A public safety communications checklist

6 questions agencies should ask a potential public safety partner

There's no perfect formula for finding the right public safety network partner, but here are 6 questions agencies should consider as they assess their options.

verizon

When disaster strikes, Americans rely on public safety officials and frontline workers to keep them out of harm's way. That sentiment has proven especially true over the past several months, as wildfires devastated the western United States and a deadly Hurricane Ida made its way up the East Coast.

However, this uptick in natural disasters has also exposed the fact that public safety agencies are strapped for resources. High employee turnover, low pay rates, a lack of supplies and a widely overlooked mental health epidemic across the first responder community has only made it more difficult to respond to disasters in a timely and effective manner.

To ease the burden, today's public safety agencies are turning to technology providers to provide secure data sharing capabilities and connected, reliable solutions that make it easier for responders to keep citizens safe.

There's no perfect formula for finding the right network partner. In fact, one organization's public safety needs may vastly differ from another. However, there are several factors agencies should consider as they approach the process. Here are a few questions they can ask potential network partners as they assess their options.

1. What level of coverage do you provide?

If there's one thing all public safety agencies need to achieve their mission, it's coverage.

"Whenever we talk to public safety agencies, it doesn't matter how advanced, secure or innovative the solutions are," says Nick Nilan, director of Verizon's federal civilian practice. "It doesn't matter if you don't have network coverage. It means nothing if the network's not there."

Of course, first responders and frontline workers rarely operate from a single location. Their job requires them to be constantly on the go. As a result, they need coverage that keeps up with their every move.

"In most cases, that means the macro-network coverage needs to exist wherever your operations occur," Nilan explains. "That means your phone, router, tablet, your [Internet of Things] sensors, your body-worn camera — all of the different technologies that our public safety agencies use — now work when they're expected to, and wherever their mission takes them."

> **“A battery backup at our towers allowed the network to continue to function and provide reliable, resilient coverage.”**
>
> **Nick Nilan,** director of Verizon’s federal civilian practice

2. Is your coverage reliable amid unforeseen circumstances?

Plenty of network providers can provide coverage on a good day. The real test is whether they can deliver that same level of reliability in the face of unforeseen circumstances.

“Most networks work well when skies are blue, but it’s important to make sure they also work well when we have bad weather,” Nilan says.

Take Hurricane Ida: When the major storm passed through Louisiana, Verizon’s services remained intact because it had a disaster recovery plan embedded in its technical operations.

“A battery backup at our towers allowed the network to continue to function and provide reliable, resilient coverage,” Nilan notes. “And it’s all supported by the virtualization and software-defined aspects of the network, which allow us to get back up and running when there are challenges.”

3. Do your solutions interoperate with other public safety systems and technologies?

During any large-scale mission, public safety agencies must communicate with other organizations to enable situational awareness and complete the mission effectively. For example, during a public safety emergency, law enforcement officers must communicate with emergency medical technicians and paramedics. Depending on the situation, they might also call in additional rescue teams. But often, these different public safety agencies and response teams leverage different network providers, so it’s critical to ensure a potential partner is committed to being fully interoperable with other carriers.

verizon

"Barriers and restrictive practices that limit real-time communication and collaboration between frontline workers must be removed. Regardless of carrier or device, all frontline workers must be able to communicate and share information seamlessly during times of crisis" says Bill Bratton, Former New York City Police Department (NYPD) commissioner and Los Angeles Police Department (LAPD) chief.

"At the end of the day, all of these agencies need to work together and ensure their citizens are safe," says Azhar Khan, managing client partner at Verizon. "But that's only possible when systems and technologies can seamlessly communicate with one another."

Khan adds if one of these agencies relies on a network provider that can't interoperate with the others, it can make or break the entire mission.

"If there's one service provider with a back-end infrastructure and overall supporting network layer services that do not support those feature functionalities, these responders are really going to be in a bind," he explains.

"Verizon, along with public safety organizations and partners, supports the critical goal of achieving comprehensive, cross-carrier interoperability, which includes providing all first responder communications with priority and preemption across networks," says Karen P. Tandy, Former administrator for the U.S. Drug Enforcement Administration.

4. How do you maintain the security of your network?

After a year of security breaches and ransomware attacks that wreaked havoc on public sector networks and operations, agencies can never be too careful when it comes to securing their infrastructure. Network providers must do their due diligence in mitigating threats and providing enhanced security measures to their customers.

"Data is everywhere," Nilan says. "For agencies and their partners, it's imperative to not only manage the deluge of data that's coming into public safety agencies and then making sure that the right individual gets the right data at the right time, but that all this happens in a secure and reliable manner."

Securing all the data public safety personnel access, manage and analyze daily is a challenge network providers and agencies must address together.

"You need to ensure your network partner is advanced enough in understanding the security of their own network so that they can then help the public safety agency secure their networks and their data, as well," Nilan says.

"Verizon, along with public safety organizations and partners, supports the critical goal of achieving comprehensive, cross-carrier interoperability, which includes providing all first responder communications with priority and preemption across networks."

Karen P. Tandy, former administrator for the U.S. Drug Enforcement Administration.

5. What's your vision for the future?

It's not simply enough to offer secure and reliable coverage that meets the needs of today. Concepts like IoT and 5G will become increasingly complex over the next decade — and network providers must be ready to embrace these transformations head on.

