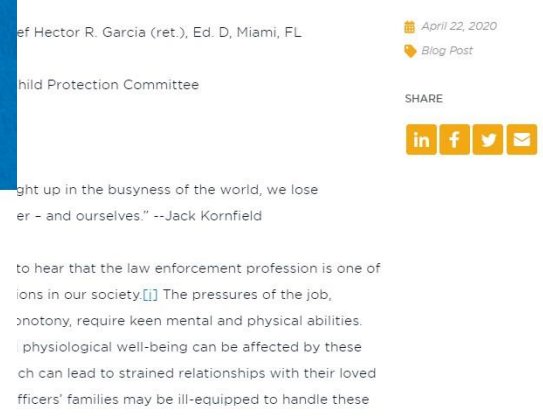
Many attacks occurred soon after the attacker returned from a break in attendance. For example, attacks

JUNE 2020 ★ POLICE CHIEF 35

IACP International Association of Chiefs of Police

IACP Blog

www.theIACP.org/blog

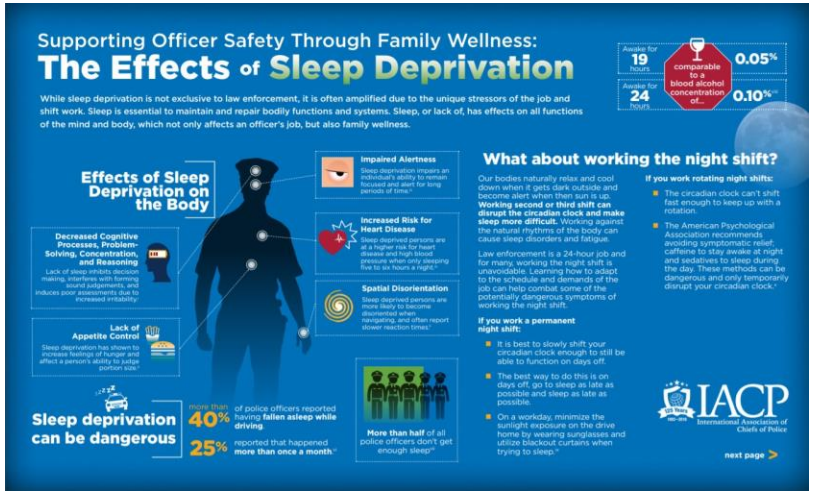


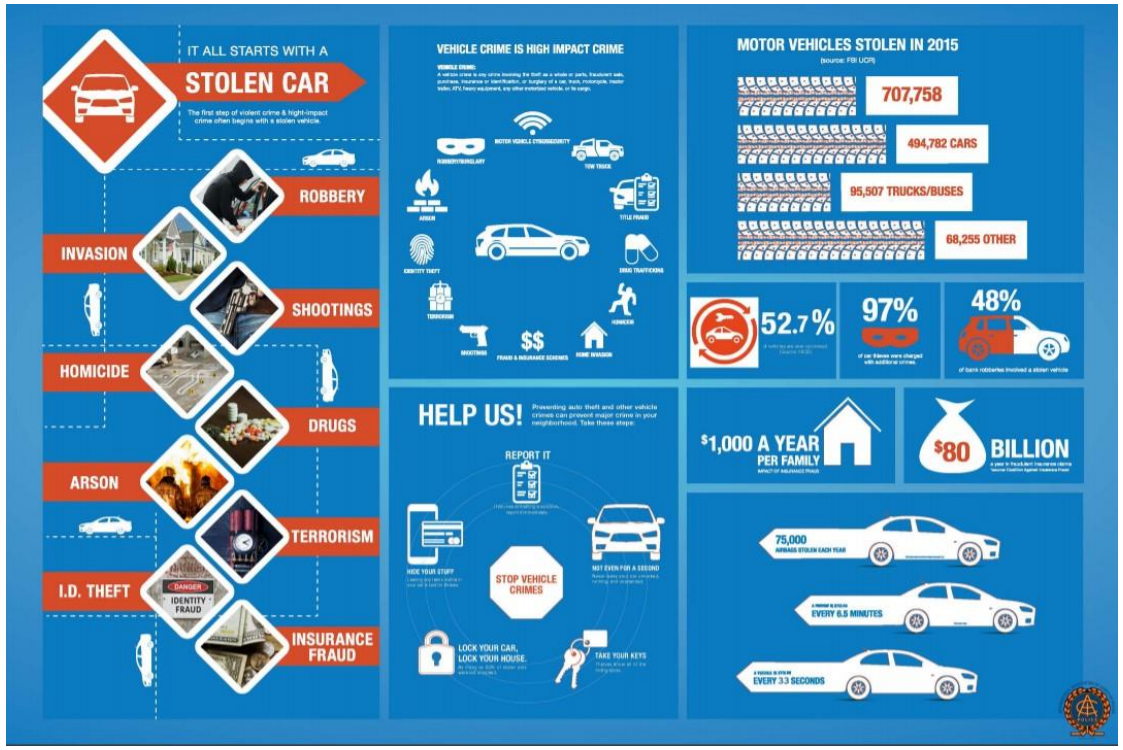
IACP
International Association of Chiefs of Police

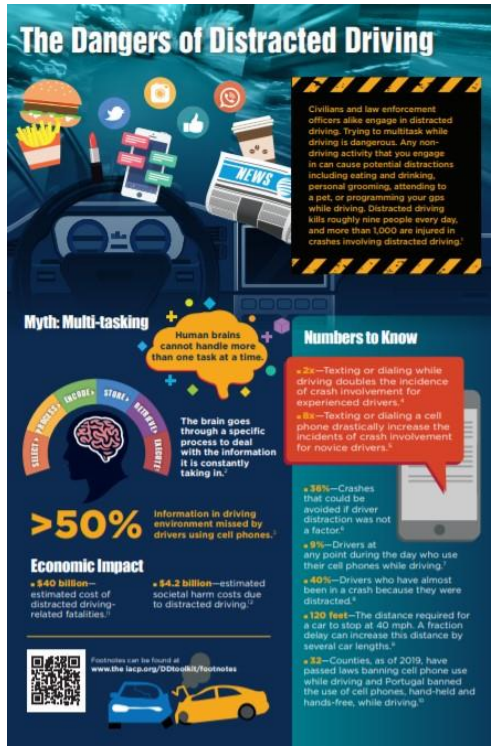
Infographic

An infographic is a collection of imagery, charts, and minimal text that gives an easy-to-understand overview of a topic. These can include posters, placards, postcards, etc. and can be printed or posted on the IACP website.

IACP
International Association of Chiefs of Police







Brochure

A brochure is an informative printed document, which can be folded into a booklet, pamphlet, or leaflet.

Going Dark

In addition to the challenges posed by the sheer volume of digital evidence, the issue of "going dark"—law enforcement's decreasing ability to lawfully access and examine digital evidence at rest and evidence in motion due to technical and nontechnical barriers—is increasingly placing public safety at risk.

Law enforcement often lacks the technical ability to access communications and information pursuant to a lawful court order. This inability to access digital communications data not only inhibits access to evidence in federal criminal and terrorism cases, but also keeps state and local law enforcement from being able to do their job effectively.

Unfortunately, current laws which were designed for non-digital communications and the development of new technologies, such as encryption products, which do not allow for third party access put public safety at risk.

Education and Outreach

To assist in addressing these concerns, law enforcement executives need to take the lead in ensuring that the public, private sector companies, and elected officials understand the impact and threat, that digital evidence access and going dark poses to communities. Below are some key points that should be stressed when discussing this issue with the public or elected officials.

