FirstNet Operations Manual

February 2026

FirstNet® Authority

During a simulated rescue, Virginia Communications Cache teams placed FirstNet Wi-Fi hotspots at the mouth of a cave and ran fiber reels over 1,000 feet inside, bringing wireless capabilities for computers and cellphones. The teams used push-to-talk apps on FirstNet to communicate via radio channels and streamed video back to the local communications center.

FirstNet® Authority

The FirstNet Authority was established in light of 9/11 to lead the creation of a dedicated nationwide broadband network using spectrum set aside for the public safety community (Band 14). Through a combination of government, commercial, and public safety partnerships, we are committed to delivering a network and supporting an ecosystem of apps, devices, and capabilities that are innovative, reliable, accessible, and secure. By modernizing public safety communications with our partners, we can help responders keep America safe — every day and in every emergency.

To learn more, visit **FirstNet.gov**.

ABOUT THE FIRSTNET OPERATIONS MANUAL

The FirstNet Operations Manual is intended to be a reference for public safety officials and their partners to use the products, services, and capabilities of the Nationwide Public Safety Broadband Network (NPSBN) known as FirstNet.

FirstNet service is provided by AT&T under a 25-year contract with the First Responder Network Authority (FirstNet Authority), an independent authority of the federal government. The FirstNet Authority's mission, as mandated by Congress, is to ensure the building, deployment, and operation of the NPSBN. For more information on the FirstNet Authority, see **FirstNet.gov**. For more information on AT&T's delivery of FirstNet services, see **FirstNet.com**.

An increasing number of emergency management agencies (EMAs), law enforcement, fire service, emergency medical services (EMS), emergency communications, and other partners in public safety are using FirstNet. This manual is designed to provide these public safety officials with an overview of relevant FirstNet features and functions that officials use in their daily and emergency response roles. Many of the topics covered in this guide are applicable for coordinating response in the field, in an Emergency Operations Center (EOC), or an Emergency Communications Center (ECC) (e.g., 9-1-1 center, public safety answering point [PSAP]) location.

Where practical, the manual includes reference links and suggestions for users to obtain additional information on a topic. FirstNet users can also find help with their FirstNet accounts and features on **FirstNet.com**, through the **FirstNet Central portal**, by contacting their AT&T FirstNet Solution Consultant, or by calling the FirstNet Customer Care line at 1-800-574-7000.

FirstNet Authority public safety advisors are assigned to every U.S. state and territory; their contact information is available at **FirstNet.gov/advisor**.

For more information about FirstNet, visit FirstNet.gov.

TABLE OF CONTENTS

FIRSTNET BASICS

SECTION **1**

The Baltimore City Sheriff's Office switched to FirstNet after an underground fire cut power and disabled radio communications. Today, deputies rely on their FirstNet devices for field reporting, prisoner transports, and daily operations.

INTRODUCTION TO FIRSTNET

What is FirstNet?

FirstNet is a nationwide, secure, and reliable broadband wireless network that offers priority and preemption for public safety users. It was specifically designed for America's first responders and the public safety community. The Middle-Class Tax Relief and Job Creation Act of 2012 created the First Responder Network Authority (FirstNet Authority), an independent agency within the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA). The FirstNet Authority's mission, as mandated by Congress, is "to take all actions necessary to ensure the building, deployment, and operations of the Nationwide Public Safety Broadband Network (NPSBN)," also known as FirstNet. The legislation creating FirstNet also allocated $7 billion and 20 megahertz (MHz) of spectrum, known as Band 14, to the FirstNet Authority to ensure a dedicated nationwide network is built to meet the needs of public safety. In March 2017, after an open, competitive procurement for an industry partner to deploy the network, the FirstNet Authority awarded an innovative 25-year contract to AT&T to build, operate, and maintain the network.

Today, FirstNet is the largest wireless broadband network in the nation built for first responders. It is available in all 50 states, 5 territories, and the District of Columbia, as well as Tribal lands. FirstNet offers a single, nationwide network architecture that evolves with technological advances and consists of a physically separate evolved packet core (EPC) and radio access networks (RANs). For public safety officials, incident coordinators, and their partners in emergency response, the FirstNet network provides secure, prioritized communications before, during, and after incidents, whether they are daily operations, routine responses, major disasters, or pre-planned events and exercises.

The NPSBN is layered over the entire AT&T commercial domestic network. The initial buildout of Band 14 was launched in 2018 and completed in 2023. The FirstNet Authority makes significant investments to strengthen and improve FirstNet throughout the life of the contract. These strategic investments will enhance and evolve the network so public safety stays at the forefront of innovative, lifesaving technologies.

In February 2024, the FirstNet Authority announced a ten-year, $8.3 billion investment initiative under which FirstNet Authority will invest up to $6.3 billion for network evolution, delivering full 5G capabilities on FirstNet, expanded mission-critical services, and enhanced coverage. The FirstNet Authority anticipates an additional $2 billion for ongoing investments dedicated to coverage enhancements for public safety.

Overseeing the Nationwide Network

FirstNet is built through an **innovative 25-year contract** with AT&T. The FirstNet Authority is focused on ensuring that AT&T delivers on the terms of its contract to create a network designed for public safety. This function is unique to FirstNet; no other carrier gives public safety the same level of assurances and government oversight.

First Responder Network Authority

The FirstNet Authority's mission, as mandated by Congress, is to oversee the buildout, deployment, and operation of the nationwide public safety broadband network called FirstNet, making sure it delivers what public safety needs from a network. We work hand-in hand with public safety to ensure their voice is represented in the building and evolution of the FirstNet network.

The FirstNet Authority's responsibilities include:

- Nationwide Band 14 spectrum license management
- Public safety advocacy and engagement
- Contract validation and verification
- Standards development
- Boulder FirstNet Lab operations and management
- Investment management
- International collaboration
- Congressional reporting

AT&T

Under the 25-year contract, AT&T must build, operate, maintain, and enhance the network while achieving public safety user adoption targets and maintaining a minimum number of devices connected to the network. The contract also guarantees the FirstNet Authority's continued financial sustainability over the life of the contract through annual payments from AT&T to the FirstNet Authority, making the FirstNet Authority self-sustaining.

The unique requirements of this contract provide incentives for the network contractor to continue to grow and strengthen the network over the life of the contract. It also holds the

FirstNet Key Differentiators

Quality of service, priority, and preemption

FirstNet provides quality of service, priority, and preemption for voice and data communications, giving public safety's calls, texts, and data the "lights and sirens" treatment to be first on the network.

Band 14

FirstNet operates over 20 MHz of dedicated spectrum for public safety.

Dedicated core

FirstNet uses a separate core built for public safety communications traffic and security.

Tailored coverage plans

FirstNet has network buildout plans coordinated with — and approved by — every state and territory.

On-demand coverage

FirstNet provides public safety subscribers with on-demand mobile coverage assets and support at no additional cost.

Federal oversight

The FirstNet contract is overseen by a federal agency established to ensure the building, deployment, operation, and maintenance of the network, requiring accountability from the network provider. That federal agency, the FirstNet Authority, has additional Government oversight to ensure accountability to the American people.

Standards-based network

FirstNet incorporates global standards developed with public safety representation.

Local control

FirstNet offers public safety agencies local control and access to network status information.

Public safety's voice

The FirstNet Authority constantly engages with public safety stakeholders to inform network investment, expansion, and innovation.

network contractor accountable by instituting penalties and corrective actions when contract requirements are not met. This arrangement ensures the FirstNet network meets the rigorous communication needs of our nation's first responders and continues to evolve to meet their changing requirements. As part of this agreement, AT&T gained access to 20 MHz of federally owned spectrum licensed to the FirstNet Authority and $6.5 billion in initial funding, and it will invest about $40 billion over the life of the contract in the network.

AT&T is responsible for:

- Nationwide dedicated, physically separate evolved packet core
- Band 14 Radio Access Network
- Adoption and customer care
- Response Operations Group (ROG)
- Security operations center
- Mission-critical services
- Device and application ecosystems

Built for Public Safety

As public safety responds to more complex events, responders need an interoperable communications platform that can adapt during the life cycle of an emergency. FirstNet is more than an always-on network; it encompasses a suite of technological platforms, applications (apps), and functionalities specifically designed for public safety.

Importantly, the functions and features offered by FirstNet can be used for local mutual aid as well as when responders are deployed to another part of the country through an Emergency Management Assistance Compact (EMAC) mission. This section details how public safety agencies can use the FirstNet network to meet the needs of their responders.

Nationwide Available Network

First responders need to be able to communicate and coordinate with those on scene and those away from the action. FirstNet's **priority and preemption** features ensure responders' communications reach their partners in the field as well as those in the the Emergency Communications Center (ECC) or Emergency Operations Center (EOC). Priority means public safety devices gain access to the network first – public safety is at the front of the line. Preemption means public safety devices are treated as the most important on the network – network resources cannot be taken from public safety.

Push-to-talk apps enable responders to communicate with each other, including non-traditional mutual aid partners that may not share the same radio frequencies, in order to safely and effectively manage an incident. This communications traffic can be monitored and managed by the ECC or EOC command and control officials as the incident response expands.

These capabilities apply not only at the local or regional level, but during national response as well. EMAC has become the cornerstone of the national mutual aid system, and responders from a non-impacted state can quickly find themselves deployed to another state hard-hit by a disaster. In response to a major hurricane or wildfire, for example,

Types of Eligible FirstNet Users

Primary vs. Extended Primary

Primary users are public safety entities that serve as first responders — the agencies and people that are involved in the initial stages of emergency response operations. This includes law enforcement, fire protection services, emergency medical services, emergency communications centers, and emergency management.

Extended Primary users are those agencies, organizations, and companies — both non-profit and for-profit — that provide public safety services in support of Primary users.

Agency Paid vs. Subscriber Paid

Agency-Paid FirstNet users are employees and contractors of a Primary public safety entity, where the employer pays for the FirstNet service on behalf of their users.

FirstNet is also available for individuals to purchase on their own through the **Subscriber-Paid** program, where users are either verified employees or volunteers of a Primary public safety entity, or certain employees of an eligible Extended Primary entity.

Elbert County is a fast-growing, rural community in Colorado. Public safety agencies like Elizabeth Fire Rescue rely on FirstNet to keep responders connected across the county's 1,800 square miles.

responders may deploy to a challenging environment in an entirely different part of the country.

The key to any field response is communicating with other responders and with command-and-control centers away from the front lines. Because FirstNet is a nationwide network, public safety response teams can count on being able to use their FirstNet mobile devices, such as phones, tablets, hotspots, and Internet of Things (IoT) devices, to communicate and share situational awareness — regardless of what state they are operating in. They can access databases and reference materials and share planning documents. Real-time location data, sensor data, and video can be shared with responders and EOCs and ECCs to keep everyone informed and working from the same common operating picture.

Mission Critical for Public Safety

Public safety agencies can use FirstNet to send voice, text, and data communications through a network with priority and preemption of public communications. These are the core features of the network. However, FirstNet also includes many mission critical applications that are foundational to public safety's daily operations, including Mission Critical Push-to-Talk (MCPTT), Mission Critical Data (MCData), and Mission Critical Video (MCVideo). FirstNet's mission critical broadband communications can supplement an existing Land Mobile Radio (LMR) system and help to fill indoor and outdoor coverage gaps, creating more robust communications for public safety users (See: **Section 5: Mission Critical Services**).

Deployable Assets

When FirstNet users are forced to operate in remote or challenging environments where communication networks are strained or damaged, they can request and use (at no additional cost) temporary deployable communications assets. Depending on mission requirements, these assets include Cells on Wheels (COWs) Satellite Cell on Light Trucks (SatCOLTs), Compact Rapid Deployables (CRDs), and aerial assets such as Flying Cells On Wings (Flying COWs). Additionally, indoor solutions can be deployed to assist users in EOC, Command, or ECC settings. These FirstNet assets can help recover communications in disaster areas and supplement the normal terrestrial network during major events, such as large sporting events, concerts, parades, and other situations where many people are trying to access wireless networks at the same time.

FirstNet deployables can mean the difference between sending responders into an area with limited or very poor communications and enabling responders to transmit voice and data communications from the field to the EOC or ECC. Only FirstNet users can access the deployable assets, meaning that responders are not competing for bandwidth with the general public.

For more information and best practices on the FirstNet deployable fleet, see **Section 2: FirstNet Deployables Fleet and Local Solutions**.

Customer-Owned / Agency-Owned and Managed Assets

In addition to utilizing the FirstNet deployable fleet, many agencies have acquired their own communications equipment, such as CRDs and miniCRDs, Rapid Deployable Kits (RDKs), Mobile Broadband Kits (MBKs), and satellite-enabled systems. These customer-owned-and-managed platforms can allow for quick, nimble deployment of FirstNet in the critical minutes and hours after an event or incident begins. Agencies can extend the FirstNet network to remote, damaged, or even congested areas and provide secure field-to-command post communication, at their own direction and on their own timeline.

