Association of State Criminal Investigative Agencies

January 28, 2015

Charles Ramsey
Commissioner
Philadelphia Police Department
Co-Chair
President's Task Force on 21st Century Policing

Laurie Robinson
Clarence J. Robinson Professor of Criminology, Law and Society
George Mason University
Co-Chair
President's Task Force on 21st Century Policing

Dear Commissioner Ramsey and Professor Robinson,

On behalf of the members of the Association of State Criminal Investigative Agencies (ASCIA) I am pleased to submit the attached testimony for the task force's consideration. ASCIA is happy to provide any additional perspectives for task force members.

Thank you for your commitment to leading this effort.

Sincerely,

Ronald C. Sloan
President, ASCIA
Director, Colorado Bureau of Investigation

Introduction

The Association of State Criminal Investigative Agencies (ASCIA) is pleased to provide testimony for the President's Task Force on 21st Century Policing. ASCIA membership consists of the senior executives of statewide criminal investigative agencies in the United States, whether they are an independent bureau within the state or a state police agency with both criminal and other enforcement responsibilities. While our membership is qualified to provide input on a broad range of topics before the task force, this testimony focuses on three areas: 1) Investigations of officer involved shootings (OIS); 2) Responsible use of criminal intelligence and information sharing; and 3) Responsible use of technology and social media by law enforcement investigators.

Investigations of officer involved shootings by police

State criminal investigative agencies are in positions to ensure that investigations of police use of force or other actions that result in serious injury and/or death can be conducted in a skilled, impartial, unbiased, and fair manner that focuses on fact finding. While investigations of this nature are not standardized across the country today, best practice foundational protocols can enhance public trust. A recent survey of ASCIA members reveals that over the last two years, state criminal investigative agencies have successfully conducted in excess of 1500 investigations of officer involved shootings. Drawing on this considerable experience with these investigations, ASCIA would offer the following as a recommended approach.

Agents of a state's criminal investigative agency should either conduct these types of investigations, or participate on a team of investigators from different agencies. Where possible, the team of investigators should be independent from the agencies that employ the subject officers. Operational responsibility for the investigative team should be a management level agent of the state criminal investigative agency, working in conjunction with the appropriate prosecutor's office for legal guidance pursuant to any assessment of findings.

Both during and at the conclusion of an investigation, the "managing agent" for the state criminal investigative agency should work in conjunction with the prosecutor with jurisdiction and senior management of the state agency to communicate as appropriate with the involved law enforcement agency's Chief Law Enforcement Officer for purposes of managing local community communications and internal law enforcement agency concerns. Where possible, crime scene response and processing should be conducted by the state criminal investigative agency, or with involvement of the state criminal investigative agency that is focused on fact finding. Any required forensic examination of evidence should be conducted by the state criminal investigative agency.

Protocols for the timing of interviews or voluntary statements by subject officers in OIS should be written and agreed upon in advance and adhered to by the investigating agency or team. Protocols for the timing and allowances for legal representation, psychological support and/or de-briefing, administration of Miranda advisements, and the collection of non-testimonial evidence should be written and agreed upon in advance and adhered to by the investigating agency or team. Standards should be developed for collecting data associated with the case. Additionally, final prosecutorial decisions should rest with the prosecutor in whose jurisdiction the agency is located or in the jurisdiction where the incident occurred (if different from where the agency is located).

ASCIA recognizes that not all states give their state criminal investigative agency the explicit statutory authority to take over an investigation. In these states, there should be a clear set of protocols in place that encourages joint investigative teams, which have been trained to work under the direction of a special prosecutor. This can help alleviate concerns of bias and predetermined outcomes. For example, in South Dakota, the state investigative agency is the lead agency in all OIS that happen within the state. This has

come about by tradition rather than state legislative action. Clear and trusted protocols have been developed that make transparent what should be expected when a Chief or Sheriff makes a request for assistance. Additionally, through these protocols, the press and public have become accustomed to how long an investigation will take and informed of the conclusions that have been made. This has helped to engender trust with the public that the investigation will be fair and impartial.