- Digital evidence is a critical component in virtually all of today's criminal investigations.
- To safeguard communities, law enforcement needs access to appropriate legal authorities, tools, and training that are necessary to lawfully obtain and use digital evidence.
- Barriers to lawful access, whether technological or non-technological, should be minimized and factored into the development process by service providers and equipment manufacturers.
- Encryption without lawful access to encrypted content is a growing problem for law enforcement. This lack of access means cases are going unsolved, and the public is less safe.
- Policymakers should explore opportunities to enable increased lawful access to digital evidence. A lack of legal authorities regulating the retention and production of digital evidence by technology companies is driving negative public safety outcomes.
- Policymakers need to enact laws that require industry to ensure lawful access to digital evidence when a lawful court order is authorized and needed.
- Policymakers need to encourage industry leaders to identify approaches that protect privacy while still allowing lawful access to stored data and electronic communications that will help law enforcement conduct investigations and apprehend criminals and terrorists.
- Heightened legal requirements and other restrictions on law enforcement access to digital evidence impact law enforcement effectiveness, and therefore should be imposed with careful consideration of the consequences to ensure that law enforcement's ability to protect the public is not unduly impaired.

This document is a product of the IACP Digital Evidence Task Force:

Sandra Spagnoli
Chair, IACP Investigations Policy Council

John Lattimer
Chair, IACP Technology Policy Council

David Roesch
Co-Chair, IACP Forensics Committee

John Grassel
Co-Chair, IACP Forensics Committee

James Emerson
Chair, IACP Computer Crimes and Digital Evidence Committee

Thomas Ruocco
Chair, IACP Police Investigative Operations Committee

For More Information, Please Visit
www.theIACP.org/resources/law-enforcement-cyber-center

International Association of Chiefs of Police
44 Canal Center Plaza, Suite 200
Alexandria, VA 22314
703.836.6767 • fax 703.836.4743
www.theIACP.org

DIGITAL EVIDENCE TASK FORCE

EXECUTIVE PRIMER

IACP

Overview

The expansion of communications technology means that crime scenes are often digital rather than physical, which poses a growing challenge to investigators. In addition, physical crime scenes—the ones that state and local law enforcement respond to every day—are much more complex than ever before. Crime scenes from homicides, kidnappings, assaults, property crimes and incidents of domestic violence — crimes that impact thousands of victims, families, and communities annually—now, more often than not, include digital evidence.

Properly obtained and analyzed, digital evidence results in more actionable and successful investigations and prosecutions. At the same time, the complexity and sheer volume of digital evidence has greatly impacted law enforcement operations and investigations.

To succeed in this new environment, law enforcement executives need to understand the complexities of digital evidence, consider what policy changes they may need to adopt, and how they can work with both their communities and policy makers to ensure they fully understand the challenge this issue poses for law enforcement.

To assist law enforcement leaders in addressing this issue the International Association of Chiefs of Police (IACP) established the Digital Evidence Task Force (DETF). The DETF draws on the expertise of the IACP Computer Crimes and Digital Evidence Committee, Forensic Science Committee, and Police Investigative Operations Committee.

Scope of the Problem

Law enforcement encounters digital evidence in numerous ways, including, but not limited to:

- Video and audio files
- Social media posts and aggregated products
- Email and other business communications
- Evidence on computers, mobile devices, and wearables
- Ecommerce and other online financial data
- Sensor data such as license plate readers (LPR), facial recognition, and gunshot detection technology
- Website access logs
- Geolocation information
- Subscriber records for online service providers
- Data from motor vehicle computing systems
- Data from the Internet advertising ecosystem

In addition, the collection, analysis, utilization, and preservation of digital evidence must be managed under the same standards as other types of evidence. As a result, law enforcement must adapt to manage the appropriate handling and use of digital evidence available from a multitude of resources.

Challenges to Law Enforcement

Police executives should be aware of three main ways that law enforcement's access to digital crime scenes can be restricted.

- *Lack of capacity.* This includes issues such as lack of specialized training, specialized equipment, and other investigative resources within the law enforcement agency.
- *Technical barriers to access.* These barriers include unregulated encryption and communications technologies developed outside of a legal framework that allow for lawful access to data and communications.
- *Non-technical barriers.* This includes the imposition of customer notification requirements and legal barriers that arguably heighten the proof required to access evidence.

IACP's Law Enforcement Cyber Center

To assist law enforcement executives in meeting these challenges, the IACP, in cooperation with the Bureau of Justice Assistance and other law enforcement organizations, developed the IACP Law Enforcement Cyber Center (LECC) to serve as a central clearinghouse for detailed resources managed by government, professional organizations, and subject-matter experts. The purpose of this site is to provide executives, senior leadership, and staff access to information, policy and other critical resources related to computer crime, cyber issues, and digital evidence.

1 http://www.iacpcybercenter.org/

Policy Considerations

Law enforcement agencies should consider implementing new or reviewing their existing policy, oversight, and operational controls to ensure that they are positioned to successfully meet the challenges posed by digital evidence. A few key steps are outlined below, in addition, the Law Enforcement Cyber Center provides links to resources which elaborate on these topics and information on further technical detail and support.

1. **Review recommendations from the IACP Technology Policy Framework[2], to include planning, use, and management of any technology in professional policing. This should include policies related to:**
   - Technologies that generate, aggregate, and analyze data
   - Technologies used to acquire process or handle digital evidence
   - Ongoing management review of policies to ensure they are current
2. **Training and proficiency guidelines for all personnel in the collection, preservation, and analysis (where appropriate) of digital evidence, to include**
   - First responders
   - Investigators
   - Crime scene specialists
   - Forensic examiners
3. **Standard Operating Procedures and Policies for digital evidence that outline**
   - Collection and acquisition
   - Marking, documentation, and photography
   - Preservation, packaging, and handling
   - Storage, security, and accountability
   - Access considerations
   - Electronic storage considerations
   - Disaster recovery and resiliency
   - Deviations from policies
4. **Standards for validating proficiency of personnel performing critical digital forensic functions. This should include requiring**
   - Certification and recertification of all personnel involved in the acquisition and examination of digital evidence
   - Proficiency testing within the context of tools, tasks, conditions, and standards
   - Quality review of examiner process and productions
   - Process for correction and mitigation of errors
5. **Digital forensic tools, to include**
   - Authorization to operate and use various technologies
   - Context and limitation of appropriate forensic tools
   - Validation and efficacy testing of forensic tools
   - Quality review/documentation of tool validation and testing
   - Process for correction and mitigation of errors
6. **Digital evidence metrics and impact on operations that address**
   - Collection of data to measure use, context, and volume of digital evidence
   - Analysis of data to understand specific relevance and importance of digital evidence to various statutes
7. **Challenges presented by new emerging or evolving technologies, such as**
   - Cloud data
   - Internet of things (connected/smart city technology)
   - Social networks
   - Vehicle informatics (the computers and systems in cars)
8. **Legal guidelines for digital evidence, such as those related to**
   - Development of effective legal process, communications, and resources
   - Collection, preservation, and analysis of remote digital evidence from third parties
9. **Protecting law enforcement agency systems against cyber threats from seized evidence, to include**
   - General protection from malware, ransomware, and similar threats
   - LEA system design to minimize risk to records and evidence
   - Cyber security and risk management
   - Assessment, evaluation, and testing
10. **Understanding encryption and its operational impact on evidence including**
    - Its potential as a barrier to access
    - Available legal options/resources for compelling access to encrypted digital evidence
    - Available technical options/resources for access to encrypted digital evidence

2 The International Association of Chiefs of Police (2014). "IACP Technology Policy Framework." https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf. As of publication in September 2019, this document is currently being updated.