Agencies can establish deployable kits that can be pre-staged for events or at incident command post locations. Devices that are as small as a backpack or large suitcase can be transported by person, ATV, snowmobile, boat, or helicopter into remote areas or high terrain to provide responders with a temporary signal during search-and-rescue and other operations. For EOCs and command posts, there are solutions for improving service inside a building, whether it is a permanent EOC or a temporary command post or staging area location. Finally, there are satellite communications solutions that enable both voice and data to be sent from very remote areas or in cases where network infrastructure is seriously damaged.

It is important to know the operational limitations (such as ingress/egress routes, road conditions, and setup requirements) for agency-owned assets, as well as to develop policies and procedures for how an asset is requested, who can request it, and how the asset will be deployed, maintained, and demobilized after an event. For more information, see **Section 2** on enhancing coverage, including best practices for using FirstNet deployable assets and agency-owned deployable assets.

Agency-owned deployable assets provide responders with the ability to communicate from the field back to their department headquarters, their EOC or ECC. This enables responders to track and locate each other during an operation, reference online plans and databases, and communicate with one another via systems such as push-to-talk. Rapidly deployed FirstNet network equipment can fill a key niche in the command and communications chain, enabling communications from the EOC and ECC to the field command post, and to the individual responder on the ground.

Responding with FirstNet: Use Cases

FirstNet allows first responders in the field to share situational awareness with each other, with field command posts, and with EOCs and ECCs coordinating large-scale response operations. Most importantly, the FirstNet network can be adapted to meet the needs of responders during planned events and emergencies. More information on how public safety of all disciplines and jurisdictions have used FirstNet can be found at **FirstNet.gov/FirstNetInAction**.

Resources from the FirstNet Authority

Public Safety Advisors

If you need assistance in your local area, reach out to a FirstNet Authority public safety advisor. Our representatives engage with public safety to listen, educate, inform, and advance your needs.

FirstNet.gov/Advisor

Disicpline Newsletters

Sign up for one of our newsletters to understand the impact of public safety broadband on your operations from an expert in your public safety discipline — fire service, emergency management, law enforcement, EMS, and 9-1-1.

FirstNet.gov/Newsletters

Operational Assistance

The FirstNet Authority team offers advance planning and preparation support, post incident/event review, and excercise support, including an injects catalog. These engagements are offered at no charge to FirstNet subscribers.

FirstNet.gov/Assistance

FirstNet Deployables

Get the details on FirstNet deployables fleet. Deployables boost coverage in the aftermath of disasters, during large planned events or incidents, or in remote areas — and are available to subscribers 24/7 at no extra cost.

FirstNet.gov/Deployables

FirstNet in Action

Visit our FirstNet in Action page to see the best examples of public safety broadband being used in the field. Filter stories by the categories you are interested in, such as emergency management, preparedness, and natural disasters.

FirstNet.gov/FirstNetInAction

States/Territories

Visit FirstNet.gov to find a page for each U.S. state and territory where we collect examples of FirstNet use in your local area.

FirstNet.gov

FirstNet Apps and Devices

Learn how public safety agencies are using apps and devices over FirstNet.

FirstNet.gov/Apps
FirstNet.gov/Devices

The Redstone Arsenal Fire and Emergency Services team in Alabama uses FirstNet to ensure seamless communication during complex federal public safety operations. Tools, like push-to-talk and mapping services, help them work across the military base.

HELP AND SUPPORT FROM THE FIRSTNET AUTHORITY

The key to an efficient response for public safety officials is familiarity with their technology and tools. The FirstNet Authority Public Safety Advocacy team — many of whom are former first responders, communications leaders, and technology experts — aims to help public safety agencies across the nation become more comfortable with broadband technologies. Contact the FirstNet Authority Public Safety Advisor for your state or territory by visiting **FirstNet.gov/advisor**.

The FirstNet Authority offers facilitated discussions to work through pre-incident or event planning, exercise support, and post-incident or event reviews.

Network Experience and Engagement Program

Event and Incident Pre-Planning

Public safety agencies are constantly planning for risks and hazards that may impact their jurisdictions. Thinking about how FirstNet can support public safety's response to any potential incident is an important part of the planning process. The FirstNet Authority is available to engage with your agency on planning discussions that seek to identify and address key considerations related to the planning, operations, logistics, and technology needed during an incident. Whether it's a county fair or a large National Security Special Event, the FirstNet Authority can scale a planning engagement session to fit your needs.

During the planning session, the FirstNet Authority team will help you consider and identify the following:

- Agencies that may be responding to the incident
- Locations where public safety will need broadband capabilities, including but not limited to:
  - Command posts
  - Emergency Operations Centers
  - Operational areas (e.g., medical facilities, staging areas, camera locations)
  - Headquarters buildings (e.g., police, fire, EMS, ECCs, EOCs)

- Broadband capabilities needed, including but not limited to:
  - Voice/text/email
  - Mission Critical Push-to-Talk applications
  - Computer-aided dispatch
  - Situational awareness
  - GPS/Location-based services
- Devices and technology that will be used, including but not limited to:
  - Smartphones/tablets/laptops
  - Video cameras/body-worn cameras
  - Hotspots/Wi-Fi
  - In-vehicle routers

Agencies are also encouraged to check FirstNet coverage, either in the field or through FirstNet Central tools, to determine whether adequate coverage exists in the location of their planned event. Speed test apps and coverage signal apps can help determine whether public safety users will be able to use broadband devices to communicate at the location. If the service is not sufficient, working with AT&T in advance (typically 30+ days before a planned event) can help improve performance through "network optimization" (actions AT&T can take on the network side without deploying) or through sending deployable assets to the location for the event.

By participating in a FirstNet Authority pre-planning engagement, host agencies will receive maps marked with the locations they identified as well as a document with the details they provided about the locations, capabilities, and technologies that will be used during the event. This information is also provided to the FirstNet ROG to assist them in determining the right solution for the event.

Working alongside public safety officials during all phases of the event planning process provides the FirstNet Authority with valuable feedback on public safety's operational needs. This information contributes to the **FirstNet Authority Roadmap**, a public-safety-driven plan designed to help the FirstNet Authority evolve the network based on your critical communications needs.

Pre-Planned Events

Like emergency incident pre-planning discussions, the FirstNet Authority is available to engage with your agency about public safety broadband capabilities needed at your upcoming event. During the planning session, the FirstNet Authority team will lead a discussion to help you consider and identify the following:

- Agencies that will be supporting the event
- Locations where public safety will need broadband capabilities, including but not limited to:
  - Venues
  - Command posts
  - Emergency Operations Centers
  - Operational areas (e.g., medical facilities, staging areas, camera locations)
  - Headquarters buildings

At the Boulder FirstNet Lab, a team of engineers look at how the network operates, ensuring it provides key capabilities for first responders. They also demonstrate technology for public safety stakeholders, like MiniCRDs.

- Broadband capabilities needed, including but not limited to:
  - Voice/text/email
  - Mission Critical Push-to-Talk applications
  - Computer-aided dispatch
  - Situational awareness
  - GPS/Location-based services
- Devices and technology that will be used, including but not limited to:
  - Smartphones/tablets/laptops
  - Video cameras/body-worn cameras
  - Hotspots/Wi-Fi
  - In-vehicle routers

Post Incident/Event Review

Through the Post Incident/Event Review, or PIER process, the FirstNet Authority connects with FirstNet subscribers to learn and document their experiences using the network. This engagement is usually specific to an incident and/or event and is an opportunity to learn from public safety's use of the FirstNet network during their operations.

Following the PIER discussions, the FirstNet Authority develops and shares a document with the participating agencies. The PIER is much like a traditional After-Action Review (AAR) conducted by public safety agencies following an incident or event.

However, rather than providing a Corrective Action Plan, the FirstNet Authority PIER provides information and considerations that agencies and their partners can utilize to improve operations during future events.

These engagements are important to helping public safety and the FirstNet Authority learn how the network is being used in emergency situations. By capturing lessons learned and identifying successes and areas for improvement, agencies are more prepared to use broadband in future response operations.

FirstNet Inject Catalog

The FirstNet Authority has created a catalog of broadband-focused injects and questions for operations-based and discussion-based exercises. Our catalog of more than 800 broadband injects and questions covers a wide range of public safety activities, including specific injects/questions on FirstNet capabilities such as FirstNet Central and Uplift.

Most of the injects/questions are broadband-carrier agnostic. The catalog is in a format that is compatible with the Homeland Security Exercise and Evaluation Program's Master Scenario Events List template and that is easily searchable by activities to be exercised.

The FirstNet Authority recognizes that agencies may be at different stages in their broadband adoption, so we designed the inject catalog to account for these variances. Questions and injects in the catalog have varying degrees of complexity and can be modified to meet the goals of your exercise and the scenario you are using.

The inject catalog was specifically designed to assist agencies currently utilizing broadband and working to incorporate broadband capabilities in the future. The catalog is available to exercise planners upon request by emailing: **FirstNetExercises@firstnet.gov**.

Using Grants to Purchase FirstNet

SAFECOM is managed by the Cybersecurity and Infrastructure Security Agency (CISA). Through collaboration with emergency responders and elected officials across all levels of government, SAFECOM works to improve emergency response providers' inter-jurisdictional and interdisciplinary emergency communications interoperability across local, regional, tribal, state, territorial, international borders, and with federal government entities. **SAFECOM publishes Grant Guidance** to provide information on eligible activities, technical standards, and other terms and conditions that are common to most federal emergency communications grants. With the caveat to follow program requirements when applying for federal funding, SAFECOM Guidance is recognized as the primary guidance on emergency communications grants by the Administration, the Office of Management and Budget, and federal grant program offices. Best practices and technical standards located within the SAFECOM Guidance help ensure that federally funded emergency communications investments are interoperable and support national policies.

The FirstNet Authority encourages grant applicants interested in investing federal funds in broadband-related projects, potentially using the NPSBN/FirstNet, to consult with the FirstNet Authority and the federal granting agency to understand all the requirements impacting broadband investments. To find the FirstNet Authority contact for your state or territory, go to **FirstNet.gov/Advisor**.

FirstNet Boulder Lab

In disasters and emergencies, first responders need communication tools that are tested and proven to work — consistently, securely, and reliably. That's where the Boulder FirstNet Lab comes in.

The Boulder FirstNet Lab is a state-of-the-art laboratory in which the FirstNet Authority tests public safety functionality and features unique to the FirstNet network. These include current and future quality of service, priority and preemption, mission critical services and applications, and future public safety functions. The Lab is located at the technical office of the FirstNet Authority in Boulder, Colorado.

The Boulder FirstNet Lab is built with Telecommunications Industry Association standards in mind. It is a federal facility where the FirstNet Authority has the equipment needed to complete its own network validation and testing. The Boulder FirstNet Lab connects to the FirstNet network, including Band 14 and other AT&T bands.

State-of-the-art testing

Testing functionality and features for public safety in the lab allows FirstNet Authority engineers to evaluate that responders receive the prioritized user experience expected and as designed for them on the network.

For example, using specialized load test tools, lab engineers can simulate congestion on the network to show how priority and preemption work for first responders on FirstNet.

Experts in the Lab also look at new and emerging technologies to understand how they operate on the FirstNet network, such as:

- Compact Rapid Deployables (CRDs) and miniCRDs
- Land mobile radio to LTE integration
- In-building solutions like the Cell Booster Pro
- High-power user equipment

Engineers in the lab help ensure the tools, features, and functions that first responders need work as expected on current and evolving generations of broadband.

See the lab for yourself

FirstNet Authority staff provide in-person and virtual demonstrations to interested public safety agencies and officials. Lab tours are open to any public safety agency or first responder, whether they're a FirstNet user, considering using FirstNet, or just want to learn about public safety broadband technology. If you would like to set up a tour, visit FirstNet.gov/Lab.If you would like to set up a tour, visit **FirstNet.gov/Lab**.

ENHANCING FIRSTNET COVERAGE

SECTION **2**

Gert Zoutendijk

FirstNet subscribers can request a deployable asset to support critical incidents, disasters, and planned events. This SatCOLT was deployed to a rural area to support firefighters during the 2021 Bootleg Fire in Oregon.

FIRSTNET DEPLOYABLES FLEET AND LOCAL SOLUTIONS

Understanding the Deployable Program

FirstNet supports hundreds of dedicated FirstNet deployable assets, strategically pre-positioned with both satellite and terrestrial backhaul capacity. These assets can provide coverage whenever necessary in the United States, including the U.S. territories. FirstNet subscribers can request these assets through FirstNet Central or by calling FirstNet Customer Support when there is little to no terrestrial coverage in an emergency situation or they need support for a planned event.