In any criminal investigation, including officer use-of-force whether deadly or not, one of the key components is the collection and analysis of physical evidence in order to gather all facts pertaining to an incident. When properly tested and analyzed, forensic evidence can provide investigative leads, corroborate or refute testimony, and provide critical information regarding the event in question. Crime scenes should be processed by qualified individuals who are experts in the preservation and collection of evidence. Analysis of evidence should be performed by an accredited laboratory and qualified analysts. Due to the nature of these types of investigations it is imperative that the analysis of evidence be prioritized and expedited to the greatest extent possible without jeopardizing the quality or integrity of the analysis. In cases involving a death, an autopsy should be performed by a qualified medical examiner experienced in these types of cases. All ancillary testing and analyses should be done by an accredited laboratory. All aspects of the medical legal investigation should be prioritized and expedited to the greatest extent possible without jeopardizing quality or integrity. Communication between prosecutors, investigators, crime scene specialists, laboratory personnel, and medical examiner personnel should be maintained at all times. Good communication will ensure that a thorough forensic investigation is completed in an effective, timely manner.

Responsible use of criminal intelligence and information sharing

Criminal intelligence and information sharing help investigators work smarter and inform effective public safety strategies. Major progress has occurred over the past decade thanks to strong vision by policing leaders; policy leadership by entities like the Program Manager for the Information Sharing Environment (PM-ISE), the Global Justice Information Sharing Initiative (Global), and the Criminal Intelligence Coordinating Council (CICC); and groundbreaking innovation by industry partners.

But "the last mile" of a nationwide information sharing environment remains uncharted. For example, most investigators still cannot search the basic records systems of America's police departments like computer aided dispatch (CAD) and records management systems (RMS) to perform searches that can "connect the dots" in investigations. In many states the ability of one major city to find out if another major city has had involvement with a "Mr. John Smith" still requires a phone call. The value of sharing RMS records with Federal partners is also mostly unrealized, but where it occurs routinely it has significant impact on Federal investigative efforts. Local jurisdictions manage 85 percent of all public safety information, and while innovations in multijurisdictional collaboration like the National Network of Fusion Centers (fusion centers) and the Criminal Intelligence Enterprise (CIE) have greatly helped to break down barriers, more progress is essential to make criminal investigations more effective and efficient. Some states are independently moving toward that "last mile," but funding and coordinated policy support is needed for a comprehensive solution based upon national standards and privacy principles.

There are currently 78 recognized fusion centers in the United States, all of which were established by state and local governments following the attacks of September 11, 2001. ASCIA member agencies "own" the designated state fusion center in 34 states. From a federal perspective, these centers play an important counterterrorism and preparedness role by enabling both vertical and horizontal information sharing on threats to the homeland. But they have become very valuable in addressing crime every day. Early on, most of these centers adopted an "all crimes" approach. This was in recognition that the primary value of

these centers was in supporting local and state police operations to more effectively and efficiently provide services to the community, engage in advanced criminal intelligence analysis, partner with the public, and help develop prevention strategies.

Fusion centers can be leveraged for the application of "smart policing" or "information-led policing" to support local agency initiatives on a broader scale including in rural areas. The fusion centers play a critical role in making more efficient use of information provided by the community in a proactive manner to address crime, strengthen homeland security, and provide situational awareness to public safety and community leaders. They provide analytics to help local police departments and sheriffs offices utilize understaffed patrol units more effectively to patrol areas of high hazard and provide information to the public, civic groups, parole, probation, private sector and corrections partners. Better analytics and information sharing also allow the police to address the crime problems confronting neighborhoods by using tactics that are less intrusive, less disruptive to the fiber of the neighborhoods, and consistent with privacy and civil liberties imperatives. The use of information coordinated by fusion centers can enhance prevention and assist in more rapid apprehension of criminal suspects. Dealing effectively with these criminals instills in the community the feeling that law enforcement is addressing true threats to neighborhood peace and stability and reduces future victimization.