CRI-TAC Collaborative Reform Initiative
TECHNICAL ASSISTANCE CENTER

The Collaborative Reform Initiative Technical Assistance Center (CRI-TAC) provides customized technical assistance solutions designed to meet the unique needs of state, local, tribal, and campus communities throughout the United States.

The services and topics outlined in this brochure are meant to serve as examples. Requests for assistance that do not fall within one of these areas are given consideration.

Do you have a need in your community?

The CRI-TAC is here to help.

- Tailored, scalable solutions
- Informed by cutting-edge innovation and evidence-based and promising practices
- Designed in a collaborative manner with the agency
- Delivered by subject matter experts from the field
- No cost to the requesting agency

SERVICES PROVIDED

- Resource Referral
- Web-based Training
- In-person Training
- Virtual Mentoring
- Meeting Facilitation
- On-Site Consultation
- Agency Peer Exchange

TOPICS ADDRESSED

- Active Shooter Response
- Community Engagement
- Crime Analysis
- Crisis Intervention
- De-escalation
- Domestic Violence Reduction and Prevention
- Drug-related Crime
- Drug Abuse Prevention
- Elder Abuse
- Focused Deterrence
- Gangs
- Gun Violence Reduction and Prevention
- Homeless Populations
- Hate Crimes
- Human Trafficking
- Intelligence and Information Sharing
- Leadership
- Management and Supervision
- Mass Casualty Response
- Mass Demonstration Response
- Modern Police Performance Management (e.g. CompStat)
- Officer Safety and Wellness
- Private Sector Coordination and Partnerships
- Proactive Policing
- Problem Solving Techniques
- Prosecution Coordination and Partnerships
- Public Sector Coordination and Partnerships
- Recruitment, Hiring, and Retention
- School Safety
- Shared Service Models
- Traffic Safety
- Tribal Law Enforcement
- Violent Crime Reduction and Prevention
- Youth Engagement

Visit **www.CollaborativeReform.org** for more information and to request assistance.

HOW IT WORKS

1. Submit a request via **www.CollaborativeReform.org** Requests must come from a U.S. law enforcement agency and be authorized by the chief executive of the agency.
2. An IACP staff member will contact the requestor and collect additional information.
3. The CRI-TAC will assess the request and make a determination on type of TA to be delivered.
4. The CRI-TAC will work with the agency and applicable partner organizations to develop a customized plan to include success metrics and follow up.

IACP
International Association of Chiefs of Police

What is the Distracted Driving Toolkit?

The Distracted Driving Toolkit provides law enforcement chief executives, command staff, first-line supervisors, and patrol officers with effective strategies that have been used by others to improve distracted driving education and enforcement in their communities, along with tactics to reduce officer distraction in patrol vehicles.

What It Includes

- A report on promising practices for public education, enforcement, and officer safety
- Press release and talking points template that can be used to address distracted driving issues for chiefs of municipal governments and community education
- Two separate 11 x 17 poster infographics - *The Dangers of Distracted Driving & The Dangers of Distracted Driving by Law Enforcement Officers*
- A comprehensive list of resources to help agencies address distracted driving crashes

IACP
International Association of Chiefs of Police

Toolkit

A toolkit is a set of documents or resources designed to be used together.

DOWNLOAD RESOURCE

Toolkit

PowerPoint

Resource Guide

Report/White Paper/Guidelines

2019 Division Midyear

MARCH 24-26 | AUSTIN, TEXAS

The 2019 Division Midyear brought together members from the Midsize Agencies Division, the Division of State and Provincial Police, and the Division of State Associations of Chiefs of Police to discuss critical issues facing the law enforcement community, identify best practices, and participate in several networking opportunities. More than 100 people attended the Midsize Agencies Division meeting, which provided a forum for information exchange regarding topics specific to midsize agencies (outlined below).

Division Midyear Attendance

2019 Division Midyear Discussion Topics

- **Body-Worn Cameras (BWCs):** Research indicates that mid-size agencies are adopting BWC technology at lower rates than larger and smaller agencies, funding being the primary obstacle. Three panelists provided facts and figures in support of developing a program, continuing a program, or ending a program.
  - Deputy Chief Oz Flores – *Arlington Police Department (TX)*
  - Chief David Zack – *Chesterfield Police Department (VA)*
  - Lieutenant Michael Rowling – *Arlington Police Department (VA)*
- **Critical Incident Stress Management and Peer Support:** Panelists provided an overview of the Southeastern Massachusetts Law Enforcement Council Critical Incident Stress Management Unit – clinically supported, regional, law-enforcement-only model of peer assistance to help public safety personnel with critical incident stress management, mental wellness and addiction.
  - Chief Joseph Perkins – *Middleboro Police Department (MA)*
  - Patrolman Angelo Laperna – *Middleboro Police Department (MA)*
  - Detective Robert Swarts – *Taunton Police Department (MA)*
- **Responding to Catastrophic Events:** Panel discussed three significant events that impacted local communities and first responders – California wildfires, Massachusetts neighborhood natural gas explosions and Houston's Hurricane Harvey.
  - Chief Roy Vargas – *Lawrence Police Department (MA)*
  - Chief Kim Comey – *Ventura Police Department (CA)*
  - Chief Art Acevedo – *Houston Police Department (TX)*

- **First Responder's Perspective on the 2018 Santa Fe School Shooting:** Agency leadership discussed the incident, the area-wide response, and dealing with the aftermath of the event.
  - Chief Walter Bruns – *Santa Fe Independent School District Police Department (TX)*
  - Assistant Chief Gary Forward – *Santa Fe Independent School District Police Department (TX)*
- **Transitioning and Sustaining Law Enforcement Organizations through Leadership Application:** This session looked at how development and implementation of one-by-one policing can transform the organizational culture and improve trust within the department and community. The panelists discussed how Leadership in Police Organizations (LPO) programs helped transform departments from crisis into high-performing teams with a positive and ethical culture.
  - Chief Jack Caulley – *Castle Rock Police Department (CO)*
  - Chief David Zibolski – *Beloit Police Department (WI)*

2019 Midsize Agencies Division Annual Business Meeting

OCTOBER 25 | 2019 IACP ANNUAL CONFERENCE & EXPOSITION | CHICAGO, ILLINOIS

The 2019 IACP Annual Conference & Exposition brought together several members from the Midsize Agencies Division to discuss critical issues and elect new members for the Midsize Agencies Division Executive Committee. During the business meeting, attendees heard from federal partners, including U.S. Customs and Border Protection and U.S. Department of Justice Office of Community-Oriented Policing Service and Office of Justice Programs.