What is available to FirstNet users?

There are more than 180 deployable network assets dedicated to FirstNet users. Primary agencies can request a deployable to support critical incidents, disasters, planned events, and exercises. These assets, including fuel, personnel, and satellite airtime, are provided at no cost to subscribing agencies. The FirstNet deployable assets are stationed strategically throughout the country and available to subscribers 24/7/365. AT&T also has a separate but complementary Network Disaster Recovery (NDR) program with hundreds of additional assets that support the commercial network as well as FirstNet.

In addition to the SatCOLTs and COWs, there are additional solutions such as the Flying COW, which consists of a drone tethered to a trailer that can reach up to 400 feet high. The Flying COW is ideal for wildfires or mountain rescue missions where terrain may make connectivity a challenge. In 2024, AT&T began using the Flying COW for hurricane response, keeping responders connected over a wide area from just a single asset deployed in the field.

Other new deployable assets in the fleet include Response Communications Vehicles, which carry multiple networking options and provide a mobile office where responders can work out of the weather; Compact Rapid Deployables (CRDs), compact assets that can be quickly deployed to provide coverage in locations where larger vehicles can't go; and in-building kits, which can improve indoor coverage at EOCs or impromptu command posts that have been stood up in the field. The **miniCRD** is a portable version of the CRD, consisting of two medium-sized rugged cases. One case contains a

Low Earth Orbit (LEO) satellite backhaul connection to the network, and one contains the cell site equipment to create the local connection to FirstNet devices. The miniCRD has additional backhaul and power options. Additionally, the Low Earth Orbit Compact Trailer provides an asset that can be deployed into remote areas beyond the terrestrial network's limits; the LEO Compact Trailer brings FirstNet service to many responders at once via a satellite connection.

How does it work?

The deployable assets can provide up to several miles of Band 14 coverage exclusively for public safety use. Range often depends on the terrain in which the deployables are set up. These assets can support FirstNet users with FirstNet-capable devices that have a FirstNet SIM card or a FirstNet eSIM. They are intended to ensure network availability and effective assistance to public safety; they are not intended to support commercial cellular traffic. Because of the limited bandwidth available when connecting to satellites, the deployables are best suited for mobile voice, text, and light data usage. Heavy data usage, such as video streaming, is possible, but it will limit the effectiveness of the deployable asset.

Different assets have different capabilities to best support the public safety operational need, and the FirstNet ROG will determine the best solution for each deployment mission. The ROG is a dedicated team within AT&T FirstNet that supports public safety incidents where coverage for first responders is not available or requires additional capacity.

How do you request a deployable solution?

There are multiple ways to request FirstNet support for your incident or event. The easiest way is to use the online Deployable Request Tool in **FirstNet Central**. This tool is available to an agency's FirstNet Administrator(s) and those users who have been designated Uplift Managers. The online tool will take you through the entire request process in less than 10 minutes. The tool will pre-fill many of the fields based on the information in your user account.

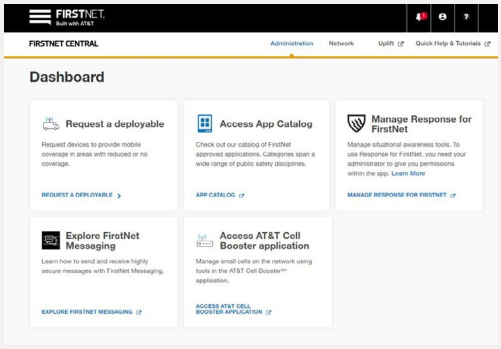
It is important to note – not every request for support will result in a deployable asset being sent by AT&T.

Once you submit your request using the online tool, you will receive an email confirming your request. You will also receive emails as your request goes through the triage process and a solution is determined. You will likely be contacted by someone on the FirstNet ROG team to discuss the best options for fulfilling the request for assistance.

FirstNet subscribers can also contact **FirstNet Customer Care (1-800-574-7000) and specifically state, "I need to request a deployable asset."**

Pro Tip:
Access Deployable Request Tile

The Deployable Request Tile only shows up in FirstNet Central if you are an Agency Administrator or an Uplift Manager.



When calling FirstNet Customer Care, the requester should be prepared to provide the agency's FirstNet Foundation Account Number (FAN). The FAN can be obtained from the agency's FirstNet Account Administrator or by working with an AT&T sales representative.

Regardless of how you make the request, the FirstNet ROG will process the request and identify the best solution to deploy. The requester will receive confirmation and follow-up emails from the FirstNet ROG as the deployment request is processed and executed.

It is important to note that only FirstNet Administrators and Uplift Managers can request deployable assets. FirstNet Administrators can create multiple sub-Administrator and Uplift Manager accounts to ensure that the agency always has personnel with appropriate account permissions available.

For planned events, use the online Deployable Request Tool in FirstNet Central or call FirstNet Customer Care (1-800-574-7000) ***at least 30 days in advance*** *of the event to request FirstNet deployable support.*

To learn more about requesting a deployable, reference the FirstNet Authority's fact sheet: **FirstNet.gov/deployableFAQ**.

What information will you need to provide?

When requesting a deployable, it is critical to describe, in detail, what mobile broadband communications needs your agency has for the event/incident. Be sure to include information about the incident conditions, the area(s) requiring coverage, and any environmental/terrain concerns. Other important information to provide may include road access and conditions, steep inclines, sharp curves, washouts or roadway/bridge restrictions, and if an escort is required. If a deployable asset will be placed on a parking garage or other structure, provide height and/or weight restrictions, turning radius, and other logistics information when making the request.

Using the deployable

AT&T technicians are responsible for transporting, setting up, and breaking down the deployable asset. When setting up the deployable, they will need a clear, level unobstructed view of the southern sky and a secure location to stage the asset. For larger deployables, such as a SatCOLT, larger areas are required to ensure there is an adequate safety perimeter (at least 100 feet) and they are not situated near areas with heavy responder radio traffic, such as a command post. Larger assets also should be parked on a solid surface, such as concrete or pavement; softer surfaces, such as grass or sand, may cause the deployable to shift and lose the satellite connection. During operation of the asset, AT&T technicians may need access to the deployable to refuel generators, but otherwise the asset will be managed remotely by AT&T.

These assets are dependent upon satellite backhaul to connect to the network; this is an important feature to have when terrestrial infrastructure may be damaged. While terrestrial connections such as fiber provide the most bandwidth, satellite backhaul is a more limited resource. When using a deployable, FirstNet subscribers are encouraged to coordinate and consolidate the use of apps and capabilities that are necessary to the mission to help manage satellite bandwidth. While technically possible to perform over the satellite connection, video streaming puts a great deal of pressure on the limited satellite bandwidth and will greatly impact the deployable's performance for other uses.

Deployables for 9-1-1

If an ECC loses connectivity or needs to be evacuated, incoming 9-1-1 calls can be routed through FirstNet deployable assets. If an agency owns a CRD or miniCRD, the asset can be set up anytime and anywhere it is needed to support ECC operations and keep vital systems up and running. If external support is needed, FirstNet customer agencies can request support from the ROG™ team who can triage and provide the appropriate solution based on the location and capacity needs.

Pro Tip: ROG Assesments

It is important to remember that not all solutions are SatCOLTs. There are some medium and smaller sized deployable assets, as well as solutions that adjust the macro network where no assets are needed to be brought to your scene. Using the information you provide, the ROG will identify the best solution for your needs.

Anytime a FirstNet deployable asset is deployed into a community, 9-1-1 calls *from any carrier* can be completed via the asset's network connection. Agencies have deployed CRDs into areas with known cellular or landline telephone outages to ensure the public can make and complete 9-1-1 calls.

Connectivity Solutions to Improve Local Coverage

As the FirstNet network continues to grow and evolve, public safety users have asked for new and improved ways to connect to the network in the field, their headquarters facilities, incident command posts, and other locations. The FirstNet Authority and AT&T are using that feedback to develop technologies to solve these challenges. As a result, public safety users now have several options to stay connected.

How to check your coverage

Several companies conduct ongoing coverage assessments through third-party data gathering from LTE connected devices. Coverage data is automatically collected by user applications and allowed under a user agreement, which is compiled to create a map of presumed coverage. This data is often available for all mobile carriers and provides first responders with information to aid their decision making on which network to use.

Additionally, there are applications available to help understand connection metrics (speed, latency, jitter, etc.), the type of connection (3G, Wi-Fi, 4G, 5G, etc.), and the LTE signal band (for example, FirstNet's Band 14) being used by the device.

Signal strength is measured in decibel-milliwatts (dBm), and the FirstNet network is designed to operate with a downlink signal as low as -122 dBm. Even so, there are situations where public safety can utilize additional equipment to improve their signal in low-coverage areas.

Large Deployable Form Factors

Compact Rapid Deployable

Antenna Height: 16 feet

Coverage Radius: Up to 1 mile

Spectrum/Backhaul: Band 14/Satellite, Ethernet, LTE, or WiFi

Capacity: ~50 Active Users

Communications Vehicle

Antenna Height: 30 feet

Coverage Radius: ~1+ miles

Spectrum/Backhaul: Band 14/Satellite, Ethernet, or LTE

Capacity: 50+ Active Users

SatCOLT

Antenna Height: 60 feet

Coverage Radius: ~1-3 miles

Spectrum/Backhaul: Multi-Band/Satellite

Capacity: ~350 Active Users

Cell on Wings

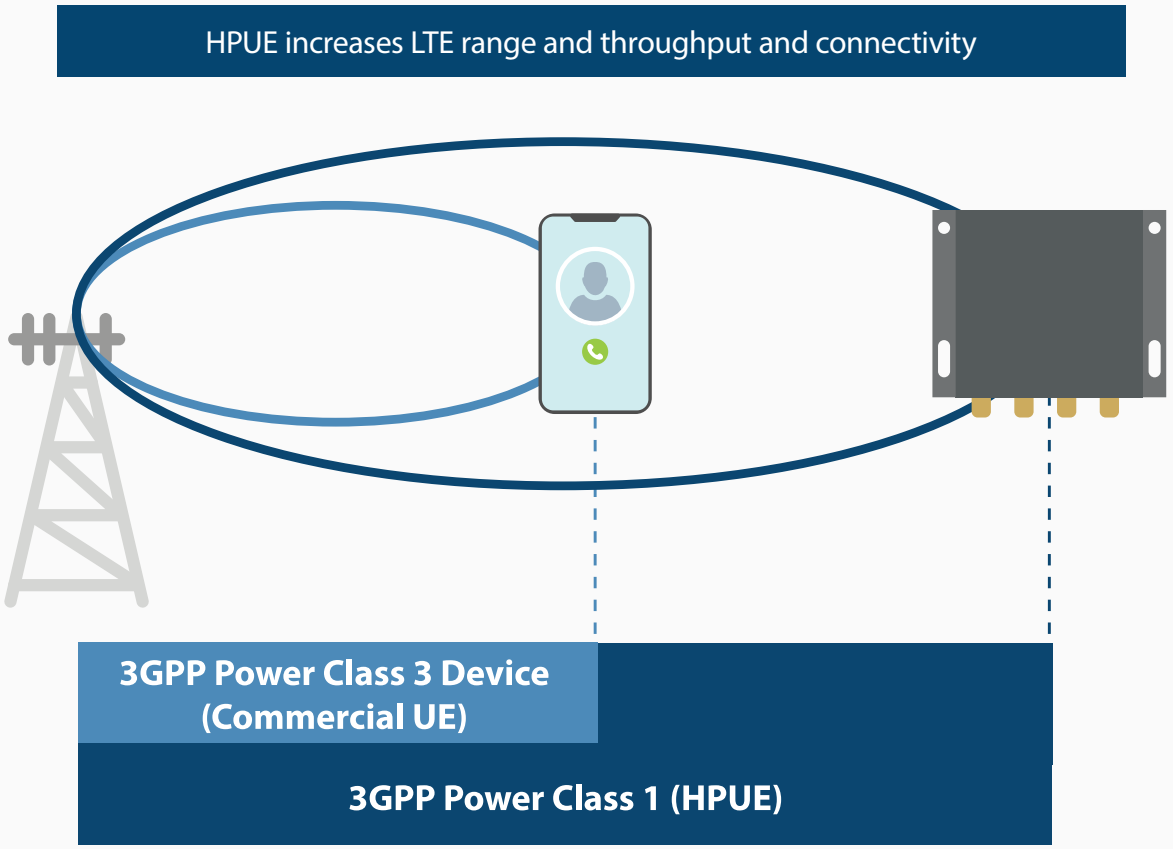
Antenna Height: 400 feet

Coverage Radius: ~5 miles

Spectrum/Backhaul: Band 14/Satellite or Fiber

Capacity: ~350 (Sat)/350+ (Fiber) Active Users

Figure 1: HPUE range information



	Commercial UE	High Power UE
Operational Bands	All bands	All bands
Maximum Transmit Output Power	200 mW (+23 dBm)	Band 14: 1.25 W (+31 dBm) Other Bands: 200 mW

High-Power User Equipment

Many public safety agencies frequently operate in rural and remote areas as part of their daily business. When emergencies occur in places that are at the fringe of cellular broadband coverage, first responders need to be able to communicate. FirstNet provides a unique solution for keeping responders connected in areas with challenging coverage.

