What FirstNet® Means to First Responders

The Future of Public Safety Networks in the United States

Overview

In an emergency situation, first responders are the first line of defense for safety and rescue missions. These events, be it a man-created or natural disaster, put first responders and the communities they serve in peril. After September 11, 2001, a weakness in the ability for first responders to communicate quickly during emergencies was identified. During the collapse of the World Trade Center, first responders were unable to radio each other to collaborate in order to evacuate people from the buildings. Consequently, the public safety community set out to find a way to improve interoperability for better communication and to ultimately save lives.

In 2012, Congress established the First Responder Network Authority to create a nationwide broadband network dedicated to public safety. To give first responders dedicated bandwidth when they need it for the communication tools they use, the First Responder Network Authority issued an RFP in January 2016 to create a public-private partnership to bring FirstNet, a dedicated communications ecosystem, to life.

In 2017, AT&T won the contract to build, operate, and maintain this nationwide network platform, FirstNet, which is dedicated to the public safety community. The FirstNet core is highly secure, reducing the risk of complications that come with a multi-core architecture, for example, operational complexity, security complexity, and increased latency.

In addition, FirstNet has spectrum licensed specifically for use on its core network, giving first responders their own communication frequencies when needed. What's more, FirstNet provides priority on the network and enables interoperability between agencies. Band 14 represents 20 MHz of spectrum in the 700 MHz band, which offers sufficient propagation in urban and rural areas and penetration into buildings.

To address the demands of first responders, FirstNet is turning to public safety communities to better understand what they need to communicate efficiently using 21st-century tools, taking a "for public safety, by public safety" approach.

First responders depend on a reliable network connection from the minute their shift begins to the time they hang up their jackets. FirstNet allows first responders to respond faster, whether on a Computer Aided Dispatch (CAD) system or laptop receiving immediate details about the situation they are about to confront.

Benefits of FirstNet
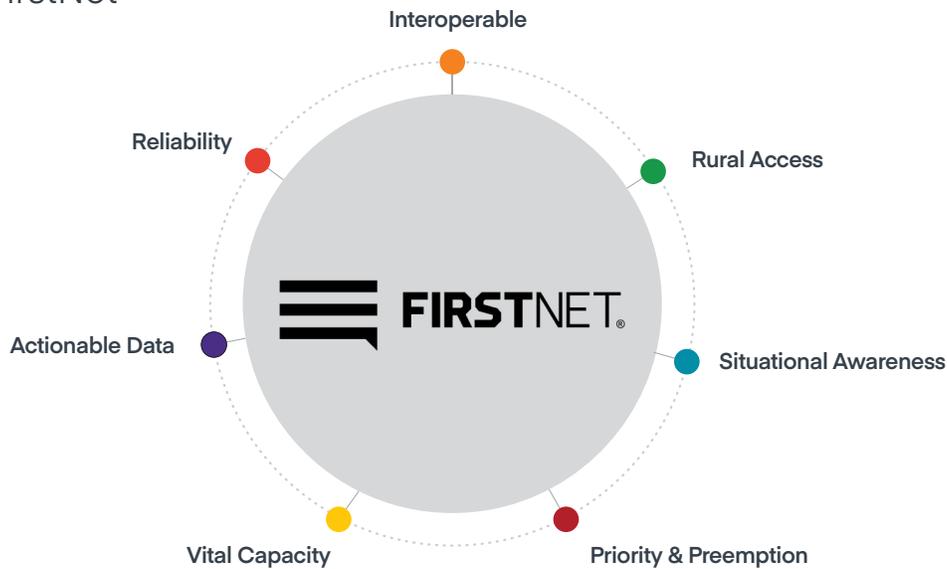
FirstNet gives first responders the highly secure connection they need for critical communications and the latest technology as it evolves. Immediate information delivery enhances the capabilities of the public safety community, so first responders can save lives, while protecting their own.

● **Interoperability** on a single, nationwide, LTE network dedicated to public safety communications.

● **Expanded rural access** for the capacity and connections you need — when you need it.

● **Situational awareness** to support the public safety community with critical information needed to operate efficiently and safely.

● **Priority and preemption** capabilities mean first responders connect first — and that they have the bandwidth they need by detouring others off the network as needed.