- **Officer Suicide Panel:** Officer suicide is a critical issue for this Division, as 40% of the suicides happen in midsize agencies. The panelists provided key perspectives on officer suicide, providing important first-hand knowledge, information, and resources for those who may be impacted.
  - Chief John W. Montney – *Kenosha Police Department (WI)*
  - Karen Solomon – *President, Blue WELLR*
- In addition, the Division membership elected new Midsize Agencies Division Executive Committee members:
  - SOUTHEAST REGIONAL CHAIR
  - Chief Howard Hall, *Roanoke County Police Department (VA)*
  - WEST COAST REGIONAL CHAIR
  - Chief John Bruce, *Richland Police Department (WA)*

Contributions

Throughout the year, Midsize Agencies Division representatives provide subject matter expertise and valuable perspective to programs within the IACP and to external groups. This activity included:

- **The IACP Board of Directors:** The IACP is an association of police leaders committed to advancing the policing profession by promoting leading practices, cooperative efforts, and the exchange of information among police administrators and other institutions and organizations. The IACP is governed by its members – who are represented by both elected and appointed leadership on the Board of Directors. The Board of Directors, which meet four times a year, has the authority to take all appropriate measures and perform all duties required to accomplish the objectives of the Association.

  The Midsize Agencies Division (MSA) General Chair is an integral part of IACP's leadership, lending voice and thoughtfully deliberation to issues of importance to MSA, IACP, and the broader policing profession. Further, the MSA Vice General Chair serves as a non-voting, ex-officio member of the Board of Directors.
- **Bureau of Justice Assistance – Criminal Justice Forecasting Group:** This group brings together executives from midsize law enforcement agencies and research partners to discuss trends, needs, and gaps impacting midsize agencies and identify opportunities to build capacity within those agencies and across the midsize agency network.
- **The IACP Law Enforcement Policy Center:** The Policy Center identifies leading practices and provides sound guidance to the law enforcement profession to assist in developing policies for individual departments. Midsize Agencies Division members participated on several Policy Center working groups to help curate model policies, considerations documents, and concepts and issues papers on various topics, including:
  - Volunteers (including the use of volunteers and volunteer program management and administration)
  - Investigation of Allegations of Employee Misconduct
  - Line-of-Duty-Death/Injury
  - Crowd Management and Control
  - Foot Pursuits
- **IACP Police Facilities Planning Guidelines:** Midsize Agencies Division members worked to develop documents to provide law enforcement executives and project managers with a planning model applicable to all types and sizes of facility projects. These published guidelines outline the facility planning process and alert law enforcement executives to specific design and construction considerations.
- **MADD Impaired Driving Law Enforcement Summit:** Attendees shared their struggles and their strengths in making drunk and drugged driving a focus of their agencies, and a priority in traffic enforcement.
- **IACP Leadership Awards:** The IACP Leadership Awards Program is designed to recognize law enforcement professionals, volunteers, and partner organizations from around the world who demonstrate leadership through their commitment to service. Midsize agencies were represented by 11 out of the 27 awardees in 2019.

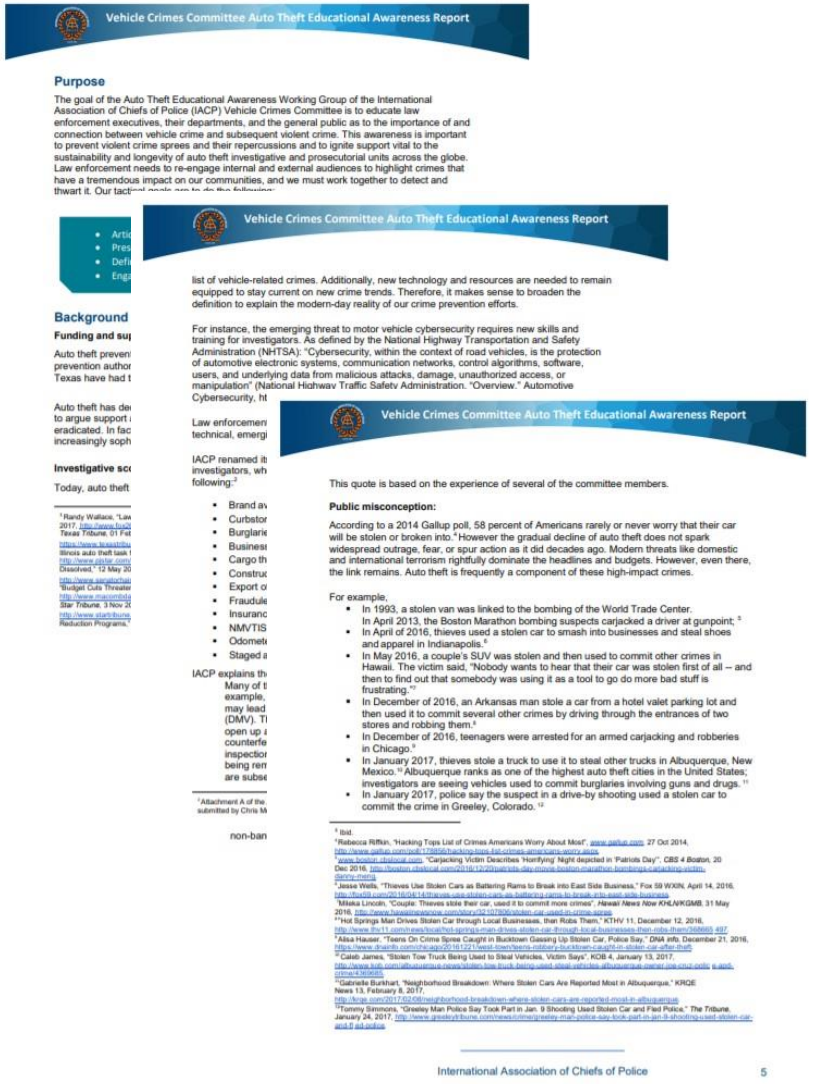
How to Join

If you are interested in elevating the impact of midsize law enforcement agencies around the globe, join the IACP Midsize Agencies Division today! All IACP members who represent agencies with 50 to 999 sworn are welcome and encouraged to join. For questions, contact your MSA Division regional chair or visit the website to learn more:

www.theIACP.org/working-group/division/midsize-agencies-division

MIDSIZE AGENCIES Division | IACP

IACP International Association of Chiefs of Police



Vehicle Crimes Committee Auto Theft Educational Awareness Report

Purpose

The goal of the Auto Theft Educational Awareness Working Group of the International Association of Chiefs of Police (IACP) Vehicle Crimes Committee is to educate law enforcement executives, their departments, and the general public as to the importance of and connection between vehicle crime and subsequent violent crime. This awareness is important to prevent violent crime sprees and their repercussions and to ignite support vital to the sustainability and longevity of auto theft investigative and prosecutorial units across the globe. Law enforcement needs to re-engage internal and external audiences to highlight crimes that have a tremendous impact on our communities, and we must work together to detect and thwart it. Our tactical goals are to do the following:

- Arti
- Pres
- Defi
- Engi

Background

Funding and su

Auto theft preven
prevention author
Texas have had t

Auto theft has de
to argue support
eradicated. In fac
increasingly soph

Investigative sc

Today, auto theft

[1] Randy Wallace, "Law
2017, http://www.fox2
Texas Tribune, 01 Fe
https://www.texastrib
Illinois auto theft task
http://www.pbcfar.com/
Dissolved," 12 May 20
http://www.sacpolice
"Budget Cuts Threate
http://www.macombda
Star Tribune, 3 Nov 2
http://www.startribune
Reduction Programs,"

[2] Attachment A of the
submitted by Chris M

non-ban

Vehicle Crimes Committee Auto Theft Educational Awareness Report

list of vehicle-related crimes. Additionally, new technology and resources are needed to remain equipped to stay current on new crime trends. Therefore, it makes sense to broaden the definition to explain the modern-day reality of our crime prevention efforts.

