

Mission Critical

HOW TO OVERCOME FOUR LAW ENFORCEMENT COMMUNICATION CHALLENGES

Do you share these communication challenges with other law enforcement agencies?

Traffic accidents, public gatherings, natural disasters—you're responsible for managing all of these events. Regardless of how different each call might be, getting the job done safely and effectively requires one thing every time: communication.

But communication involves more than ten-codes and radios. Effective communication also includes video, text, email, phone and geographical data. Plus, there are Internet of Things (IoT) technology and network considerations to account for.

With so many facets of communication riding on your decision, choosing the right solutions isn't just important—it's critical. But it doesn't have to be difficult. The keys to finding the right technology are straightforward: Identify your challenges, and then understand the available solutions. Knowing what communication challenges other departments are trying to solve can help you get started.

A recent survey conducted on behalf of the U.S. Department of Commerce asked your law enforcement peers to list their top challenges when choosing or using new communication technology. Take a look at their answers on the following pages to gut-check against your own department needs. Then learn which solutions can help you overcome each challenge so you can deliver your best response.

Challenge 1

WILL I BE ABLE TO GET THROUGH WHEN IT MATTERS MOST?

Even in non-crisis situations, events like festivals, concerts and football games generate significant public cellular data traffic, potentially affecting the reliability of law enforcement communication. If a crisis occurs at one of these events, your need to communicate becomes even more urgent—as massive amounts of data further slow public networks.

"As far as cell phones go, I can see a problem in bandwidth...we're working at a football game, while there's a concert going on right across the street...and then...everyone's texting. Everyone's calling. There's an obvious issue there."

Police Officer | Urban Area

SOLUTION:

Eliminate bandwidth challenges

To avoid potential communication slowdowns, Data Priority for First Responders is a wireless data solution that eliminates bandwidth issues by pushing your data to the front of the line, ahead of other traffic. When necessary, this solution also preempts public data, temporarily removing or reallocating it so your team or tactical unit can rely on the same quality of service no matter what.

Network crowding can also make voice communication difficult. Wireless Priority Service (WPS) queues your mission-critical calls first, so you can get through when it matters. Choosing an authorized provider of this government service will allow you to access its benefits.

For connectivity that goes where you do, mobile office solutions turn squad cars into communication hubs that connect critical devices with vehicle area networks (VANs). Mobile, secure Wi-Fi connectivity supports rugged laptops / tablets, cameras, sensors, bodycams, phones and more—inside and around the vehicle.

SOLUTION:

Choose the right network

Another factor that influences reliability is location. As one officer put it, "It's spotty sometimes. Different areas of town you lose reception, so then you lose communication."²

Choosing a provider that puts towers not only in urban areas, but also in the rural or remote areas where you may be called to respond, can help officers and entire teams stay connected. The network you choose can also power connectivity in mobile command centers that serve as communication hubs to aid interoperability.



Challenge 2:

CAN I COUNT ON MY EQUIPMENT TO HELP ME DO MY JOB?

Every piece of gear an officer carries is crucial. So it's important that every tool on your belt is in working order. And since each officer carries an average of 30 pounds of extra gear on them, every tool has to be utilized effectively so less gear gets added to the load. Digital field interviewing capabilities and 911 notifications are just a few examples of why today's law enforcement agencies consider wireless technology and devices like Smartphones to be essential. But they have to last, and they have to add value.

"One of the issues that we see is that the equipment that's being issued is not rugged enough. I mean, remember that as police officers we're out there in the sun—we're out there in the freezing cold, in the rain. They're getting in and out of their police units, so the equipment needs to be more rugged."

Police Officer | Rural Area

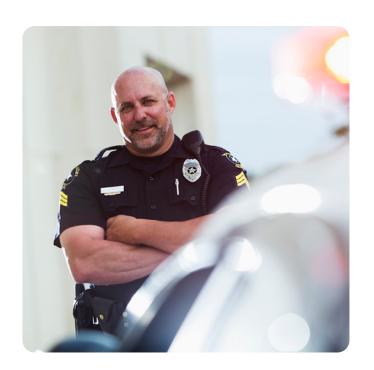
SOLUTION:

Get wireless devices built to last

Police work is notoriously hard on equipment, and there's no rule against bad weather or unexpected occurrences on duty. So regular equipment can't always do the job for law enforcement. Rugged laptops, tablets and smartphones make mobile data terminals (MDTs) resistant to spills, dust and impacts.

Similarly, rugged scanners, monitors, modems and routers are designed to withstand the extreme temperature fluctuations inside an off-duty patrol car, as well as the vibration of an on-duty vehicle.