● **Vital capacity** for instances when it's difficult to get the crucial robust network capacity needed, such as at concerts, festivals, and sporting events.

● **Actionable data** for applications, devices, and services designed to enhance public safety efficiency.

● **Reliable and highly secure communication** no matter where the first responder might be in the field, before, during, and after a disaster.

The Public Safety Landscape

When major events occur, lack of communication puts the lives of community members and public safety officers in danger. First responders need a reliable network and interoperability to effectively communicate with other public safety organizations and agencies. FirstNet will allow public safety entities to better coordinate when jointly responding to human-caused or natural disasters.

The FirstNet core was built to support Primary Users, including:

— Law enforcement

— Fire departments

— Emergency medical services personnel

FirstNet also provides services for those who support first responders, including such entities as:

— Utilities	— Hospitals	— Humanitarian organizations
— Public works	— Transportation	— Federal Response organizations
— Search & rescue	— Schools	

These Extended Primary Users are individuals or organizations who may be called upon to support public safety personnel with mitigation, remediation, overhaul, clean-up, restoration, and other services that are required during or after emergencies or incidents.
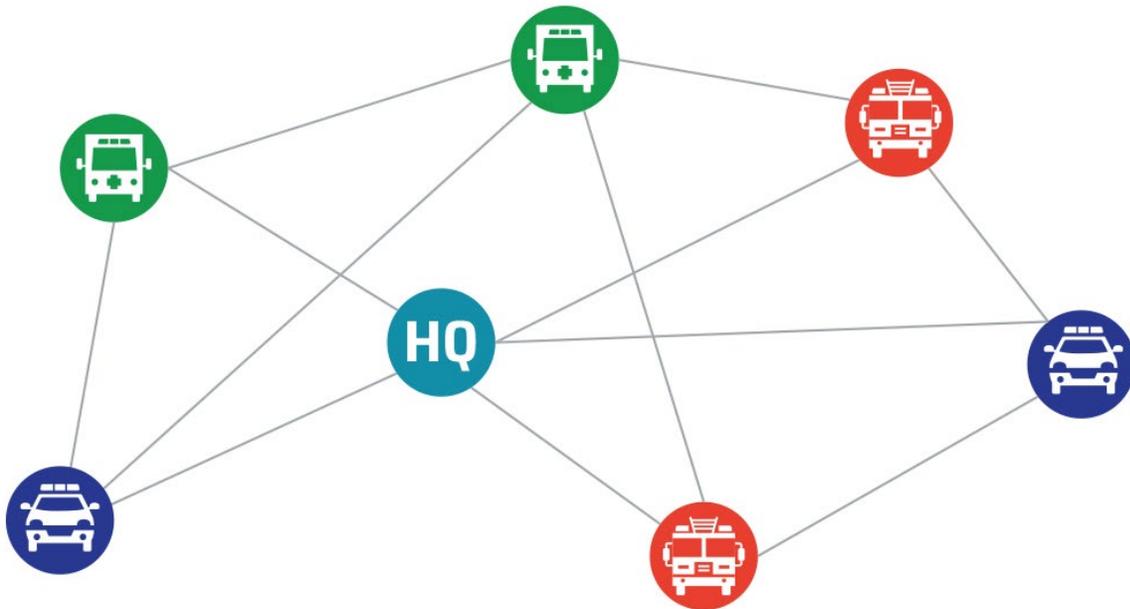
THE TOP 10

most populated cities in the U.S. trust Cradlepoint.

40%

Stress and overexertion cause over 40 percent of firefighter fatalities from 1990 to today.[2]

FirstNet offers the ability to transmit firefighters' near real-time vital signs over the network, helping to identify potential risks and save lives.

2 Source https://www.usfa.fema.gov/downloads/pdf/publications/ff_fat16.pdf

LTE & FirstNet

LTE is the evolution of cellular technology, which is now in its fourth generation. Each generation of LTE brings improvement in speed and functionality. The First Responder Network Authority broadly defines the FirstNet LTE network into distinct layers: Core Network, Transport Backhaul, Radio Access Network (RAN), and Public Safety Devices.