The right network partner will not only adapt to technology trends of the future, but help shape them.

"Don't be afraid to inquire about the future vision of the service provider," Khan advises. "How are they looking to change and evolve some of these trends in the public safety area? What type of standards and practices are they developing that will outline future solutions that can help solve crimes and reduce the challenges and problems of tomorrow?"

A proactive network partner tests and pilots its technologies today so they are ready for the future. "Your network operator and provider should have the capability to respond to unexpected system interruptions efficiently through pre-existing disaster recovery tools," Tandy says.

"A strong communications provider partner that can make a mission successful is one that trains with you," Nilan adds. "They test the technology that they're looking to deploy before they need to actually deploy it."

He would know: With the oversight of public safety partners and first responders, Nilan's team has tested more than 100 different technologies on the Verizon network. The goal? Ensure people, processes and technology are in place to mitigate disaster before it strikes.

Understanding public safety priorities and needs evolve, Verizon has also introduced a virtualized core built to augment and adjust network capabilities and performance to meet the ever-changing needs of public safety agencies.

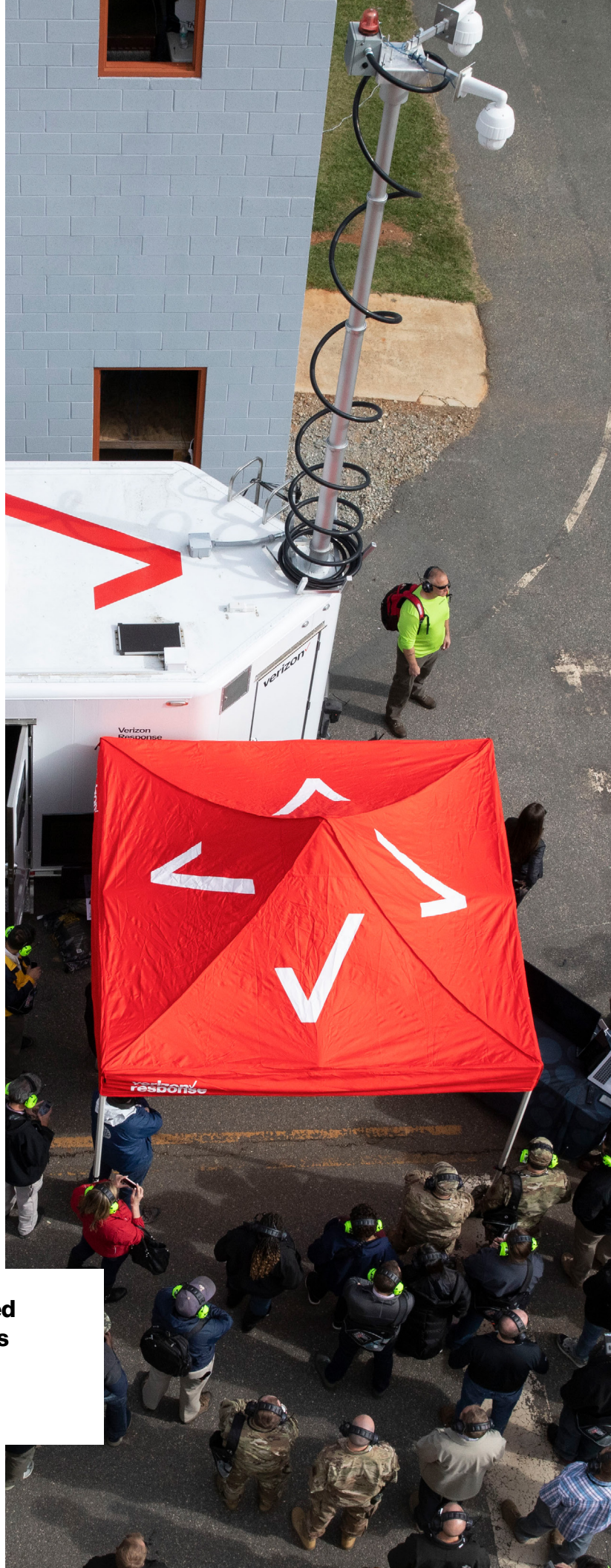
6. Are you committed to the cause?

It's not simply a knack for innovation that keeps Nilan and Khan engaged in their work — it's also a call to public service.

In fact, during a major emergency incident in December 2020, the Verizon response team handed out more than 400 phones to first responders because the competitor network they were using was down. That same year, the Verizon response team responded to the pandemic, wildfires, hurricanes and other emergencies, including 2,000+ customer engagements, 1,200+ solutions deployed and 6,000+ devices loaned to first responders.

"There's something special about industry supporting the mission of our public sector agencies," Nilan says. "They really put themselves in harm's way for all of us. The least we can do is make sure that they have the right technology, the right solutions and the right services to support their mission."

These types of high-stress response efforts can certainly make a mission partner's job challenging. But they can also prove incredibly rewarding. "Verizon has consistently delivered on customers' demand for reliable network connectivity and is committed to setting the industry standard for first responder communications," Tandy adds.



Find out how Verizon Frontline, the advanced network and technology for first responders and frontline workers, was built to help public safety agencies weather crises.

verizon