Outside the squad car, rugged smartphones and tablets are designed to be used (and dropped) in rain, ice and snow. Their tougher components, screens and cases mean that you'll ultimately spend less on repair.



Challenge 3:

ARE MY DATA COMMUNICATIONS SECURE?

"My initial reaction was 'No way!" said a sheriff in Maine, when his system was frozen by ransomware. After 48 hours, he reluctantly paid the hackers who sent it. "We are cops. We generally don't pay ransoms." In another instance, a police chief in New Hampshire refused to pay, and his files were deleted." 4

Sheriff | Rural Area • Police Chief | Suburban Area

Stories like this are more common than you might think. In fact, the LAPD found itself victim to a data breach that exposed the names, dates of birth, e-mail addresses and passwords of thousands of officers and applicants.⁵ It's not just an inconvenience—officer and civilian safety could be at risk when data gets exposed. As more and more data is collected, and hackers find new ways to use stolen data, departments are at greater risk for cyber threats like these.

SOLUTION:

Safeguard data at rest

The equipment in your patrol cars and the smart devices your officers carry relies on your network to send and receive information. As sensitive information is transferred, a private network solution for public safety data ensures you're never connected to external networks that can leave your data vulnerable, keeping it safe from the threat of hackers who prey on unprotected networks and data.

In addition, private networks offer tiered levels of data priority depending on department needs, so that mission-critical data gets there safely—and with the speed you need.

SOLUTION:

Safeguard data during transfer

When you're connecting mission-critical devices in the field, private static IP services provide you with an extra layer of security to protect data as it goes to and from your network.



Challenge 4:

WILL NEW SOLUTIONS FEEL COMPLICATED?

No one likes technology that's difficult to use, or data plans that are impossible to figure out. But in law enforcement, where wasted seconds could negatively affect the outcome of your response, complicated communication technology and data plans are more than an inconvenience. And customer service that can't help you figure things out when you need it is unacceptable. There simply isn't time for self-help portals and retail locations manned by junior staff.

"In the police world, if you want somebody to use something, it has to be simple.

The more complicated it is, it's very seldom getting used."

Police Officer | Rural Area

SOLUTION:

Keep your support local

Public safety solutions can help you prepare for and respond to any situation with greater peace of mind and improved team communication. With the right support, you can customize a data plan and set of solutions that work best for your department's needs. Local representatives with experience in law enforcement solutions can provide the personalized support you need to keep your department moving forward. Reps who know you, your staff and your department can answer questions faster, offer better suggestions, and make your staff feel more comfortable.

SOLUTION:

Keep your data plan unlimited

During a crisis, there's no way to predict how much data you'll use—especially when devices like Tablets and routers will be using more data than you're used to, as you transfer video and other data. And you don't have time to manage overages. Keep it simple by choosing a customized first-responder plan that allows unlimited data usage for phones and all other devices.



Conclusion

PREPARE FOR THE FUTURE, STARTING NOW

From solutions that offer data and voice priority, to physical equipment like rugged devices, routers and Cell on Light Trucks (COLTs), there are many solutions available and many providers to consider. Considering the issues presented here will help you make informed decisions that put new wireless communication technologies into the hands of your officers—with less hassle and better results.

Building a strong base of communication solutions will also put your department in a better position to take advantage of 5G technology and the changes it brings. Surveillance videos are crystal-clear and delivered instantly. Facial recognition and behavioral analytics put officers a step ahead during developing situations. And sensors deliver instant information about weapon use and officer location, turn on streetlights where an incident is unfolding, and allow enhanced use of fingerprint scanners on-scene.

Working with a technology partner who can get you started and keep you going with a customized set of solutions that offer reliability, durability, security and ease of use is the key to keeping your officers and community safe and connected. Today and tomorrow.

Law enforcement agencies rely on UScellular's Critical Connectivity public safety solutions. From data priority and mobile office solutions to private networks and rugged devices, we offer what your officers need to be safer and more efficient in the field.

References

¹Choong, Yee-Yin, et al. "Voices of First Responders — Identifying Public Safety Communication Problems," Phase 1, Volume 1. NIST, 2018.

2 ibid

³ Dawkins, Shaneé, et al. "Voices of First Responders — Identifying Public Safety Communication Problems," Phase 1, Volume 2.1. NIST, 2018.

⁴ Francescani, Chris. "Ransomware Hackers Blackmail U.S. Police Departments." CNBC, 2016.

⁵ Doffman, Zak. "Cyberattack On LAPD Confirmed: Data Breach Impacts Thousands Of Officers." Forbes, 2019.

⁶ Choong et al., Phase 1, Volume 1

