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

---

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

September 8, 2016

Good Morning Chairman King and Members of the Subcommittee:

Thank you for inviting me to testify today on state and local perspectives on federal information sharing. I am currently the chief of police for the University of Central Florida, the largest university in the state. I am also the immediate past president of the International Association of Chiefs of Police (IACP).

On February 26, 2015, I sat before members of this subcommittee and testified on this very same topic. I would like to thank this committee and subcommittee for reconvening a hearing on this very important issue and for the support it has demonstrated over the years for the law enforcement field and our communities.

Over a year ago, I spoke about issues such as "going dark," the integral role of the National Network of Fusion Centers, and how things had advanced since 9/11. While there is no doubt that our fusion centers remain absolutely essential, and law enforcement still faces great challenges, even with the legal authority, to gaining access to electronic communications information pursuant to a court order, I would like to focus on a few other issues today. Those issues are terrorist attacks and information sharing around incidents like the Pulse nightclub shooting, cyber threats, and federal funding.

During my career, I have watched the threats to our communities evolve. While we are still dealing with the problems of violent crime, drugs, prostitution, smuggling/trafficking, and gangs, we now face additional challenges. Those challenges include violent extremism, terrorism, cyber threats, and highly organized criminals with access to specialized equipment to aid them in their mission to harm others and devastate our communities.

June 12, 2016. I will never forget this day. It was in the early hours of June 12 that Omar Mateen killed 49 people and wounded countless others inside Pulse nightclub in Orlando, Florida.

Members of my agency were first responders to this horrific scene, and our victim advocates assisted family members at three local hospitals. Now, three months later, we continue to provide counseling services to victims and their families as they work to restore some type of normalcy to their lives while the FBI and our Joint Terrorism Task Force continues the criminal investigation. This incident highlights how one heavily armed individual can inflict numerous casualties with weapons purchased legally here in the United States.

As law enforcement continues to deal with radicalized people and groups, there is growing concern about refugees from war-torn countries coming to our country. Thus far, we have not been informed how they will be vetted or where they will be located. Our need to know is not about targeting or tracking, but more in line with assistance during assimilation and protecting them from individuals with ill intent.

Another issues of significance is cyber threats. The cyber threat confronting the United States has never been greater. The cyber threat is real, and it is here and now.

It seems like we read or hear about cybercrime and cyber attacks against government agencies, businesses, and critical infrastructure every week in the media. However, cybersecurity is not just a national-level challenge—it affects state, local, tribal, and territorial law enforcement agencies every day. These agencies encounter issues ranging from cyber-enabled crime committed against local individuals and businesses, to forensic cyber investigations, to protecting against and responding to cybercrime, cyber attacks, and intrusions.

Police departments themselves have become the targets of ransomware attacks, which threatens our operations and the security of our information systems and data.

Nearly three-quarters of the 18,000 law enforcement agencies throughout the United States have fewer than 25 sworn officers; nearly half have fewer than 10 sworn officers. This means that many of our nation's law enforcement agencies do not have robust IT capabilities and protecting their systems from intrusions is a challenge.

Therefore, we cannot, and must not overlook the importance of fully engaging smaller agencies and agencies in non-urban areas in cybersecurity threat assessments as well as including them in cyber attack exercises and training. Fully engaging all law enforcement agencies in this increasingly growing threat is the only way we will be able to prepare for and prevent future attacks that threaten the security of our agencies and the United States.

I would also recommend that the FBI consider adding cybercrime reporting to the Uniform Crime Reporting system. My 39 years of government experience has shown me that something can only become a priority for action when we begin to officially count it.

This should come as no surprise to members of this subcommittee, but federal funding to support federal, state, local, and tribal agency efforts is essential. This includes federal funding to support fusion centers, crime analysis centers, Regional Information Sharing System (RISS) Centers, and High Intensity Drug Trafficking Areas (HIDTA). These have proven to be very effective platforms for integrating federal, state, local, and tribal law enforcement criminal information and intelligence, and they need to be maintained in order to insure the protection of the homeland. As these platforms continue to mature, their immense value in helping investigative agencies to "connect the dots" has been demonstrated. As part of this maturity process, de-confliction of both targets and events between these platforms is becoming an increasingly important area that needs attention and support from Congress moving forward.

On behalf of the IACP and our more than 27,000 members in 132 countries, thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.