For instance, the emerging threat to motor vehicle cybersecurity requires new skills and training for investigators. As defined by the National Highway Transportation and Safety Administration (NHTSA): "Cybersecurity, within the context of road vehicles, is the protection of automotive electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation" (National Highway Traffic Safety Administration. "Overview." Automotive Cybersecurity, ht

Law enforcemen
technical, emergi

IACP renamed it
investigators, wh
following:[2]

- Brand av
- Curbstor
- Burglarie
- Busines
- Cargo th
- Construc
- Export c
- Fraudule
- Insuranc
- NMVTIS
- Odomete
- Staged a

IACP explains th
Many of t
example,
may lead
(DMV). Th
open up a
counterfe
inspectior
being ren
are subse

Vehicle Crimes Committee Auto Theft Educational Awareness Report

This quote is based on the experience of several of the committee members.

Public misconception:

According to a 2014 Gallup poll, 58 percent of Americans rarely or never worry that their car will be stolen or broken into.[4] However the gradual decline of auto theft does not spark widespread outrage, fear, or spur action as it did decades ago. Modern threats like domestic and international terrorism rightfully dominate the headlines and budgets. However, even there, the link remains. Auto theft is frequently a component of these high-impact crimes.

For example,

- In 1993, a stolen van was linked to the bombing of the World Trade Center.
  In April 2013, the Boston Marathon bombing suspects carjacked a driver at gunpoint; [5]
- In April of 2016, thieves used a stolen car to smash into businesses and steal shoes and apparel in Indianapolis.[6]
- In May 2016, a couple's SUV was stolen and then used to commit other crimes in Hawaii. The victim said, "Nobody wants to hear that their car was stolen first of all – and then to find out that somebody was using it as a tool to go do more bad stuff is frustrating."[7]
- In December of 2016, an Arkansas man stole a car from a hotel valet parking lot and then used it to commit several other crimes by driving through the entrances of two stores and robbing them.[8]
- In December of 2016, teenagers were arrested for an armed carjacking and robberies in Chicago.[9]
- In January 2017, thieves stole a truck to use it to steal other trucks in Albuquerque, New Mexico.[10] Albuquerque ranks as one of the highest auto theft cities in the United States; investigators are seeing vehicles used to commit burglaries involving guns and drugs.[11]
- In January 2017, police say the suspect in a drive-by shooting used a stolen car to commit the crime in Greeley, Colorado.[12]

[3] Ibid.
[4] Rebecca Riffkin, "Hacking Tops List of Crimes Americans Worry About Most", www.gallup.com, 27 Oct 2014, http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry-about.
[5] "Carjacking Victim Describes 'Horrifying' Night depicted in 'Patriots Day'", *CBS 4 Boston*, 20 Dec 2016, http://boston.cbslocal.com/2016/12/20/patriots-day-movie-boston-marathon-bombings-carjacking-victim-danny-cheng/.
[6] Jesse Wells, "Thieves Use Stolen Cars as Battering Rams to Break into East Side Business," Fox 59 WXIN, April 14, 2016, http://fox59.com/2016/04/14/thieves-use-stolen-cars-as-battering-rams-to-break-into-east-side-business/.
[7] Mileka Lincoln, "Couple: Thieves stole their car, used it to commit more crimes", *Hawai'i News Now* KHL/KGMB, 31 May 2016, http://www.hawaiinewsnow.com/story/32197806/stolen-car-used-in-crime-spree.
[8] "Hot Springs Man Drives Stolen Car through Local Businesses, then Robs Them," KTHV 11, December 12, 2016, http://www.thv11.com/news/local/hot-springs-man-drives-stolen-car-through-local-businesses-then-robs-them/398693 497.
[9] Alisa Hauser, "Teens On Crime Spree Caught in Bucktown Gassing Up Stolen Car, Police Say," *DNA info*, December 21, 2016, https://www.dnainfo.com/chicago/20161221/west-town/teens-robbery-bucktown-caught-in-stolen-car-after-theft.
[10] Caleb James, "Stolen Tow Truck Being Used to Steal Vehicles, Victim Says", KOB 4, January 13, 2017, http://www.kob.com/albuquerque-news/stolen-tow-truck-being-used-steal-vehicles-albuquerque-owner-joe-cruz-colls s-said-crime/4369685.
[11] Gabrielle Burkhart, "Neighborhood Breakdown: Where Stolen Cars Are Reported Most in Albuquerque," KRQE News 13, February 8, 2017, http://krqe.com/2017/02/08/neighborhood-breakdown-where-stolen-cars-are-reported-most-in-albuquerque.
[12] Tommy Simmons, "Greeley Man Police Say Took Part in Jan. 9 Shooting Used Stolen Car and Fled Police," *The Tribune*, January 24, 2017, http://www.greeleytribune.com/news/crime/greeley-man-police-say-took-part-in-jan-9-shooting-used-stolen-car-and-fled-police.

Psychological Fitness-for-Duty Evaluation Guidelines

Ratified by the IACP Police Psychological Services Section
Philadelphia, Pennsylvania, 2013

1. **Purpose**

1.1 The IACP Police Psychological Services Section (PPSS) developed these guidelines to educate and inform the public safety agencies that request fitness-for-duty evaluations (FFDEs) and the practice of examiners who perform them.

1.2 These guidelines are most effectively used through collaboration between examiners and public safety agencies. It is desirable that these guidelines be reviewed by both the referring agency and the examiner and that any conflicts between an agency's or examiner's policies or practices and these guidelines be discussed and the rationale for action contrary to the guidelines be documented before commencing the FFDE.

2. **Limitations**

2.1 The term "guidelines" refers to statements that suggest or recommend specific professional behavior, endeavors, or conduct for examiners. Guidelines differ from standards in that standards are mandatory and may be accompanied by an enforcement mechanism. Guidelines are aspirational in intent. They are intended to facilitate the continued systematic development of the profession and facilitate a high level of practice by examiners. Guidelines are not intended to be mandatory or exhaustive and may not be applicable to every professional situation. They are not definitive, and they are not intended to take precedence over the judgment of examiners.

2.2 These guidelines are not intended to serve as a basis for disciplinary action or civil or criminal liability. The standard of care is established by a competent authority not by the guidelines. No ethical, licensure, or other administrative action or remedy, nor any other cause of action, should be taken *solely* on the basis of an examiner practicing in a manner consistent or inconsistent with these guidelines.

2.3 These guidelines are not intended to establish a rigid standard of practice for FFDEs. Instead, they are intended to reflect the commonly accepted practices of the PPSS members and the agencies they serve.

2.4 Each of the guidelines may not apply in a specific case or in all situations. The decision as to what is or is not done in a particular instance is ultimately the responsibility of the agency and examiner.

2.5 These guidelines are written to apply to agencies within the jurisdiction of the United States and, as such, may require modification for use by agencies in other countries.

3. **Definition**

3.1 A psychological FFDE is a formal, specialized examination of an incumbent employee that results from (1) objective evidence that the employee may be unable to safely or effectively perform a defined job and (2) a reasonable basis for believing that the cause may be attributable to a psychological condition or impairment. The central purpose of an FFDE is to determine whether the employee is able to safely and effectively perform his or her essential job functions.

4. **Threshold Considerations**

4.1 Referring an employee for an FFDE is indicated whenever there is an objective and reasonable basis for believing that the employee may be unable to safely and/or effectively perform his or her duties due to a psychological condition or impairment. An objective basis is one that is not merely speculative but derives from direct observation, credible third-party report, or other reliable evidence.