A cornerstone of accountability in law enforcement information sharing and analysis is Chapter 28 of the Code of Federal Regulations, Part 23 (28 CFR Part 23). It contains guidelines and implementing standards for law enforcement agencies working with criminal intelligence systems. It was last clarified in the late 1990s. While the guidance has stood the test of time and helped thousands of agencies, ASCIA recommends that an initiative be undertaken to refresh 28 CFR Part 23 to address the myriad issues that have developed in criminal intelligence analysis and sharing over the past 15 years. Additionally, standardization of law enforcement criminal intelligence units can be supported through a refresh of Law Enforcement Intelligence Unit (LEIU) standards.

Deconfliction is an important information sharing practice among law enforcement agencies. It enhances officer safety by preventing "blue-on-blue" incidents, it enhances operational coordination, and is a professional courtesy to notify jurisdictions about operational activity. Major progress has occurred over the past year to make the largest national deconfliction technical systems interoperable, and more should be done to ensure deconfliction is standard practice across all law enforcement agencies.

Responsible use of technology and social media by law enforcement investigators

To conduct effective criminal investigations in the 21st Century, law enforcement at all levels must be able to access digital evidence with appropriate legal process. Many of today's crime scenes are full of digital evidence – information that can help generate leads, identify criminal networks, and help implicate or exonerate a suspect. Given this reality, law enforcement officials and lawmakers have aired concerns about the "going dark" phenomenon – the increasing difficulty in obtaining access to potential evidence of a crime via communications systems and computing devices.

Even when an impartial judge has signed a search warrant indicating probable cause that evidence of a crime will be found in a search of communications content, law enforcement may not be able to access the information. For example, some increasingly popular communications methods (e.g. Voice over Internet Protocol; messaging via Internet enabled gaming consoles) were not engineered to enable lawful intercept activity by law enforcement. These technologies enable criminals to communicate with less fear of their activity being detected or intercepted by law enforcement. Another example is technology companies that are now selling communications devices with encryption enabled as a default setting for information on the device. Even with a warrant, investigators will be unable to access information from the devices unless

the owner "unlocks" the device with a PIN code, which current law does not allow law enforcement to compel. As a result, evidence of criminal conduct on the device such as child sexual exploitation, human trafficking, and illegal drug distribution becomes undiscoverable.

ASCIA members certainly understand the imperative to protect individual privacy and prevent cyber threats. However, ASCIA strongly believes that policy makers and the public should have a clear understanding – through transparent debate – of the potential consequences of criminal investigators' inability to obtain evidence that can solve crimes. Put yourselves in the shoes of a crime victim or their family members – do you want certain evidence to be technically impossible to obtain by investigators who are working to bring justice to the victim?

The Communications Assistance for Law Enforcement Act (CALEA) was enacted to ensure that law enforcement has the ability to conduct electronic surveillance activities pursuant to a lawful court order. An update to CALEA should be considered to ensure that 21st Century law enforcement investigators can obtain access to evidence that is increasingly important in criminal investigations, while strengthening safeguards for citizens' privacy and civil liberties. Similarly, emergency provisions should be strengthened in existing laws (e.g. Stored Communications Act). Today, federal law puts the decision in the hands of communications providers to determine whether an "emergency" public safety situation exists that would enable providers to provide certain information to investigators. This should be reversed: with appropriate oversight and after-action process, the decision to deem an "emergency" situation should be made by law enforcement – not communications providers.

Congress should also consider updating the Stored Communications Act to equate "addressing information" for newer technologies with addressing information in traditional communications technologies. Current law makes a distinction between these two types of information despite their functional equivalency, which requires different levels of legal process to obtain the same type of information.