In accordance with the FirstNet Authority's Federal Communications Commission (FCC) license for the Band 14 spectrum and standards established by 3GPP, certain FirstNet devices are authorized to transmit on Band 14 at a power level significantly higher than normal cellular power. The specific devices are allowed to communicate with FirstNet towers at the higher power level of 1.25 watts. This mission critical capability is called **High Power User Equipment (HPUE)** and is currently only available on FirstNet.

HPUE can improve connectivity and data uplink speeds — particularly at the edge of signal coverage — to keep first responders communicating. HPUE devices increase transmission power up to six times beyond what is allowed for commercial devices. The increased signal extends

Other Coverage Solutions

Mini Compact Rapid Deployable

Coverage Radius: Up to 0.5 mile

Spectrum/ Backhaul: Band 14/
Starlink, fiber, WiFi, LTE, LAN

Capacity: ~50 Active Users

Mobile Broadband Kit

Capabilities:

Portable, ruggedized CradlePoint that will provide WiFi capabilities using Band 14 coverage; one button setup and demobilization.

CEL-FI GO RED

Capabilities:

Cell signal booster that will bring outside cellular coverage indoors.

Cell Booster Pro

Capabilities:

Indoor coverage solution. Coverage area is about 15,000 square feet. Requires agency-provided internet internet or Starlink backhaul.

High Power User Equipment

Capabilities:

Consistent with 3rd Generation Partnership Project (3GPP) standards, transmits higher uplink power on Band 14 at six times that of a standard user equipment.

coverage in rural areas and provides stronger building penetration when in or near structures. HPUE devices operate at the higher power setting for Band 14, and at standard power levels on all other bands. FirstNet's HPUE solution is called FirstNet MegaRange, which can be used in vehicles, on the go, or at fixed locations. In addition to providing a data connection, these devices have built-in Wi-Fi capability that allows them to connect to smartphones with the appropriate credentials and Wi-Fi calling enabled.

MegaMobile is designed to be used in public safety vehicles and mobile command posts. It can support connectivity on land and water.

MegaGo is a portable HPUE device that comes in a rugged waterproof carrying case with a rechargeable battery pack, Wi-Fi hot spot, and integrated antennas.

MegaFixed is for use at fixed locations to boost FirstNet connectivity in remote sites, command centers, and IoT applications. It has HPUE technology plus an ethernet port and a wall adapter for AC power sources.

In urban environments, MegaRange can improve connectivity and data throughput when signal penetration is hindered by dense urban surroundings or in underground locations. It can boost coverage in hard-to-reach spots such as tunnels, basements, elevators, stairwells, parking garages, and building shadows.

In remote environments, connectivity is extended at the edge of the network's typical signal. HPUE can be particularly helpful when fighting wildland fires, going on maritime missions, conducting remote search and rescue operations, or responding in rural areas.

In-building solutions

Public safety command and control operations often happen inside a large building, possibly in an older structure or basement, posing challenges to getting strong LTE signals inside. Even modern buildings with new materials can interfere with cellular signals reaching those working within. Headquarters facilities, EOCs, and ECCs can benefit greatly from FirstNet technologies that help improve indoor cell coverage for public safety officials.

One recommended option for permanent public safety facilities is the FirstNet Cell Booster Pro (CBP). The CBP acts as a miniature cell site inside a fixed facility, providing indoor FirstNet coverage up to 15,000 square feet. Up to six CBPs can be connected in a building to provide up to 90,000 square feet of coverage. The CBPs are simple to install and provide all the benefits of being on the FirstNet network (Band 14, quality of service, priority and preemption, and mission critical services). The CBP requires a wired internet connection and can be installed by the user or through a professional installation service. Depending on the number of CBPs in a facility, users will experience increased download and upload speeds, and a greater number of users will be able to connect to FirstNet at the same time.

If a hardwired internet connection is not available, there are other options that can potentially bring LTE signal from outside into the building to improve FirstNet connections.

- The Cel-Fi GO RED smart signal booster is an in-building enhancement tool that public safety users can quickly deploy to improve indoor coverage when establishing a temporary EOC, remote command post, or ECC backup center. The GO RED helps boost the FirstNet signal for improved voice and data connectivity in both indoor and outdoor environments and can also cover up to 15,000 square feet. Multiple GO REDs can be connected to each other to provide improved network connectivity in larger spaces. In contrast to the CBP, the GO RED may be useful for facilities where there may not be a wired internet connection, but there is strong FirstNet LTE service outside the facility.
- Another option for both permanent structures or for temporary locations, is a MegaFixed HPUE device. This device works similarly to the GO RED but also includes the capabilities of FirstNet's High Powered User Equipment (see: **HPUE section**) to connect to available LTE signals outside the building at a higher transmitting power setting. The MegaFixed device then helps to

Pro Tip: Agency-Owned and Managed Assets

Many agencies are purchasing their own deployable assets to provide for emergency communications or to supplement AT&T requested assets.

1. Make the most of your agency-owned deployables by identifying where and how responders will operate before deploying the asset.
2. Explore "EOC-in-a-box" approaches where a vehicle or trailer asset is used to stand up a mobile command post.
3. Use devices like personal hotspots or mobile broadband kits to provide broadband service in rural, marine, or subterranean environments.

FirstNet Authority participated in a Northern Mariana Islands communications exercise where they demonstrated how FirstNet can support public safety through tools like MiniCRDs.

bring that signal inside the building for improved FirstNet connectivity.

Low Earth Orbit (LEO) satellite solutions

The FirstNet Authority continues to enhance coverage in rural and remote areas. Various solutions are being explored, including satellite-to-device services to provide coverage in areas outside the typical terrestrial coverage footprint. AT&T has received authorization from the Federal Communications Commission (FCC) to test direct-to-cellular connectivity on Band 14 starting in 2025. Initial capabilities may support basic functions, such as talk, text, basic location-based data, and low-bandwidth data, with additional advancements over time. Building Redundancy with FirstNet

How to Make a FirstNet Support Request

AT&T FirstNet Response Operations Group (ROG™) support is available at no cost to all FirstNet customer agencies 24/7/365. Support can be requested anytime additional network coverage is needed. This could include support for a planned event, a search and rescue mission, response to an incident or disaster, planned maintenance, or a network outage, among many others.

There are three (3) methods to request support from AT&T FirstNet ROG™.

Option 1: FirstNet Central Website

The easiest option is through the FirstNet Central website. Any user who is designated as an agency administrator or an uplift manager by their organization will have access to the Request a Deployable tile on the FirstNet Central landing page. There will be 3 simple pages of information to fill out.

Some things to have ready when requesting support this way:

- Your phone number or a phone number on scene where the support is needed
- When you need this support to arrive — immediately (within 14hrs), more than 14 hours but less than 30 days, more than 30 days
- Location where the support is needed
- A detailed description of your issue (not the solution you think you need) and any logistical challenges

Option 2: Local AT&T Sales Team

The second way to submit this request is through your local AT&T sales team. You will need the same information as you would need for the website.

Option 3: Customer Support Representative

The third way is to call 800-574-7000 to talk to a customer support representative. For this method, besides the information above, you will also need your Foundation Account Number (FAN) to begin the process.

FirstNet Deployable Request Worksheet

When requesting a deployable or other coverage enhancement, it is critical to describe what mobile broadband communications needs your agency has. The FirstNet deployable program has many different form factors in the fleet. It is important to describe your problem in detail so that the right solution can be deployed. Use this worksheet to prepare before making your request.

Incident Conditions

What problem is being experienced/expected?

Area(s) requiring coverage, inlcuding whether you need in-building coverage:

Environmental/terrain concerns:

Number of users/number and types of devices:

What communications capabilities will be needed (e.g., voice, text, email, apps, data, images, video, web browsing, sensors)?

Access and Conditions

Note any steep inclines or sharp curves:

Note any washouts or roadway/bridge restrictions:

Is an escort or credential required to access the site?

Is the site secure and clear of pedestrian/vehicle traffic?

Parking and Structures

Is a 100 x 100 foot hard-packed parking spot with a clear view of the southern sky available?

Note any height, weight, or turning radius restrictions:

Does the site have underground or overhead utilities? Is the site accessible for refueling?

Best Practices: FirstNet Deployables

 Know how to request a deployable and who is authorized to do so.	Don't assume support was requested. A deployment request from an authorized FirstNet user must be submitted to formally start the process.
 Specify any problems that are being experienced, identify locations where coverage is needed, know the approximate number of users, the approximate number and types of devices in use, and what capabilities will be needed.	Don't specify a particular solution. The AT&T Response Operations Group (ROG) will evaluate requirements and deployment conditions in order to send the most appropriate solution to meet your coverage needs.
 Provide incident conditions, including terrain and access.	Don't skip the details. Knowing more about your situation will help the ROG provide the best solution.
 Request a deployable for a planned event at least 30 days in advance and coordinate with Emergency Operations Centers and other responding agencies that may also be requesting a deployable for the same event.	Don't wait for the disaster to strike. Make a plan with you and your partner agencies on how to request deployables and use FirstNet devices/ caches before they are needed.
 Use deployables responsibly. Only stream video or use high-bandwidth applications if they are necessary to the mission. Educate users that may be unaware.	Don't stream non-mission-critical video or use high-bandwidth applications unless necessary for the mission. Satellite backhaul is a limited resource and impacts the experience of all users who are connected.
 Plan to have adequate numbers of Band-14-enabled FirstNet devices available and to use wireless hot spots to help non-FirstNet users connect their devices to the FirstNet deployable's signal.	Don't expect the deployable to arrive with "spare" devices that can be distributed to non-FirstNet users.
 Request a Post Incident/Event Review from the FirstNet Authority to let us know about your experiences, successes, and challenges so we can help improve the next deployment.	Don't forget to review what worked well and any areas of improvement following a deployment.

Customer Owned and Managed (COAM) CRD Operations and Maintenance

Operational considerations:

Prior to deployment, email AT&T at **DL-FirstNetEmergencyOps@att.com** informing them of a CRD for FirstNet deployment. Include the following information:

- CRD serial number (located on the scissor lift crossbar)
- Deploying agency
- Nature of the deployment
- Lat/Long location of the deployment
- Start time and duration

Key deployment steps:

- Stabilize the CRD.
- Turn on all circuit breakers located on the rear of the controller.
- Power using either shore power or supplied generator.
- Deploy the satellite dish.
- Verify Wi-Fi functionality.
- If using cellular broadcast LTE function, deploy the mast and install LTE antennas. Verify cellular functionality.
- Once the Wi-Fi and LTE cellular functions (if required) are verified, the deployment is complete.

Maintenance:

Conduct maintenance check with each CRD unit individually, not simultaneously, to ensure connectivity tests are not contaminated by adjacent unit.

Do the following once a month:

- Turn on all circuit breakers located on the rear of the controller.
- Test shore power operation.
- Test supplied generator operation.
- Charge the unit completely until the battery monitor synchronizes to full state.
- Install the LTE antennas, deploy the satellite dish, acquire signal, and wait for CRD to be fully functional.
  - Verify Wi-Fi functionality.
  - Verify cellular functionality.
- Once the wifi and cellular functions are verified, the test is complete.
- Secure and stow the CRD.

COAM miniCRD Operations and Maintenance

Operational considerations:

- Check the location of the deployment for maximum coverage.
- Check to see if the miniCRD can be integrated into the existing communications network (mesh network).
- Conduct coverage testing once deployed to ensure you have the coverage you need where you need it.
- Starlink updates during operational periods do not need to be applied immediately, they can wait until the incident is completed.
- Consider adding the external antenna upgrade kit which provides full power of the radio and extends the coverage area.

Key points:

- Ensure you have the proper tools needed to access the equipment.
- Ensure you have an alternative external power source available/ready.
- MiniCRD battery levels below 50% cannot be plugged into a cigarette lighter in a vehicle (it will blow the fuse).
- Seek alternative backhaul sources to the Starlink panel.
- Ensure you have duplication of cables between the two cases in case something needs to be switched out.