4.2 When deciding whether or not to conduct an FFDE, both the agency and examiner should take into account its potential usefulness and appropriateness given the specific circumstances, and the agency should consider whether other remedies (e.g., education, training, discipline, physical FFDE) might be more appropriate or useful instead of, or in addition to, a psychological FFDE.

4.3 In all consultations, the examiner strives to remain impartial and objective and to avoid undue influences by any of the parties involved in the case.

4.4 In general, mental health professionals refrain from rendering fitness-for-duty opinions when they are not conducting an FFDE, such as when providing debriefings in the context of an officer-involved shooting or similar services in other situations when return to duty is at issue.

5. **Examiner Qualifications**

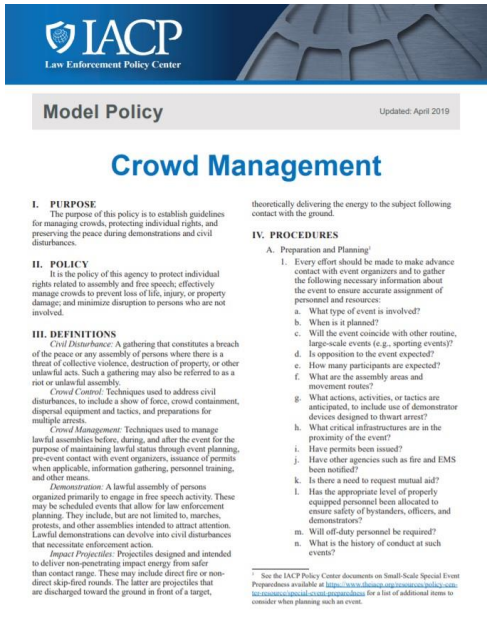
5.1 In light of the nature of these evaluations and the potential consequences to the agency, the examinee, and the public, it is important for examiners to perform FFDEs with maximum attention to the relevant legal, ethical, and practice standards. Such standards include, but are not limited to, the American Psychological Association's (APA's) Ethical Principles of Psychologists and Code of Conduct. Examiners should also consider and be guided by statutory and case law applicable to the employing agency's jurisdiction. Consequently, it is recommended that these evaluations be conducted only by a qualified mental health professional. At a minimum, it is recommended that examiners:

5.1.1 be licensed psychologists or psychiatrists with education, training, and experience in the diagnostic evaluation of mental and emotional disorders;

5.1.2 be competent in the evaluation of law enforcement personnel;

Model Policies

The IACP Law Enforcement Policy Center has been identifying leading practices and providing sound guidance to the law enforcement profession to assist in developing policies for individual departments. All policies and policy documents that are developed are run through the Policy Center to ensure that other groups and perspectives are included and that there is alignment among the policy positions put forth by the IACP Board.



IACP Law Enforcement Policy Center

Model Policy — Updated: April 2019

Crowd Management

I. PURPOSE

The purpose of this policy is to establish guidelines for managing crowds, protecting individual rights, and preserving the peace during demonstrations and civil disturbances.

II. POLICY

It is the policy of this agency to protect individual rights related to assembly and free speech; effectively manage crowds to prevent loss of life, injury, or property damage; and minimize disruption to persons who are not involved.

III. DEFINITIONS

Civil Disturbance: A gathering that constitutes a breach of the peace or any assembly of persons where there is a threat of collective violence, destruction of property, or other unlawful acts. Such a gathering may also be referred to as a riot or unlawful assembly.

Crowd Control: Techniques used to address civil disturbances, to include a show of force, crowd containment, dispersal equipment and tactics, and preparations for multiple arrests.

Crowd Management: Techniques used to manage lawful assemblies before, during, and after the event for the purpose of maintaining lawful status through event planning, pre-event contact with event organizers, issuance of permits when applicable, information gathering, personnel training, and other means.

Demonstration: A lawful assembly of persons organized primarily to engage in free speech activity. These may be scheduled events that allow for law enforcement planning. They include, but are not limited to, marches, protests, and other assemblies intended to attract attention. Lawful demonstrations can devolve into civil disturbances that necessitate enforcement action.

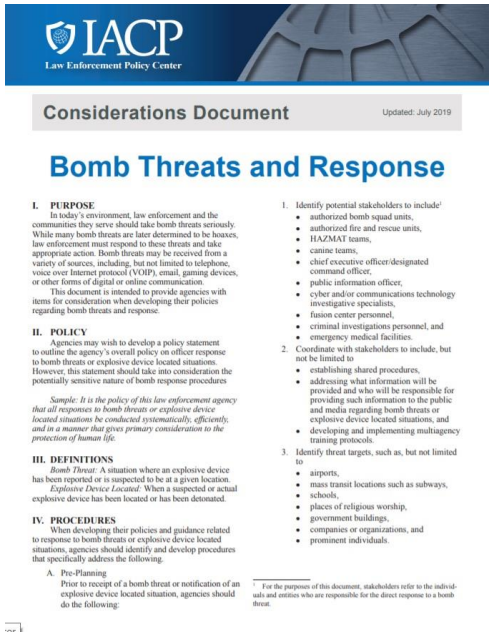
Impact Projectiles: Projectiles designed and intended to deliver non-penetrating impact energy from safer than contact range. These may include direct fire or non-direct skip-fired rounds. The latter are projectiles that are discharged toward the ground in front of a target, theoretically delivering the energy to the subject following contact with the ground.

IV. PROCEDURES

A. Preparation and Planning[1]

1. Every effort should be made to make advance contact with event organizers and to gather the following necessary information about the event to ensure accurate assignment of personnel and resources:
   a. What type of event is involved?
   b. When is it planned?
   c. Will the event coincide with other routine, large-scale events (e.g., sporting events)?
   d. Is opposition to the event expected?
   e. How many participants are expected?
   f. What are the assembly areas and movement routes?
   g. What actions, activities, or tactics are anticipated, to include use of demonstrator devices designed to thwart arrest?
   h. What critical infrastructures are in the proximity of the event?
   i. Have permits been issued?
   j. Have other agencies such as fire and EMS been notified?
   k. Is there a need to request mutual aid?
   l. Has the appropriate level of properly equipped personnel been allocated to ensure safety of bystanders, officers, and demonstrators?
   m. Will off-duty personnel be required?
   n. What is the history of conduct at such events?

[1] See the IACP Policy Center documents on Small-Scale Special Event Preparedness available at https://www.theiacp.org/resources/policy-center-resource/special-event-preparedness for a list of additional items to consider when planning such an event.



IACP Law Enforcement Policy Center

Considerations Document — Updated: July 2019

Bomb Threats and Response

I. PURPOSE

In today's environment, law enforcement and the communities they serve should take bomb threats seriously. While many bomb threats are later determined to be hoaxes, law enforcement must respond to these threats and take appropriate action. Bomb threats may be received from a variety of sources, including, but not limited to telephone, voice over Internet protocol (VOIP), email, gaming devices, or other forms of digital or online communication.

This document is intended to provide agencies with items for consideration when developing their policies regarding bomb threats and response.

II. POLICY

Agencies may wish to develop a policy statement to outline the agency's overall policy on officer response to bomb threats or explosive device located situations. However, this statement should take into consideration the potentially sensitive nature of bomb response procedures

Sample: It is the policy of this law enforcement agency that all responses to bomb threats or explosive device located situations be conducted systematically, efficiently, and in a manner that gives primary consideration to the protection of human life.