New investigative technologies continue to play a crucial role in helping criminal investigators generate leads and solve crimes. Without the ability of law enforcement to take advantage of available technology, it simply means that unnecessary roadblocks are thrown in front of investigators. Automatic license plate readers, facial recognition software, "IMSI-catchers", social media research, and other tools are increasingly important in generating and analyzing information in an investigation. ASCIA fully recognizes and appreciates the concerns of the public and policy makers over the use of technology by law enforcement. However, in many instances these concerns are based on misinformation, innuendo, and a misunderstanding of how the technology works, how it is used in practice, and the nature of the data it collects.

With appropriate constraints, law enforcement should be able to take advantage of ever-improving technology just like any other profession. Policy makers should make an extra effort in the 21st Century to understand the application of these technologies to public safety and criminal investigations so that legislative and regulatory protections for citizens' privacy, civil rights, and civil liberties do not prevent the use of technology or the data that is produced.

For instance, automatic license plate readers (LPR) are important tools that police use daily to recover stolen vehicles, generate investigative leads, and solve crimes. Despite the effectiveness of this and many other technologies, however, some are pushing false narratives and misinformation about law enforcement "tracking" innocent people. The real story about law enforcement's use of technology to investigate crimes is one of responsible use every day that is guided by strict adherence to relevant laws and policies. Yet we

still must work across all levels of law enforcement to solidify policies regarding allowable use, privacy protections, and officer accountability. To help with this, there should be recognition of the need by any agency that wishes to acquire certain technologies that standards and policies must be established *prior* to operationalizing the technology. The International Association of Chiefs of Police (IACP) published a helpful resource (*IACP Technology Policy Framework*) for law enforcement executives in January 2014 that should be consulted to assist agencies with policy development. This includes promotion of social media research policies that explain how and when social media can be used to support criminal investigations.

More generally, we encourage policy makers and law enforcement executives to think about 21st Century technology in policing from a broader perspective than simply developing one-off policies for different types of technology. The core of the issue is how law enforcement should handle *data* in terms of collection, analysis, and sharing. We suggest that universal principles should regulate law enforcement's use of data. Specifically, policies should specify **access restrictions** to certain technologies and data, **mandatory audits** of technology use and data access, and **reporting of metrics** that indicate the value of the technology or data in supporting policing outcomes.

Technology advancements help law enforcement to more efficiently generate high-quality investigative leads and gather evidence. While we must be able to take advantage of the latest innovations to support our mission, we must do more to proactively communicate with policy makers, political leadership, and our communities about how we use technology to create better understanding of its effectiveness.

Conclusion

The issues we addressed above represent just a few of the many considerations that ASCIA members believe are important to advance policing in the 21st Century. As criminal investigators, our people are extremely good at tackling tough and often emotionally disturbing challenges in the aftermath of a crime. But preventing crime in the first place is always preferable. Effective evidence-based prevention and intervention programming such as the Gang Resistance Education and Training (GREAT) program and Community Anti-Drug Coalitions should be supported with substantial investment by all levels of government in collaboration with the private sector. Doing more across all communities to encourage respect for follow human beings and the rule of law is essential.

The efforts of local police to effectively engage the community to develop trust and respect for the role of law enforcement in preventing crime will always be a fundamental element of crime control. Without basic policies that support the historic notion that the police are nothing more than members of the community with responsibility to maintain community safety and order, we will never be successful in engendering the trust and cooperation of community members in general. That partnership is essential as the police innovate strategies designed to continue the significant reduction of crime that we have experienced across the country.

Through clear and consistent policies that ensure an independent and fair process to investigate officer involved shootings, to "connect the dots" through greater use of criminal intelligence and information sharing, and to take advantage of cutting-edge investigative technologies, ASCIA members believe that we will get even better at investigating crimes in the 21st Century while maintaining high levels of trust with the communities we serve.