Maintenance:

- Ensure everything is charged.
- Routinely check for updates on the Cradlepoint, Radio, Victron unit and Starlink panel.
- Ensure the Victron unit's state of charge is in sync with the app.
- Check that all connection points are cleaned/clear of debris.
- Ensure the Victron unit is set to no more than a max draw of 15 amps.

How to provision 9-1-1 calls to the appropriate PSAP on a CRD or MiniCRD

Send email in the proper format to provision 9-1-1 calls to the appropriate PSAP.

Email: **dl-firstnetemergencyops@att.com**

Subject: Agency, type of deployable (CRD, miniCRD), include number of units if deploying multiple

Body: Provide incident or event name and a short description of the deployment

Provide the information below for each unit you are deploying:

FirstNet Account Number (FAN): (Located on the CRD/miniCRD Placard)

SBO SN: (Located on the CRD/miniCRD Placard)

SBO CELL ID: (Located on the CRD/miniCRD Placard)

GPS: Lat, Lon

Closest Address to CRD/miniCRD:

Start Date and Time:

Duration:

BUILDING REDUNDANCY WITH FIRSTNET

SECTION **3**

In Kansas, FirstNet is used as a tertiary backup to their statewide dispatch system and as the network connection powering a statewide Emergency Mobile Dispatch and Training Center.

ESINETS, ECC SOLUTIONS, AND REMOTE OPTIONS

ESInet Wireless Redundancy

As ECCs begin to transition from analog systems to digital Next Generation 9-1-1 (NG9-1-1) services, telecommunicators increasingly have access to complex data, including enhanced caller location, artificial intelligence (AI)-assisted real-time translations, and real-time photo and video. Uninterrupted connectivity has been and will continue to be of utmost importance for ECCs. FirstNet can support ECCs with wireless redundancy by providing a reliable, secure, interoperable network, allowing telecommunicators to safely and securely access, analyze, and share data in real time.

FirstNet can function as a wireless redundant solution to back up an ECC's regular ESInet, or emergency services Internet protocol network, that handles 9-1-1 calls and services. If the network experiences a maintenance window or fiber cut, FirstNet can be on active standby to automatically provide connectivity, even if there is a 9-1-1 call in progress. As a redundant solution, it can work with any other call handling and ESInet provider. FirstNet's priority and preemption offers reassurance the connectivity will prevail even when there is network congestion.

Additionally, 9-1-1 calls can be routed to a FirstNet enable smartphone's 10-digit number to serve as a last order back up effort to an ESInet. This routing approach also works for a selective router problem to get calls returned from a backup location or in the situation where a different location exchange carrier is being used than the ESInet provider. Additionally, a FirstNet smart phone can support 9-1-1 calls, should they ever need to be routed to a 10-digit line, bringing quality of service, priority and preemption to ensure the calls go through. Using the phone's hot spot can also keep connectivity up and running.

ECC Redundancy/Resiliency

ECCs have several options to maintain connectivity and operational readiness during an incident, including terrestrial wired and/or wireless connectivity, as well as satellite connectivity. The most appropriate option will depend on the ECC's needs, intended use, and available funding.

Basic connectivity can include a MiFi device, such as a personal hotspot or high-power user equipment (HPUE). The HPUE mobile hotspot offers six times the transmit power of regular hotspots for better range, better building

penetration, and higher upload speeds. Hot spots on FirstNet-connected cellular devices can be used to support remote call taking and dispatching, as well as provide internet access for the center.

More advanced connectivity options include mobile routers with enhanced capabilities, such as cellular redundancy (i.e., dual SIMs), bonding of SIMs, and/or satellite redundancy. Another option is to use a multi-wide area network (WAN) mobile router that can bring together local WAN, cellular, and satellite in one device. The device can bond to create greater bandwidth than any of the single WAN sources or configure to do simple failover without packet loss.

Remote Call Taking and Dispatching

ECC's are no longer bound to brick-and-mortar limitations. Remote call taking and dispatching redefines how telecommunicators respond to emergencies – with broadband, IP technology, and FirstNet powering location-independent operations.

Remote call taking and dispatching have become a proven model for ECC business continuity and surge staffing, allowing for immediate assistance. High-priority, low frequency events such as natural disasters can now be addressed through flexible remote deployments in the event an ECC is inaccessible or needs to evacuate. Remote capabilities continue to evolve offering resiliency, agility, and extended coverage during any emergency.

Remote workstations can operate effectively using IP remote consoles and secure VPN connectivity. Routers and hotspots with FirstNet sims, along with FirstNet enabled smartphones, will provide quality of service, priority, and preemption.

Go-bags and deployment kits can be created using laptops, dual monitors, headsets, smartphones, mobile routers, and VPN-accessible CAD software. These can easily be scaled up or down for daily use to disaster recovery ranging from a basic MIFI hotspot or to more advanced mobile routers in deployable cases for larger capacity.

USE CASE

Evacuation of an ECC

Scenario:

A large thunderstorm with heavy amounts of rain is impacting the region, causing flooding, damage, and road closures. The 9-1-1 call volume has steadily increased as the storm has worsened, homes are flooding, and evacuations are underway, hampered by widespread flooding. Flood water has begun to fill the ECC, requiring telecommunicators to evacuate. The ECC has a backup center; however, due to the impact of the storm and shelter in place orders at the backup center, staff are unable to reach it. As a contingency, there is a County Highway Department facility that can provide premises for dispatch operations. The Highway Department location would require the use of ECC go-kits that contain telephony, radio, and CAD capabilities. Identified staff have access to remote call-taking and dispatch kits, which means that off-duty staff may be able to maintain simplified operations while on-duty staff transition to the contingency location.

Scenario Objectives:

- Highlight planning best practices; including multiple, geo-diverse locations for contingency plans and equipment staging.
- Highlights the ability to stand up an ECC anywhere there is connectivity, to continue to manage a high-stakes emergency, and ensuring robust communication across diverse challenging environments.
- Demonstrate the practical application of equipped remote telecommunicators during emergency operations.

1. Deployment of remote call taking and dispatching

Telecommunicators can be set up with remote workstations including laptops, monitors, headsets, VPN-accessible CAD software, FirstNet smartphones and hotspots. These workstations can be deployed virtually anywhere, as long as there is connectivity. Often, remote workstations are deployed in a telecommunicator's home.

Benefits:

- FirstNet enabled devices provide quality of service, priority, and preemption, ensuring connectivity
- Nearly instantaneous staffing resources during surge events
- Telecommunicators don't need to travel to the ECC, saving valuable time
- Ensures the telecommunicator can respond despite weather and road conditions
- Familiarity and experience with the equipment
- Opportunities for continuation of basic operations if the ECC must evacuate

2. Evacuation of the ECC

An ECC may have backup center, but there is no guarantee that staff can reach it or that it will be usable when they get there. Being able to connect and stand-up operations from anywhere is a key element of all PACE planning. Go-bags, which provide remote call taking and dispatching capabilities, including FirstNet connectivity, are essential.

Benefits:

- Mobile routers, as simple as MiFi routers, all the way to more advanced routers such as CradlePoints, with FirstNet SIMs establish connectivity to the internet and other ECC resources
- FirstNet smartphones ensure calls can be completed and received

3. Satellite connectivity

The ECC needs advanced connectivity as more users are added to the network and to ensure 9-1-1 calls are connected to the alternate location while the primary ECC is evacuated. FirstNet agencies can request the support of the Response Operations Group (ROG) to bring in larger assets that provide low earth orbit (LEO) satellite backhaul.

Benefits:

- If an agency owns a CRD or miniCRD, they can deploy those assets anytime and anywhere
- 9-1-1 calls can be routed through the FirstNet deployable to provide continuity of operations
- Provides Band 14 coverage for public safety with satellite backhaul
- There is no charge for these assets
- Larger assets, such as SatCOLT, can be as required to support the size and needs of the event
- 9-1-1 calls from any carrier are processed through the deployable network connection to complete the emergency call

4. Outcome

The use of FirstNet SIMS in routers, hotspots, and through deployable assets ensures uninterrupted, interoperable communications to ECC operations outside of the actual center. Key advantages include:

- **Rapid Coordination:** Remote call takers and dispatchers are prepared with equipment and connectivity to engage in a timely manner to assist with surge events
- **Resilience:** Hotspots and routers can be added to remote kits for resilient connectivity
- **Scalability:** Deployable assets are available at no cost to FirstNet agencies to provide the appropriate solution for the incident

By leveraging remote connectivity capabilities, the ECC effectively: 1) manages the influx of calls by activating remote call takers and dispatchers, 2) creates a backup center wherever they can, and 3) keeps 9-1-1 calls routed to their center. Telecommunicators can continue protecting lives and property while demonstrating the power of modern, remote public safety communications outside of the physical communications center.

FIRSTNET CENTRAL TOOLS

SECTION **4**

With the help of FirstNet, paramedics in Jackman, Maine, can conduct telehealth sessions and treat residents at the local health clinic or in their homes, rather than transporting patients to a hospital over an hour away.

NETWORK STATUS TOOL AND ALERTS

FirstNet users can access an online portal called FirstNet Central. Agencies or individuals create an administrative account during the onboarding process. Additional accounts may be granted varying levels of access to tools and features on the platform.

FirstNet Central supports multiple tools, including:

- Administrative functions that provide resources to aid FirstNet Administrators in the general management of their FirstNet account and services. This includes everything from shopping and provisioning devices to managing applications to administering coverage solutions like Cell Booster Pros.
- Operations functions that provide tools that can be used for situational awareness and to support operations when managing an incident or event. The five primary operations functions include: requesting a deployable, viewing network status, subscribing to network and application alerts, creating and managing uplift requests, and administering FirstNet PTT, if applicable.
- A quick help and tutorials area that has various videos, user guides, and instructor-led training opportunities.
- A mobile app — FirstNet Assist — that is used to access or interact with different elements of FirstNet Central. It is available to download in both the Apple App Store and the Google Play store.

Network Status Tool

The Network Status Tool shows the status of the FirstNet network and can be accessed via FirstNet Central. Public safety agencies have the authority to determine which personnel in their department should have access to the tool and should consider EOCs and ECCs.

The Network Status Tool enables public safety agencies to monitor various conditions that may affect the network (e.g., weather), identify potential impacts to operations, and help guide decisions on the use of resources (e.g., positioning resources in areas with good coverage, requesting a deployable). The tool is periodically updated by AT&T based on public safety feedback, with new features being added or functionalities improved.

Many public safety officials find this tool useful to monitor the status of FirstNet cell sites in their area, including a projected area of service impact when sites are experiencing an outage. The tool is also useful when sending mutual aid, search and rescue, or recovery forces into an impacted area. Knowing where cell sites are located and whether FirstNet service is operational can signal the need to request a deployable or send an agency-owned asset with the field team so they can communicate with the EOC, dispatch, and other partners.

There are two views within the Network Status Tool:

Standard View

A. Provides visibility into the status of the network to identify areas that may be experiencing outages. In the Standard View, higher severity unplanned outages are indicated by a yellow shading over the network market area(s) impacted by the outage. It does not mean the entire area shaded in yellow is impacted by the outage, but simply that an outage is occurring somewhere within the yellow shaded area. Clicking in the shaded area will display a window with available details regarding the outage. It is important to note that not all outages are noticeable or user-impacting, and an outage must reach a certain severity level for the county to be shaded in yellow on the map.

B. Allows users to view on-demand reports on locations scheduled for planned maintenance.

C. Enables users to subscribe to receive notifications of unplanned network outages. Notifications may be sent via SMS text, email, or push notification to the FirstNet Assist mobile app (same login credentials as FirstNet Central account). Users must subscribe to each desired notification method by entering contact information and target network market locations to receive alerts.

D. Includes additional layers that can be toggled on/off that provide awareness on conditions such as weather, active fire incidents, flooding, drought, wind, traffic, and hospital trauma center locations.

Advanced Network View

The Advanced Network View provides critical information for communications leads, Emergency Support Function (ESF) #2 personnel, communications coordinators, or equivalent roles that have communications expertise or who are responsible for managing the communications functions (e.g., daily operations, emergency incidents, planned events).

Pro Tip:
Access FirstNet Central

FirstNet Central can be accessed through the FirstNet website: **www.FirstNet.com** by clicking the Login button in the upper right corner of the page.

Access to this view is authorized by FirstNet Administrators and their designated users. Every user must accept the terms and conditions each time they access the system to acknowledge the confidential and proprietary nature of the network information displayed/shared with public safety.

This view includes everything from the Standard View, as well as the following information:

A. States or counties experiencing outages – these are shaded in yellow, with lighter shades indicating a single impact/outage and darker shades indicating multiple outages affecting the same area. Sites within those markets that are experiencing an outage are indicated by a red icon.