III. DEFINITIONS

Bomb Threat: A situation where an explosive device has been reported or is suspected to be at a given location.

Explosive Device Located: When a suspected or actual explosive device has been located or has been detonated.

IV. PROCEDURES

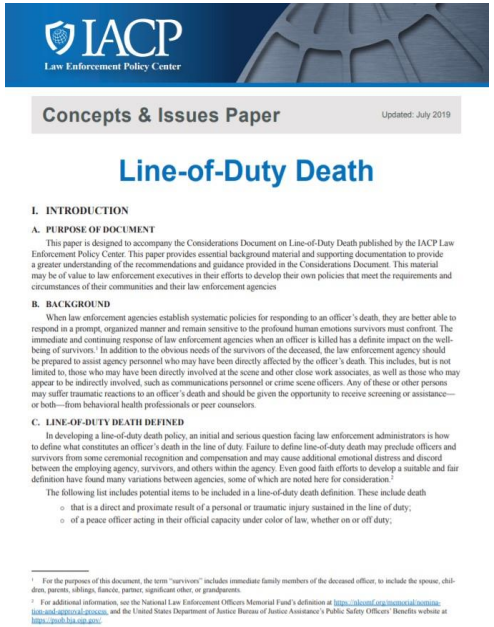
When developing their policies and guidance related to response to bomb threats or explosive device located situations, agencies should identify and develop procedures that specifically address the following.

A. Pre-Planning

Prior to receipt of a bomb threat or notification of an explosive device located situation, agencies should do the following:

1. Identify potential stakeholders to include[1]
   - authorized bomb squad units,
   - authorized fire and rescue units,
   - HAZMAT teams,
   - canine teams,
   - chief executive officer/designated command officer,
   - public information officer,
   - cyber and/or communications technology investigative specialists,
   - fusion center personnel,
   - criminal investigations personnel, and
   - emergency medical facilities.
2. Coordinate with stakeholders to include, but not be limited to
   - establishing shared procedures,
   - addressing what information will be provided and who will be responsible for providing such information to the public and media regarding bomb threats or explosive device located situations, and
   - developing and implementing multiagency training protocols.
3. Identify threat targets, such as, but not limited to
   - airports,
   - mass transit locations such as subways,
   - schools,
   - places of religious worship,
   - government buildings,
   - companies or organizations, and
   - prominent individuals.

[1] For the purposes of this document, stakeholders refer to the individuals and entities who are responsible for the direct response to a bomb threat.



IACP Law Enforcement Policy Center

Concepts & Issues Paper — Updated: July 2019

Line-of-Duty Death

I. INTRODUCTION

A. PURPOSE OF DOCUMENT

This paper is designed to accompany the Considerations Document on Line-of-Duty Death published by the IACP Law Enforcement Policy Center. This paper provides essential background material and supporting documentation to provide a greater understanding of the recommendations and guidance provided in the Considerations Document. This material may be of value to law enforcement executives in their efforts to develop their own policies that meet the requirements and circumstances of their communities and their law enforcement agencies

B. BACKGROUND

When law enforcement agencies establish systematic policies for responding to an officer's death, they are better able to respond in a prompt, organized manner and remain sensitive to the profound human emotions survivors must confront. The immediate and continuing response of law enforcement agencies when an officer is killed has a definite impact on the well-being of survivors.[1] In addition to the obvious needs of the survivors of the deceased, the law enforcement agency should be prepared to assist agency personnel who may have been directly affected by the officer's death. This includes, but is not limited to, those who may have been directly involved at the scene and other close work associates, as well as those who may appear to be indirectly involved, such as communications personnel or crime scene officers. Any of these or other persons may suffer traumatic reactions to an officer's death and should be given the opportunity to receive screening or assistance—or both—from behavioral health professionals or peer counselors.

C. LINE-OF-DUTY DEATH DEFINED

In developing a line-of-duty death policy, an initial and serious question facing law enforcement administrators is how to define what constitutes an officer's death in the line of duty. Failure to define line-of-duty death may preclude officers and survivors from some ceremonial recognition and compensation and may cause additional emotional distress and discord between the employing agency, survivors, and others within the agency. Even good faith efforts to develop a suitable and fair definition have found many variations between agencies, some of which are noted here for consideration.[2]

The following list includes potential items to be included in a line-of-duty death definition. These include death

- that is a direct and proximate result of a personal or traumatic injury sustained in the line of duty;
- of a peace officer acting in their official capacity under color of law, whether on or off duty;

[1] For the purposes of this document, the term "survivors" includes immediate family members of the deceased officer, to include the spouse, children, parents, siblings, fiancée, partner, significant other, or grandparents.

[2] For additional information, see the National Law Enforcement Officers Memorial Fund's definition at https://nleomf.org/memorial/nominate-and-approval-process, and the United States Department of Justice Bureau of Justice Assistance's Public Safety Officers' Benefits website at https://psob.bja.ojp.gov/.

IACP Law Enforcement Policy Center

Need to Know... — Updated: April 2019

Investigation of Allegations of Employee Misconduct

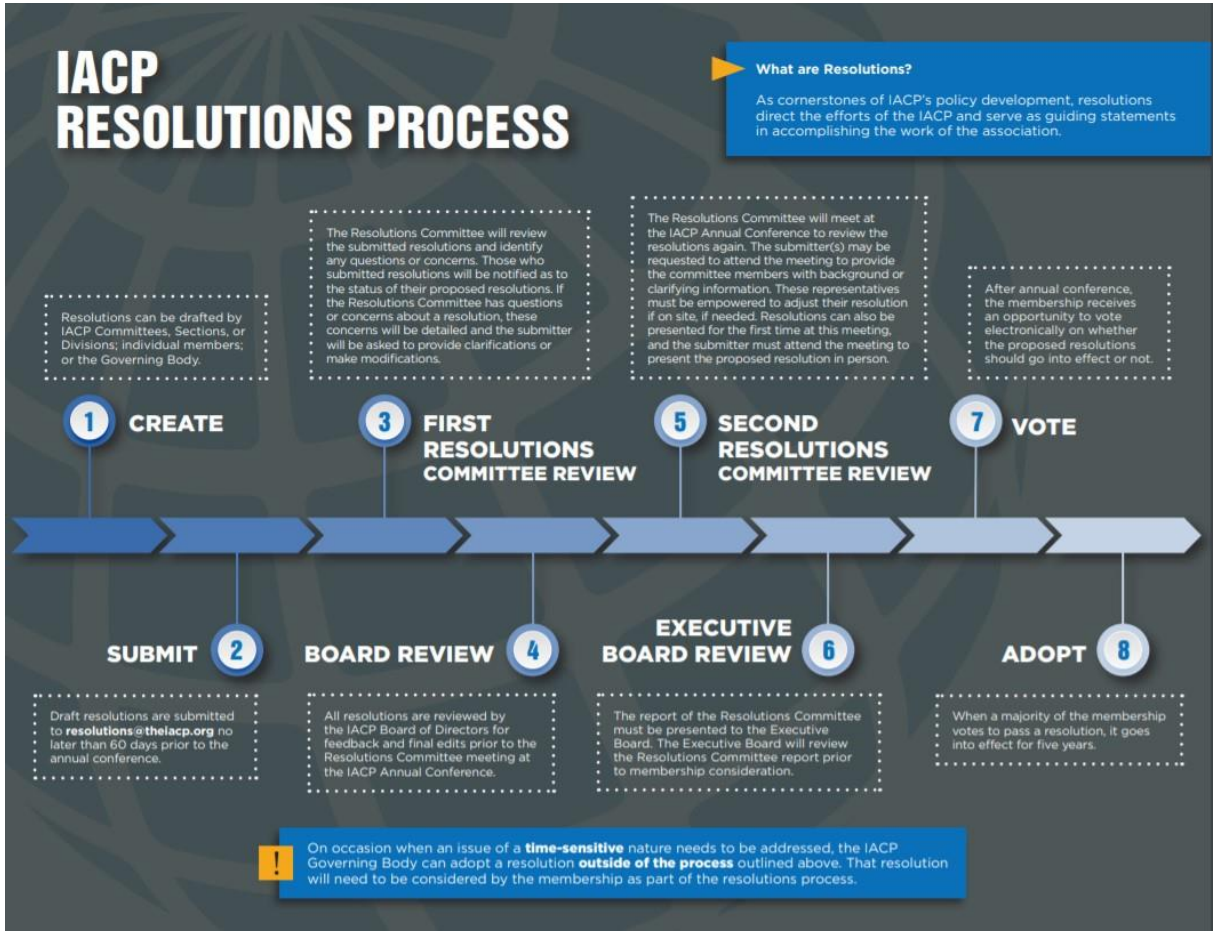
Law enforcement agencies should establish policies and procedures for fully, fairly, and impartially investigating complaints and allegations of employee misconduct. Transparency of these procedures will aid in fostering trust with the community and acceptance of the process by agency employees.