The First Responder Network Authority and AT&T work closely with 3GPP, the organization that sets the LTE standards, for maximum interoperability with current and future cellular technology. Public safety organizations are also central contributors to the specifications of the FirstNet core. Much of the focus is on setting international standards that will allow FirstNet to deliver mission-critical voice to network users. These same technologies are intended to work across the platforms of all standards-based equipment and networks, not just in the U.S., but worldwide.

The FirstNet Core

The FirstNet core is an enhanced packet core network and is key to agency interoperability on a nationwide platform. The core serves as the communication platform with other public sector organizations. Examples of these organizations include 911, local, state, FEMA, and federal networks.

There are six primary functions of the FirstNet core:

— Switching data

— Processing & reformatting data

— Storing & maintaining data

— Applications

— Services

— Operational & business support

Devices, Applications & Solutions for FirstNet

Devices on FirstNet connect to all the user access points that send and receive data over the network. These devices — such as smartphones, MDTs/MDCs, tablets, routers, and specialty devices — have been and continue to be developed and certified for use on FirstNet. Wireless LTE routers are key connection points for systems and applications ensuring that the data is transmitted efferently and securely.

FirstNet is committed to transforming public safety operations through innovations such as video surveillance with body-worn cameras, image recognition, drones, CAD and integrated CAD solution, and GIS mapping, to name a few.

FirstNet has already developed an app eco-system program to enable developers to build innovative apps that improve the performance of first responders.

With the ability to transmit firefighters' near real-time vital signs, FirstNet could help greatly improve lifesaving interventions and risk identification.

Tech Tools for Emergencies Today

Video Surveillance	Tablets & MDTs	GPS	Analytics	License Plate Readers
Body Cameras	Wearables	Sensors	WiFi	Drones

The Value of MiMo Antennas

Today's first responders require the best, most up-to-date technology as well as the ability to connect to a wireless network — whenever the need arises. Whether in the office or the field, first responders must perform daily duties, from pulling up files on a laptop to accessing GPS location information. These actions require having access to devices such as smart phones, tablets, or dashboard cameras, all of which require reliable network access.

For the best LTE connection with FirstNet, first responders are turning to MiMo antennas. With the bandwidth requirements of video, audio, and data systems, MiMo is often the best solution for communication, especially in urban environments where clear line-of-sight is harder to achieve. MiMo communication sends the same amount of data as several signals through multiple antennas, while still utilizing a single radio channel. This antenna diversity improves signal quality and strength. Overall throughput can be improved, allowing for greater quality and quantity of data to be sent over the network and the impact from issues such as fading, caused by lost connectivity, can be reduced.

First responders operating in chaotic or changing situations can depend on antenna diversity to help compensate for disruptions when natural disasters, power outages, overloaded networks, or other issues occur and to remain operational. Law enforcement or military users can benefit from MiMo antennas to operate their own separate communication networks on dedicated radio bands, including team-to-team communication between small groups, as well as larger networks that include ground vehicles.

The Days of USB Modems are Dwindling

The days of manually plugging memory cards into computers are quickly fading, and similarly, plugging in USB modems will follow the same fate. While a USB modem is a quick, affordable, and portable solution, the cellular connection is not reliable, nor is it designed to work inside harsh transportation environments, such as in police or paramedic vehicles, where a more rugged solution is necessary. USB modems aren't designed to withstand extreme temperatures or dust and water, and they can easily break from road vibrations and normal wear and tear. Furthermore, USB modems are at a disadvantage due to their lack of external antennas, which can impede optimal performance.

Other drawbacks to using USB modems include lack of cloud management capabilities and no capabilities for wireless-to-wireless failover or access to multiple carriers. The lack of cloud management also means that deploying firmware patches, updates, and configuring changes to the fleet is a manual process, making USB modems difficult and time intensive to manage and maintain.

Security also becomes a risk when using USB modems. Consumer-grade USB modems have basic security features — though many applications today require enterprise-grade security — and most are not built for handling sensitive data and are vulnerable to breaches.

The Value of Cloud Mangement & Applications

With advancements in cloud management, first responder IT organizations can manage far-flung mobile networks — and the users, devices, and applications that depend on them — from a central location so everyone and everything stays connected and protected.