B. Cell site level detail – this information can only be viewed within one state or territory at a time. Clicking on a white square to turn on cell site details for a state/territory also provides a total count of macro sites in that region, as well as a count per county. A pop-up window will display the number of outages in that state or county.

C. Off-air tower sites – indicated by red flag icons.

   a. Users can click directly on a red icon to review the type(s) of communications technology or services that are impacted. Clicking on the icon also displays the cause of the outage (e.g., power, transport), if known, and an estimated restoration time.

   b. By zooming down to street level, users see the estimated geographic impact area of a site's outage, denoted as a red hash-marked area.

D. Sites in a planned maintenance window by AT&T – these will be indicated by purple icons. If the tower is taken offline for maintenance, the icon turns red; the icon returns to purple when the site is back on-air but still within the maintenance window.

E. On-air deployable assets – these are indicated by an icon. Clicking on the icon provides details about the deployable asset, such as its location and when it went on air.

Using the Network Status Tool

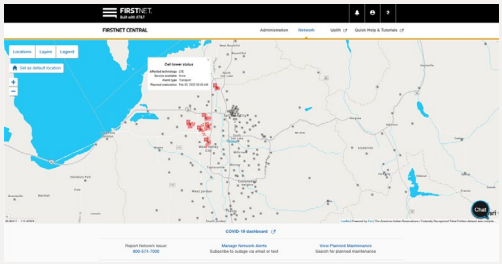
Public safety users should consider leveraging FirstNet capabilities and tools throughout the life cycle of an emergency. The following are suggested strategies to maximize the use of the Network Status Tool.

Pre-Planning/Pre-Event Phase:

- Identify FirstNet Agency Administrator(s) and create FirstNet Central user accounts for designated personnel.
  - To provide a user access to the Standard View of the Network Status Tool only, toggle on access to the Uplift Request Tool, which automatically includes access to the Standard View of the Network Status Tool.
  - To provide a user access to the Advanced Network View, toggle on access to the Advanced Network View.
- Develop and implement policies, procedures, and training for the use of the Network Status Tool to ensure familiarity with the platforms.
  - Implement routine checks of the Network Status Tool as part of an agency's operational/situational awareness activities to maintain proficiency with the tool and ensure passwords remain active.
  - Implement a weekly log-on task to review the status of the network and check for scheduled/planned maintenance within the local jurisdiction/region.
- Leverage user guides and instructor-led training resources on FirstNet Central and the Network Status Tool by selecting the Quick Help and Tutorials link within FirstNet Central.
- Direct designated users to subscribe and receive notification alerts for unplanned network outages within the desired locations via email, push notifications to the FirstNet Assist app, or SMS text message. Alerts can be viewed in the Advanced Network Status Tool to see more detail on the nature of the outage, sites involved, and potential impact to operations. To subscribe for alerts, users should select the "Manage Network Alerts" link directly below the map.
- Create reports detailing planned maintenance that may impact operations during an incident or event. It may be necessary to reach out to the agency's AT&T FirstNet Solution Consultant or **FirstNet Customer Care (1-800-574-7000)** if planned maintenance might conflict with a known operational event. Reports cover an approximately 60-day window, so running reports in advance of a pre-planned event provides reasonable time to work with AT&T if there is scheduled maintenance that may impact agency operations.

Pro Tip:
Tower Status

Simulated image from Advanced Network Status Tool. Red icon shows an impacted tower.



During Incident/Response Phase:

- Monitor the Network Status Tool during emergency incidents or planned events for network outages, planned maintenance, or weather events that may impact area(s) of operation. Note that a FirstNet Central user's session will time out after approximately one hour, and the map does not automatically refresh. It may be necessary to perform a manual refresh, as needed, to ensure current information is being displayed.
  - Continue to monitor the Network Status Tool periodically until operations are terminated.
- If sending resources, personnel, or teams outside the jurisdiction, check the destination in the Network Status Tool prior to deploying to identify the status of the network and availability of sites in the area(s) of operations.
- If deploying to an area where there is determined to be poor or no coverage, consider requesting a FirstNet deployable asset through the online Deployable Request Tool in FirstNet Central or by **calling FirstNet Customer Care at 1-800-574-7000** (see **Section 2: FirstNet Deployables Fleet and Local Solutions**).
- Depending on circumstances, consider use of the Uplift Request Tool (see **Section 4: Using the Uplift Request Tool**).

Preparing for Planned Maintenance

Understanding when planned maintenance is happening in your area can be very important. Are you having an event? Will the network be offline for an extended period?

Within the Advanced Network Status Tool, users can view a Planned Maintenance Report for any market. The report will show the user the start and end date of the planned maintenance, the city and state, as well as the services that are expected to be affected.

If the maintenance will cause a network outage in your area for a period of time, the agency should request deployable support from the AT&T FirstNet Response Operations Group (ROG™). It is always a good idea to submit the request for support and allow the AT&T FirstNet ROG™ to determine if a deployable asset will be necessary.

If AT&T has planned maintenance on a site near your planned event, contact your sales team and request the maintenance schedule be changed so it will not affect coverage during the event.

If you are requesting deployable support from AT&T FirstNet ROG™, select "Immediately" if the maintenance has already started or will begin within 14 hours or "Within 30 days" if there is time before the maintenance will begin. Include in the description that this request is to provide coverage while planned maintenance is occurring on the network in your area.

How to see planned maintenance:

Option 1

The easiest way is to log into the Advanced Network Status Tool and select Cell Site Details in the Layers tab and the state you are interested in. Cell sites scheduled for maintenance are identified by a purple flag. Clicking on the purple flag will show the user details of the maintenance, including start and end dates.

Option 2

The second way to see planned maintenance is to select View Planned Maintenance in the lower right corner of the screen once you have logged into the Advanced Network Status Tool. Select a state and a market then click on View Planned Maintenance. A report with all the planned maintenance in that market will be displayed on your screen.

Network Alerts

FirstNet Central users can subscribe to network alerts at the county level, as well as specific application alerts. Clicking on the link under the Network Status map will lead to a page where the user can manage all alert subscriptions.

Signing up for alerts

Users can choose to receive alerts via push notification in the FirstNet Assist mobile application, email, or text message. Email notifications provide the greatest level of detail on a specific network issue.

Users can select alerts for individual or all counties in a state and can select any combination of states/counties across the United States. Subscribing to at least one county will also enable nationwide network alerts. Network alerts are not currently available in the Pacific territories.

The volume of alerts is high, and we recommend starting with the smallest relevant geographical area to avoid being overwhelmed by too many notifications. Users can add/revise their notification settings as needed. To modify alert settings, users enter the same email address or phone number that was used to set up the alerts.

In addition to geographic network/tower alerts, users can also elect to receive application-specific alerts for information and details about known issues with FirstNet-branded applications such as:

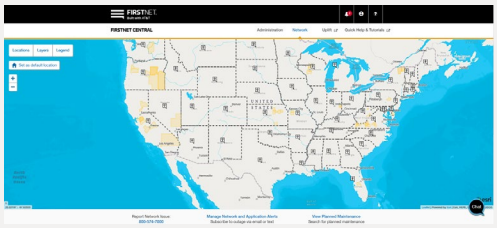
- FirstNet Account Management
- FirstNet Assist
- FirstNet Messaging
- FirstNet Network Status Map
- FirstNet Push-to-Talk
- FirstNet Single Sign-On FirstNet Uplift Request Tool (accessed through FirstNet Central)

Types of notifications

- Alert notifications are typically generated as an initial notification, an updated notification, or a final notification; these are noted in the subject line of an email message or within the alert notification details when pushed to the FirstNet Assist mobile app.
- Email notifications indicate which zip code(s) are impacted by the outage. The alerts include a start time; if it is the final alert, it will also include an end time (if known).
- Text message alerts have fewer details, but include a link to FirstNet Central for more information. Clicking on the link opens a mobile-friendly browser window where users can log in to FirstNet Central to access the Network Status Map.

Pro Tip:
Outages in Network Status Tool

Simulated image from Advanced Network Status Tool. Areas experiencing outages will be shaded in yellow.



- Alerts in the FirstNet Assist App will appear as a banner on the device's lock screen. Once in the app, users will see the bell icon in the top right corner with a red circle identifying at least one notification. Tapping the bell will present the notification(s). Select a specific alert to view the details.

FirstNet Central Network Alerting

FirstNet Central offers alerting for public safety users when there are conditions impacting the network or FirstNet-specific applications. Users can choose to receive alerts via push notification in the FirstNet Assist application, email, or text message (or any combination of these three methods).

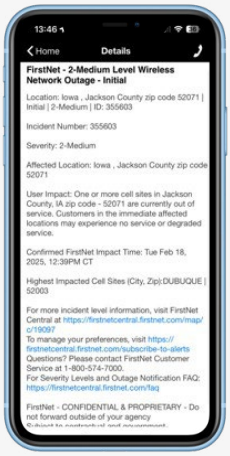
Alerts can be modified by the user to fine-tune the geographic area and number of alerts being received. It is recommended to start with the smallest geographic area relevant to the user, to avoid receiving unwanted alerts. By subscribing to alerts for at least one county, users are subscribed to nationwide alerts.

The platform also issues notifications if there is weather likely to impact the network. Weather events will be declared for a county prior to impact, and for high volume disruptions caused by power outages or structural damage, updates are provided twice per day at 9 a.m. and 5 p.m. Central time.

Alerts are also issued for specific FirstNet-branded applications, providing information and details about known issues. These applications include:

- FirstNet Assist
- FirstNet Uplift Request Tool (which is accessed through FirstNet Central)
- FirstNet Push-to-Talk
- FirstNet Messaging
- FirstNet Network Status Map (also accessed through FirstNet Central)
- FirstNet account management
- FirstNet single sign-on (SSO

E-mail Notification



Text Message Alert

FirstNet Assist App Notification

Alert notifications are typically generated as an “initial” notification, “update”, or “final” notification; these are seen in the subject line of an e-mail message or within the alert notification details when pushed to the FirstNet Assist mobile app. The alerts include a start time, and if it is the final alert, it will also include an end time (if known).

SMS text message alerts have fewer details. The message directs users to FirstNet Central for more details. Clicking on the link in the text will open a mobile friendly browser window where users can log in to FirstNet Central and access the Network Status Map.

If using the FirstNet Assist App, users will see a banner message on the lock screen. Clicking into the app itself will display a bell icon in the top right corner with a red circle identifying a number of notifications. Touch the bell to see the list of notifications. Select the specific one to view the details, which is the same language as email notifications.

FirstNet improved public safety communications in St. Augustine, Florida. FirstNet allows all city officials — from first responders to city management to public works — to work together.

USING THE UPLIFT REQUEST TOOL

The Uplift Request Tool, available in FirstNet Central, is used to temporarily elevate specific users (e.g., Extended Primary users) on the network. During an incident or planned event, broadband networks can become heavily congested as users take to their mobile devices to make calls, send texts, post updates on social media, and stream live video. FirstNet is built to provide priority and preemption for Primary users during these conditions. When there is a potential of extreme network congestion, the Uplift Request Tool is a supplemental resource that may be used to elevate specific users for a temporary period. Uplift is typically intended for Extended Primary users that provide support to Primary public safety entities.

The importance of Uplift

While Primary users have always-on FirstNet priority and preemption for all communications, Extended Primary users may or may not have prioritized access depending on the FirstNet plan in which they are enrolled. Extended Primary users can be temporarily granted priority and preemption status on FirstNet through a process called "uplift."

For an Extended Primary user, uplift temporarily provides the same level of priority and preemption as a Primary user.

Uplifting Extended Primary agency devices must be coordinated through an Uplift Manager from a Primary agency. Under FirstNet Authority and AT&T policy, Extended Primary agencies are not able to uplift their own devices. Therefore, pre-planning with all response and mutual aid partners becomes extremely important to ensure that uplift can be initiated quickly and efficiently for targeted users during an emergency. Depending on the size of the group to be uplifted, the process could take several minutes to complete. However, for most uplift operations, the impact is nearly instant.

For more information on how uplift can be utilized by your agency, contact your **AT&T FirstNet Solution Consultant.**

Requesting Uplift via the FirstNet Assist Mobile App

When an Uplift Request Manager creates an uplift request, FirstNet Assist users who are within a 100-mile radius may view the event and request to be added to the "uplift." An Uplift Request Manager can approve or deny uplift requests from the app. Notifications will be sent to all Uplift Request Managers for the uplift event when users with the FirstNet Assist app submit a request to be added.

Uplift Managers will receive information from the requesting user, including the user's name, phone number, agency, job title, alternate contact number, and skills, as well as notes provided by the requesting user. If the Uplift Request Manager does not act on the request within 15 to 20 minutes, the request will time out, sending a message back to the requesting user and to all Uplift Managers assigned to the event. Any of the Uplift Managers for the event can approve or deny the request before it times out. The requesting user and all Uplift Manager(s) will receive a notification of whether the request is approved or denied. When denying a request, the Uplift Manager must provide a reason for denial and can send notes back to the requesting user with instructions or additional information.