- Agencies should develop **individualized complaint forms** that allow members of the public to report alleged employee misconduct. Agencies should also identify methods for internal reports of misconduct.
- Complainants should be provided with the opportunity to submit complaints **in person, over the telephone, in writing, or via the Internet**.
- A **central authority** with primary responsibility for conducting investigations of employee misconduct allegations should be identified. This may include the Office of Professional Standards (OPS) or Internal Affairs Unit.
- **Supervisors** should be given the opportunity to conduct preliminary assessments of complaints to determine if grounds exist to conduct an administrative investigation. However, OPS should maintain the authority to assume responsibility of the investigation at any time.
- Employees accused of misconduct should be **interviewed** as part of the investigation. All applicable warnings regarding compelled statements should be provided to the employee and the employee should be allowed a personal or professional representative to be present as an observer.
- **Examinations and searches** may be necessary as part of the investigation. This may include breath, urine, or polygraph examinations; lineups; and/or searches of property belonging to the agency. Agencies should consult their legal advisors regarding applicable restrictions.
- Once the investigation is complete, a final **disposition** (sustained, not sustained, exonerated, unfounded, or policy failure) should be determined by the supervisor or OPS, as appropriate, and forwarded to the agency chief executive for review and approval.
- If the investigation results in a disposition of **sustained**, a formal document outlining the administrative charges should be drafted and provided to the employee. The employee should be provided with an opportunity to respond and/or appeal.
- Where necessary, all **corrective actions** should be approved by the chief executive or their designee and fully documented.
- All information related to the investigation of allegations of misconduct should be considered **confidential** and retained under secure conditions.
- Once the investigation is complete, a letter should be sent to the **complainant** explaining the final disposition.

© Copyright 2019. Departments are encouraged to use this document to establish policies customized to their agency and jurisdiction. However, copyright is held by the International Association of Chiefs of Police, Alexandria, Virginia U.S.A. All rights reserved under both international and Pan-American copyright conventions. Further dissemination of this material is prohibited without prior written consent of the copyright holder.

IACP International Association of Chiefs of Police

Resolutions



IACP
International Association of Chiefs of Police

Crime Prevention, Domestic Security and Quality of Life: Definition and Significant Value of Community Policing

Submitted by: Community Policing Committee

Co-Sponsored by: Communications & Technology Committee, Crime Prevention Committee, Education & Training Committee, Forensics Committee, Committee on Homeland Security, Human & Civil Rights Committee, Juvenile Justice & Child Protection Committee, Narcotics & Dangerous Drugs Committee, Police Administration Committee, Private Sector Liaison Committee, Police Professional Standards Ethics & Image Committee, Research Advisory Committee, Terrorism Committee, Transnational Crime Committee, Victim Services Committee

COM.01.19

WHEREAS, for decades the IACP has recognized, acknowledged, and endorsed the value and effectiveness of community policing; and

WHEREAS, over the years various e
philosophy, principles, and practic

WHEREAS, it is beneficial to clearly

WHEREAS, problem-solving throug
key elements of community policir

WHEREAS, police legitimacy and p
on the conditions that produce cri
and

WHEREAS, the essential elements
partnership, community trust build
involvement and responsibility, are

Worldwide Call for Legislation and/or Appropriate Regulation That Mandates Encryption Implementation Regimes That Maintain Reasonable Security of Communications and Stored Data, yet Permit Lawful Access by Law Enforcement Pursuant to the Rule of Law

Submitted by: Police Investigative Operations Committee and Computer Crimes & Digital Evidence Committee

PIO.23.19

WHEREAS, the use of user and provider-controlled forms of strong encryption applied to communications in transmission and to data storage devices, although simultaneously serving to help prevent certain types of crimes and preserve privacy, has also, with increased frequency, been implemented in such a manner as to significantly degrade the ability of law enforcement worldwide to detect and prevent serious crime before it occurs, as well as inhibit the identification of those responsible for crimes already committed; and

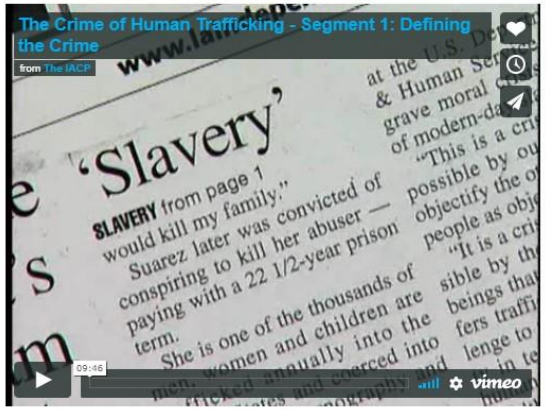
WHEREAS, the expanding implementation of user-only access encryption, in addition to enhancing privacy generally, is also specifically facilitating criminal activity worldwide by ensuring that evidence of crime is beyond the reach of law enforcement despite compliance with legal requirements that authorize the lawful seizure and use of such evidence and information in accordance with the applicable laws of each nation; and

WHEREAS, the expanding implementation of user-only access encryption may be seen by some in the industry as a means of plausibly denying knowledge of and responsibility for the use of their services or devices by criminals, terrorists, and spies so as to potentially obviate any legal obligation to stop or mitigate such harms; and

WHEREAS, it is recognized that providers who implement end-to-end encryption are also under economic pressure to compete with other international providers on a level playing field and that,

Videos

Videos can include YouTube/Vimeo videos, Biteables, or Roll-Call videos.



IACP
International Association of Chiefs of Police

Webinar/Podcast

Recorded Webinar: Frontline Officer's Role Interacting with Children at Domestic Violence Scenes

Recorded Webinar: Death Notification when Children are Involved: Trauma-informed Strategies for Delivering the Most Difficult News to the Most Vulnerable

Recorded Webinar: The Impact of Exposure on Children and Families: What Law Enforcement Professionals Should Know and Be Able to Do

Recorded Webinar: Building Trauma-Informed Police Responses to Children Exposed to Violence: Training and Tools

IACP
International Association of Chiefs of Police