The simplicity, orchestration, and automation aspects of modern cloud management systems enable IT administrators to deploy branch, mobile, and IoT networks quickly and manage more endpoints with fewer people. By making use of efficient, wireless protocols designed for cellular networks, cloud management enables administrators to configure, deploy, monitor, and manage mobile networks without running up cellular bills, and integrate remote troubleshooting capabilities to reduce truck rolls or the need to take vehicles off the road.

Complete Security for Vital Operations

Protecting mission-critical applications, collaboration strategies, and connected technologies across an ever-expanding network attack surface is as essential for IT organizations within public safety agencies as it is for enterprises. A modern mobile network solution needs to provide comprehensive edge security capabilities that protect local users, devices, cloud communications, and the WAN with access control, FIPS-certified data encryption, IoT device isolation, and Internet threat management.

5 **Source** CJIS Security Policy (08/16/2018) Appendix G.3 (pg. G-16)

6 **Source** https://aws.amazon.com/compliance/ services-in-scope/

7 **Source** CJIS Security Policy (08/16/2018) Section 5.10.1.5

8 **Source** CJIS Security Policy (08/16/2018), Appendix A, Page A-4, Par. 4

Software-Defined Perimeter (SD-P)

As the number of connected devices that first responders utilize continues to increase, so does the risk of a dangerous security breach. Software-Defined Perimeter (SD-P) is a new Software-Defined Network technology designed for securing IoT devices and device-to-cloud communications. It provides a perimeter-secured Internet overlay that encrypts and isolates IoT data from the rest of the mobile network.

As a cloud-delivered service, SD-P makes it simple to deploy and manage a secure overlay network that connects mobile users and IoT devices directly to the resources they need, reducing the time to connect and man-power to manage. Each overlay has its own private IP address space, so it remains hidden from the rest of the Internet — and potential hackers. These invitation-only networks offer fine-grain control with firewalling and filtering to regulate communications going in and out.

Benefits of Cradlepoint Solutions for First Responders

Cradlepoint COR IBR900 Series for use in Cradlepoint routers through Cradlepoint NetCloud Packages

Cradlepoint is providing a link between first responder agencies and FirstNet. The dedicated network platform allows public safety to get the job done — unthrottled, no matter where they are in the United States.

Only CJIS Mobile Solution of First Responders

Cradlepoint's Secure Threat Management comprehensive intrusion detection systems (IDS) and intrusion prevention systems (IPS) defend against evasion attacks, improve network availability, and protect sensitive data powered by Trend Micro's industry leading Deep Packet Inspection (DPI) engine. Cradlepoint goes a step further, offering the unified threat management system for mobile devices, so first responders remain CJIS compliant at headquarters and in the field.

The Criminal Justice Information Services (CJIS) Security Policy measures IPS and IDS as:

- Monitoring inbound and outbound communications for unusual or unauthorized activities

- Sending individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort

- Employing automated tools to support near real time analysis of events in support of detecting system level attacks

Federal Information Processing Standard (FIPS)

CJIS also recommends that agencies use Federal Information Processing Standards (FIPS) 140-2 certified devices. Cradlepoint NetCloud Service, a remote administrative management tool, received FIPS 140-2 Inside security validation from the U.S. federal government's National Institute of Standards and Practices (NIST).

Cradlepoint's FirstNet Ready™ LTE routers also include the unified edge security suite and FIPS 140-2 Inside.

Trusted Reliability

Cradlepoint customizes all modem software to get better performance with a more resilient WAN connection detecting outages, hung modems, and dropped packets — and switching between diverse WAN link sources faster. With Cradlepoint, first responders can quickly switch between fallback carriers, WiFi WAN sources, wired links, and even satellite connections so networks are always connected and protected.

Ease of Network Management

With Cradlepoint solutions, lean IT teams have the ability to easily deploy hundreds or thousands of devices, manage updates, perform maintenance, and easily analyze operational and network data. This also means an MDT in a vehicle works just as a PC would in an office. The IT team can extend domain security to the vehicle and troubleshoot device problems without taking the car off the road.

100%

of the top 10 U.S. cities trust Cradlepoint.

(Per Cradlepoint collected data.)