The FirstNet Assist app can be downloaded on a smartphone or tablet (Android or iOS) and requires the device to have a FirstNet SIM or eSIM. Users must have a FirstNet account and will use FirstNet Central login credentials to sign into the app.

Using the Uplift Request Tool

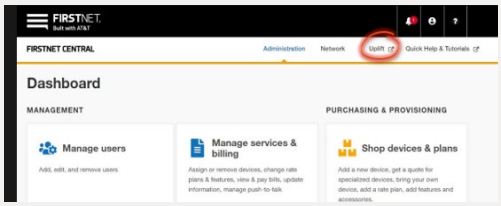
The Uplift Request Tool can be accessed by clicking "Uplift" in the top-right corner of the FirstNet Central home screen. An uplift event can be created and launched immediately or scheduled for a planned event up to one year in advance. An uplift event can be created by an Uplift Manager in any location, and the FirstNet device(s) will be uplifted, regardless of location. Any device provisioned with a FirstNet SIM (phones, tablets, routers/hotspots, and IoT devices) can be uplifted. Any wireless device number that is not eligible for uplift will be ignored and will show a status of "Not Eligible." Any device in a "suspend" status will be uplifted; however, these devices cannot be utilized until they are reactivated by the Agency's Account Administrator. This status will also be reflected in the Uplift Request Tool.

The initial duration of the uplift event can be set for between 1 to 48 hours, and once the event has been activated, it can be extended for up to 30 days. The uplift event cannot be canceled once activated and must expire for the specific device(s) to lose uplifted status.

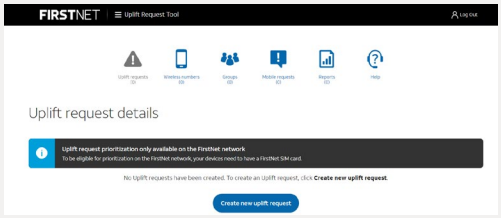
Pro Tip:
Finding Uplift

Simulated image from Advanced Network Status Tool. Red icon shows an impacted tower.

FirstNet Central Home Screen



Uplift Request Tool Screen



Pro Tip:
Using Uplift Effectively

1. Identify Primary (public safety) and Extended Primary (public safety support organization) users and their FirstNet phone numbers.
2. Set up groups in advance using FirstNet Central Uplift Request Tool.
3. Schedule uplift events in advance, using pre-identified groups, locations, and duration.

During normal network activity, an uplift will not necessarily provide a discernible level of higher network performance. Uplifting a device does not impact wireless coverage or throughput speeds.

As with other aspects of the FirstNet network, the Uplift Request Tool can be adapted to meet the needs of your agency. The following are suggested strategies to maximize the use of the Uplift Request Tool.

During steady-state operations

- Create FirstNet Central user accounts for a designated pool of personnel to serve as Uplift Request Manager(s). Toggle on access to the Uplift Request Tool.
- Download the FirstNet Assist app on smartphones and tablets to see nearby uplift events and to request to be uplifted for an event by its respective Uplift Manager. Note: an uplift event cannot be created directly within the app itself.
- Create and regularly update contact groups of users that would potentially be uplifted. Use the Groups function within the Uplift Request Tool and/or download the CSV file template to create desired groups of users.
  - Within an uplift group, consider launching a brief (1 hour) uplift test at least quarterly for a limited number of devices to retain proficiency with using the tool.
- Leverage Uplift Request Tool user guides and instructor-led training resources through Quick Help and Tutorials within FirstNet Central.
- Develop and implement governance, policies, and procedures for the use of the Uplift Request Tool.

Pre-event planning

- Check the Nationwide Scheduled Uplift Requests report to see if an uplift event has been created for a planned event.
  - This report is available in the Uplift Request Tool under the Reports module. The Nationwide Scheduled Uplift can be downloaded in various file formats.
  - If you do not want your planned uplift event to appear in the list of Nationwide Scheduled Uplift Requests (due to the sensitive nature of the event, security reasons, etc.), check the "Exclude from Report" box. This only removes the uplift event from appearing in the report, but when the uplift event becomes active, it is then viewable by users with the FirstNet Assist app if they are within 100 miles of the location.
- Select the desired date and time for the uplift event to ensure all eligible devices are successfully uplifted by the start time.
  - Uplift events can be created up to one year in advance of a planned event. Pre-planned uplift events can be seen in reports and can be accessed by Uplift Managers who were designated when the original uplift request was created.
  - Name the uplift event similar to or the same as the planned event.
  - If you do not want your uplift event to be visible to FirstNet Assist app users (due to the sensitive nature of the event, security reasons, etc.), check the "Make Private" box to prevent the uplift event from being seen by other users. This can be toggled on or off while the uplift event is active, in case the situation changes. Please note, once the scheduled uplift event goes live, it will be visible to FirstNet Assist app users unless the "Make Private" box is checked.
- Periodically review the uplift request prior to the event, ensuring required responders, devices, and mutual aid agencies are included and will be uplifted.
  - A scheduled uplift event can be edited or canceled at any point prior to its launch.

Pro Tip:
Primary and Extended Primary

Primary users include the public safety disciplines of Emergency Communications/9-1-1, Emergency Management, Emergency Medical Services, Fire Service, and Law Enforcement.

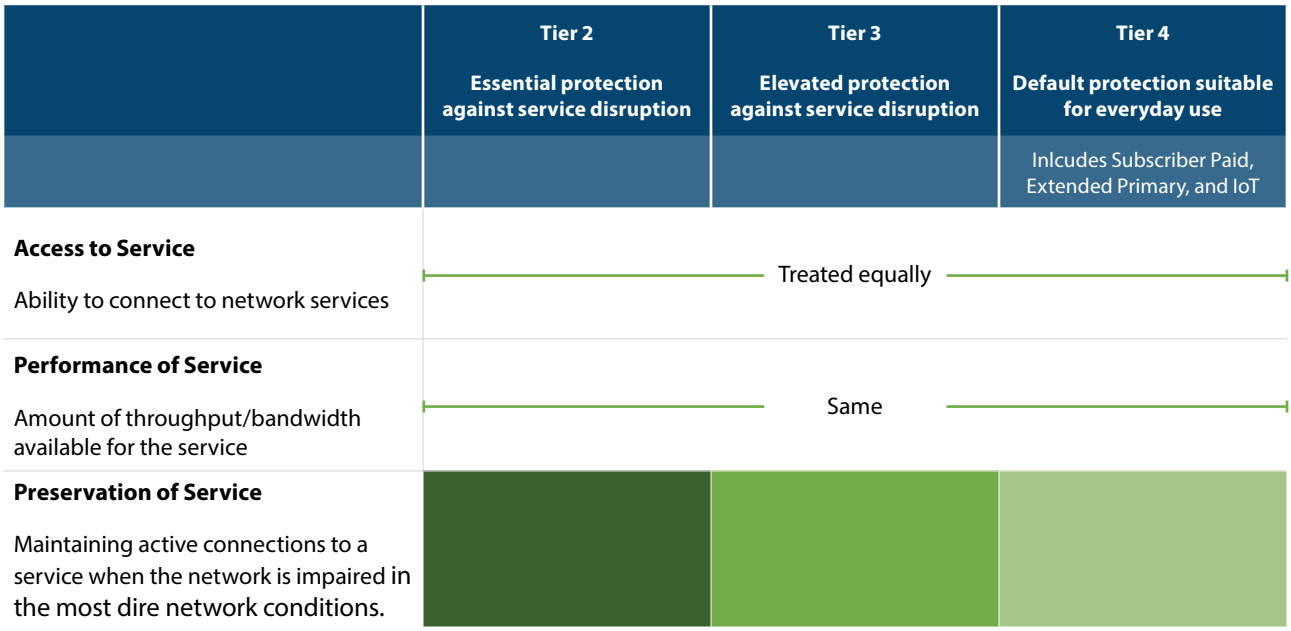
Extended Primary Users are those agencies, organizations, non-profit or for-profit companies that provide public safety services in support of Primary Users. They provide mitigation, remediation, overhaul, clean-up, restoration, or other such services during or after an incident.

Source: **www.firstnet.com/power-of-firstnet/get-started.html**

During incidents/response phase:

- If extreme network congestion in a concentrated area is expected or if Extended Primary entities are supporting response, consider creating an uplift event.
  - Name the uplift event similar to the incident name.
  - During the operational period(s) for an incident or event, the uplift event can be edited, as needed, to add wireless numbers, extend the duration, change the privacy/visibility status, or add Uplift Request Managers.
  - Designate at least two Uplift Request Managers based on the operational period or duration of the incident.

Figure 2: Priority Tier Differentiation



Tier 1, or uplift, is a temporary priority level that provides maximum protection against service disruption. It has the same performance and throughput as primary static levels.

- If an uplift event expires but was needed for a longer period, use the 'Copy' function to duplicate the expired event and quickly activate an identical uplift event.
- Review any uplift requests sent via the FirstNet Assist app.
  - FirstNet Assist App users can view active uplift events within a 100-mile radius of their location and can request to be uplifted if they anticipate network congestion in their location.
  - All active uplift events are visible in the app, except for those marked private.

Any additional questions can be directed to FirstNet Customer Care at 1-800-574-7000, via live chat on the FirstNet.com site, or through the FirstNet Assist app by selecting "Customer Support."

Considerations for using FirstNet Uplift

There is a difference between "priority and preemption" and the four levels of preservation of service:

- FirstNet primary users always have the highest level of priority, preemption, and quality of service on the network, referred to as "First Priority™" or "QPP."
- Priority gives FirstNet users preferred access to network resources.
- Preemption will relocate or terminate non-primary or commercial users if needed to allow FirstNet primary users access (aside from 9-1-1 calls). FirstNet primary users are not pre-emptible. No manual intervention is required.

FirstNet devices are assigned a preservation of service priority tier upon provisioning:

- When a device is provisioned on the FirstNet network, it is assigned the default preservation of service priority level Tier 4 but may also be provisioned at Tier 2 or 3.
- At any time after initial provisioning, an Agency Administrator may elect to modify the setting for Primary Users between Tiers 2-4 as they deem appropriate. Extended Primary and Subscriber Paid Users are fixed at Tier 4, unless uplifted.
- Uplifting an eligible device temporarily elevates it to the highest preservation of service level on the network, also referred to as Tier 1 or "incident level."
- Preservation of service establishes protection for maintaining active connection to a service during extreme circumstances when the network is impaired.

Using FirstNet Uplift for Major Events

FirstNet Uplift is an important capability that is unique to the FirstNet system, giving public safety the option to protect their always-on network connections during major emergencies and large events.

Imagine a scenario where a tornado or earthquake impacts several cell sites in a geographic area, but not all towers are incapacitated. The towers that remain on-air are now serving as the network connection for a much greater area with many more users than they were built to serve under normal circumstances. As a result, these towers may become congested and start to "shed" users to keep up with network capacity demands. Shedding appears to the user like a phone call taking too long to connect, a text message that takes too long to send, or a webpage or application that is slow to load. The network is automatically allocating resources in fractions of a second, trying to serve every user in range of the network.

FirstNet primary users are always connected to the network with priority and preemption. In cases of extreme network congestion, even these users can be shed by the system if it is completely overloaded. By enabling an uplift incident for certain FirstNet numbers, public safety managers can ensure their **key FirstNet users and devices remain connected** to the network even during heavy congestion conditions.

Additionally, uplifting any extended primary users (such as partner agencies like transportation, utilities, water, wastewater, etc.) ensures they have the same priority and preemption in place to communicate with primary public safety agencies during an event.

Uplift events can be staged and scheduled to go into effect at a certain date or time and can be set to last for 1 to 48 hours. Once the uplift has started, it can be extended for up to 48 hrs. If more time is needed, extend it again for up to an additional 48 hrs. For major events, agencies can initiate uplift for their key personnel to ensure their FirstNet connection in the case of an immediate or no-notice emergency incident.

To initiate an uplift event:

1. Users must have uplift manager permissions to create/manage uplift events
2. Log on to the FirstNet Central portal: **localcontrol.firstnet.att.com**
3. Select uplift from the tabs in the top right bar of the screen (users will not see this option if they are not uplift managers)
4. Select "Create a New Uplift Request"
5. Complete the on-screen form to include the name, parameters, and location of the uplift event
6. Add numbers to be uplifted, either manually or by uploading a .CSV file of numbers
7. Add any additional uplift managers who are authorized to make changes to the event
8. Submit

USE CASE

Using the Advanced Network Status Map

Scenario:

A significant ice storm has impacted the Northeast, causing widespread power outages and many road closures caused by debris from fallen trees and power lines. Public safety, transportation and utility crews are responding in force to clear roads and restore essential services, but the impact of the storm is expected to continue for several days. As a result, cellular communication infrastructure is starting to lose battery back-up power and generators are beginning to run out of fuel.