Vehicle & Device Visiblity

Cradlepoint combines the most resilient cellular WAN with best-of-breed Automated Vehicle Locator (AVL) providers, which offers dead reckoning to help never lose sight of assets, even when they enter areas with no GPS signal and poor cellular reception.

Cradlepoint specializes in keeping fixed offices and command centers up when a wired connection goes down. Furthermore, with Cradlepoint's unique Out-of-Band Management, first responders can quickly access other systems to get complete visibility of an otherwise unreachable systems or device, including recorded video camera footage.

Ruggedness

First responders cannot afford to second-guess whether their equipment will stand up in poor conditions. Cradlepoint routers use field-proven specifications for shock, vibration, humidity, and temperature protection to ensure mission-critical connectivity in the most challenging environments. Cradlepoint mobile routers also meet MIL-STD 810G / SAEJ1455 / IP54 standards.

Customized Applications

First responder agencies face different types of crises and emergencies and often rely on customized applications to get their jobs done safely and quickly. Cradlepoint has very flexible SDK and GPIO interfaces to allow agencies to create all kinds of applications such as light bars, shotgun holster sensors, ready-vehicle battery health, and smartphones to unlock vehicle doors in dangerous areas.

All-Inclusive LTE Tracking & Management

During an emergency, first responders rely on anywhere from 7-10 applications and devices that all run in or around their vehicle. With Cradlepoint, all networked communications systems and applications can run on one highly reliable platform. A literal communications hub is created with devices and applications like MDTs, dash cameras, DVRs, satellite connections, ODB-II adapters, license plate readers, and body cameras — all working to deliver first responders and command centers with real-time information.

United States-Based Company

For many government agencies, vendor source is important. Cradlepoint is a United States company headquartered in Boise, Idaho, with a United States-based support organization. Included in each solution, Cradlepoint support consists of comprehensive 24x7 online, chat, and native English-speaking phone assistance.

Cradlepoint has public safety & first responder deployments in every U.S. state, including 25 of the largest cities.

According to Cradlepoint data

Six Considerations to Get on the Road to FirstNet:

1 **Who are the Primary Users and Extended Primary Users?**

Primary Users are public safety entities that act as first responders and are the first to arrive at an emergency scene. Extended Primary Users provide public safety services in support of Primary Users. Contact your FirstNet Specialist to find out if your agency is eligible.

2 **Have we talked to our FirstNet Specialist to consider our FirstNet options for our agency?**

3 **What are our critical applications and what do we need to consider to ensure they are supported in this transition?**

There will be mission-critical applications available specifically for agencies through on FirstNet. As the network advances, more of those applications will be available over time.

4 **Have we established an in-vehicle network yet?**

5 **What are we doing for our in-building FirstNet coverage, such as network failover, Out-of-Band Management, and cellular WiFi access points?**

6 **Have we established a rapidly deployable temporary network?**

If the building network should become unstable, a temporary pop-up network, such as a command center pop-up networks, event pop-up networks, will be needed in case of an evacuation and other planned or unplanned events.

Learn more at cradlepoint.com/first-responders

Additional Sources

firstnet.gov, firstnet.com, cradlepoint.com

FirstNet and FirstNet Ready are registered trademarks and service marks of the First Responder Network Authority, an independent authority within the U.S. Department of Commerce.

About Cradlepoint

Cradlepoint is the global leader in cloud-delivered wireless edge solutions for branch, mobile, and IoT networks. The Cradlepoint Elastic Edge™ vision — powered by NetCloud services — provides a blueprint for agile, pervasive, and software-driven wireless WANs that leverage LTE and 5G services to connect people, places, and things everywhere with resiliency, security, and control.

More than 27,000 enterprise and government organizations around the world, including 75 percent of the world's top retailers, 50 percent of the Fortune 100, and first responders in 10 of the largest U.S. cities, rely on Cradlepoint to keep critical branches, points of commerce, field forces, vehicles, and IoT devices always connected and protected. Major service providers use Cradlepoint wireless solutions as the foundation for innovative managed network services. Founded in 2006, Cradlepoint is a privately held company headquartered in Boise, Idaho, with a development center in Silicon Valley and international offices in the UK and Australia.