1. Request coverage solution

Public safety needs to communicate from units in the field back to EOCs and ECCs to coordinate response and keep track of personnel and assets. With degrading cell service across a wide area, agencies using FirstNet can request assistance from the Response Operations Group (ROG) in the form of deployable assets and other network enhancements.

2. Identify health of network with Advanced Network Status Tool

The Advanced Network Status Tool (ANST) in FirstNet Central provides public safety users with a near real-time look at the health of the FirstNet network. Users can quickly see and understand where FirstNet service is up and running and where it is not. If storm response and restoration efforts are active in an area where there is no service, public safety can plan ahead and request assistance from ROG to help keep their field teams in communication.

Additionally, cell tower locations are marked on the ANST map and can be compared with road closure and other transportation route information. This helps public safety officials to strategize where to focus road clearing efforts for FirstNet deployable access, so that utilities can be restored, or to bring fuel to generators keeping towers on-air.

The ANST system provides transparency and situational awareness to public safety users so they can efficiently and effectively plan their response operations and enables them to better collaborate with FirstNet ROG to get deployable assistance where and when it is needed most.

MISSION CRITICAL RESOURCES

SECTION 5

Agencies from across Rhode Island used FirstNet-enabled devices to help manage communications between care teams and the emergency communications center during an emergency management exercise at T.F. Green International Airport.

MISSION CRITICAL SERVICES

The **3rd Generation Partnership Project (3GPP)** defines "mission critical" as a communication activity, application, service, or device that requires low latency, high availability and reliability, the ability to handle a large number of users and devices, strong security, and priority and preemption handling.

Within the world of public safety, a tool or service may be deemed "mission critical" when public safety users decide that it is required for successful response operations. The FirstNet Authority works with public safety to assess when and if a tool or service is determined to be mission critical to their operations.

3GPP is a global initiative made up of telecommunication professional organizations that sets standards for public safety communications systems. The FirstNet Authority is actively involved with 3GPP, working to ensure that public safety's needs and requirements are reflected in the standards development process and resulting 3GPP standards. The FirstNet Authority also works to ensure the FirstNet network meets 3GPP standards.

Within 3GPP's definition of Mission Critical Services (MCS), there are three major components that are relevant to public safety: Mission Critical Push-to-Talk (MCPTT), Mission Critical Data (MCData), and Mission Critical Video (MCVideo). FirstNet's mission critical broadband communications can supplement an existing LMR system and help to fill indoor and outdoor coverage gaps, creating a more robust communications capability for public safety users.

The FirstNet ecosystem supports MCS through tailored devices and apps designed for public safety. Agencies should explore Wireless Priority Service and FirstNet device caches to ensure resilient MCS and mutual aid that supports these critical communications.

Mission Critical

Any factor of a system (equipment, process, procedure, software, etc.) that is critical to the success or failure of mission operations.

FirstNet Devices and Applications for Everyday Use

The ecosystem of devices and apps designed for public safety continues to grow as more solutions are developed to meet their operational needs. This section will discuss some of the considerations for selecting devices and apps to take advantage of FirstNet's key benefits.

Selecting FirstNet Ready Devices

Many of today's commonly used devices are certified for use on FirstNet, including smartphones, feature phones, tablets, laptops, Wi-Fi hotspots and modems, and wearable devices such as smartwatches, body cameras, and more. The National Institute of Standards and Technology's (NIST) Public Safety Communications Research Division (PSCR) maintains a **list of these devices**.

To be added to the NIST list of certified devices for FirstNet, a device must have gone through the FirstNet Device Approval Program and been certified by AT&T and accepted by the FirstNet Authority. The FirstNet Device Approval Program ensures devices are compatible with the FirstNet ecosystem. Devices that have a FirstNet Ready badge support access to Band 14 — FirstNet's public safety spectrum — and can work on the FirstNet network simply by installing a FirstNet SIM card.

For public safety officials who evaluate and manage technology for their agency, it is important to look for devices certified for use on FirstNet. Doing so will ensure you are able to take advantage of the network's public-safety-focused features, such as tower-to-core encryption, priority, and preemption. Using FirstNet Ready devices also helps ensure that responders can access FirstNet deployables when they are mobilized in an emergency. This is because FirstNet deployables provide service on Band 14 and FirstNet Ready devices have built-in access to this spectrum.

Using FirstNet Devices on 5G

First responders maintain voice and data communications with priority and preemption on LTE, while the FirstNet network automatically determines the best route for data traffic, whether that's LTE spectrum, 5G, or 5G+. Depending on a responder's location, service plan, and device, they will see one of these indicators: LTE, 5G, or 5G+.

Using millimeter wave spectrum, AT&T 5G+ delivers the fastest speeds in high-traffic areas, including major cities, stadiums, and venues. AT&T is continually rolling out 5G+ locations across the country. Current information on the AT&T 5G+ deployment can be found at: **www.firstnet.com/5G**.

To access 5G on a FirstNet device, FirstNet users can take the following actions:

Pro Tips: Utilizing Apps

FirstNet Verified™

- The app meets criteria for relevancy to public safety
- The app has gone through a vetting process that includes the security, data privacy, and availability (99.9% available) needed for inclusion in the FirstNet App Catalog

FirstNet Certified™

- The app meets the criteria for relevancy, security, and data privacy
- The app also has the increased availability (99.99% available), mobility, resiliency, and scalability to meet public safety demand
- The source code for the app has passed a separate security review process

Emergency Managers should take an inventory of apps being used by mutual aid partners in their county or region.

For Agency-Paid devices:

Visit **FirstNet.com/coverage** for the latest list of 5G/5G+ locations to ensure the area of operation is within the current 5G/5G+ coverage footprint.

Visit **FirstNet.com/devices** to determine if your device is 5G capable or if you'll need to acquire a new device.

Work with the AT&T FirstNet Solution Consultant to be moved from a 4G rate plan to a 5G rate plan; there is no additional charge, but it needs to be adjusted in AT&T's system.

For Subscriber-Paid devices:

Visit **FirstNet.com/coverage** for the latest list of 5G/5G+ locations to ensure the area of operation is within the current 5G/5G+ coverage footprint.

Visit **FirstNet.com/devices** to determine if your device is 5G capable or if you'll need to acquire a new device.

Log in to your **FirstNet account** and modify the rate plan or call FirstNet Customer Care [800-874-7000]. Alternatively, visit a retail store to obtain a 5G-capable device certified for use on FirstNet and move from a 4G to 5G rate plan.

FirstNet App Catalog

FirstNet users have access to the **FirstNet App Catalog**, which identifies pre-approved apps for public safety's use. The apps within the catalog are relevant to the mission of public safety. Every app undergoes a thorough evaluation by an App Review Board with members from both the FirstNet Authority and AT&T. The executable code for all apps is scanned and reviewed by cybersecurity experts at AT&T.

There are two levels of app certification within the catalog:

- FirstNet Verified means the app meets criteria for relevancy to public safety and has gone through a vetting process that includes the security, data privacy, and availability (99.9% available) needed for inclusion in the FirstNet App Catalog.
- FirstNet Certified means the app meets the criteria for relevancy, security, and data privacy, but also has the increased availability (99.99% available), mobility, resiliency, and scalability to meet public safety demands. In addition, to become FirstNet Certified, the source code for the app must pass a separate security review process.

Public safety officials can search for FirstNet Verified and FirstNet Certified apps in categories such as situational awareness, public safety communications tools, in-building coverage and mapping, cybersecurity, cloud solutions, secure connections, device security, and more. The number of apps will continue to grow as more public safety solutions are reviewed and included in the FirstNet App Catalog. As a best practice, agencies should take an inventory of apps being used by mutual aid partners in their county or region. These apps may be available in the FirstNet App Catalog and can be deployed to FirstNet devices.

The FirstNet App Catalog is available at: **FirstNet.com/Apps**.

FirstNet App Developer Portal

Like the expanding device ecosystem, there are also many software apps developed to specifically take advantage of FirstNet's public-safety-focused capabilities. To drive innovation for first responders, FirstNet has a first-of-its-kind **developer portal for public safety apps**.

For example, FirstNet apps include vertical positioning for z-axis mapping, authentication for single sign-on, device and app uplift for heightened network prioritization, and more. Some apps integrate Mission Critical Push-to-Talk and FirstNet Messaging designed specifically for public safety. For more information about the FirstNet App Developer Portal or to submit apps for inclusion in the FirstNet App Catalog, go to **Developer.FirstNet.com/FirstNet**.

Pro Tip: FirstNet and IPAWS

The FirstNet Authority and FEMA's Integrated Public Alert and Warning System (IPAWS) are working together to support alerting authorities and educate and encourage alert and warning software developers to submit their applications to the FirstNet App Developer Portal for testing and certification.

FirstNet and the Integrated Public Alert and Warning System

The FirstNet Authority works with the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System (IPAWS) Program Management Office to support public safety officials who are authorized to send alerts and warnings and to strengthen the nation's alert and warning ecosystem.

FirstNet can be used to support public safety officials in the origination of an alert or warning. To access IPAWS capabilities (including Wireless Emergency Alerts, or WEAs), alert and warning officials are encouraged to use dual-certified IPAWS and FirstNet alert origination software available to public safety in the FirstNet App Catalog. This software helps enhance public safety officials' ability to send the public secure, relevant, timely, and actionable lifesaving alerts and warnings.

WEAs are a different technology than SMS text alerting; they are not affected by network congestion. If, during an emergency, the public cannot make or receive calls or text messages due to network congestion, they will still be able to receive WEAs. FirstNet provides quality of service, priority, and preemption on a reliable, resilient, and secure broadband network so alerting authorities can connect to IPAWS to issue emergency alerts to the public for their awareness and safety.

FirstNet and Wireless Priority Service

Wireless Priority Service (WPS) is an emergency phone service managed by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). WPS supports national leadership; federal, state, local, tribal, and territorial governments; and other authorized national security and emergency preparedness users. It is intended to be used in emergencies or crisis situations when wireless networks are congested and the probability of completing a normal call is reduced. WPS provides pre-authorized personnel priority voice-only access nationwide and several regional cellular networks, greatly increasing the probability of call completion. WPS does not preempt other users and does not provide any additional priority for user data sessions (such as SMS, pictures, etc.). Note: WPS is not the same as Government Emergency Telecommunications Service (GETS), which prioritizes voice calls over wireline networks.

FirstNet users are always given priority access on the FirstNet network; WPS is not needed for calls between FirstNet users. FirstNet subscribers with a FirstNet SIM card or FirstNet eSIM are eligible for WPS and can access both FirstNet and WPS capabilities with a single FirstNet phone. FirstNet users are always given priority access on the FirstNet network; WPS is not needed for calls between FirstNet users. Using WPS in addition to FirstNet supports priority for voice calls to wireless users who aren't on the FirstNet network. Once the FirstNet call traverses another network, it is up to the other carrier to ensure the WPS tag is recognized, and the call is given priority on the non-FirstNet receiving device.

WPS is provided at no additional charge to FirstNet subscribers. Current AT&T WPS users migrating to FirstNet do not need to request WPS for their FirstNet phone as the WPS feature will automatically transfer. Older FirstNet accounts may need to have WPS enabled, so it is best to check with an AT&T account representative to verify that WPS is correctly set up. New FirstNet customers coming from another carrier should request WPS using the standard WPS subscription process.

More information on WPS can be found at **www.cisa.gov/wireless-priority-service-wps**.

Using a FirstNet Device Cache

There are many preparedness measures that public safety communications officials and their partners — in coordination with their information technology staff — can take to improve crisis response. One recommendation is to provision a cache of FirstNet Ready devices that may include smartphones or basic phones, tablets, or wireless internet hotspots. Having these communication tools available for rapid deployment and under the agency's own control and oversight can hasten public safety's ability to respond to an emergency.

Pro Tip: Distributing Devices

If you anticipate distributing devices to mutual aid partners, develop a process for tracking those devices for accountability and to ensure the devices are returned after an event.

Pro Tip: Devices for Deployables

FirstNet deployables **do not** come with a cache of devices on board for agency use. Have a plan for providing devices or hotspot access in advance.

In addition, agencies should consider pre-loading the cache of FirstNet Ready devices with specific applications that their jurisdiction uses, such as push-to-talk communication programs, alerting and notification systems, location-sharing applications, or file-sharing systems. This will allow for enhanced collaboration and reduce traditional barriers to situational awareness. Devices may also have apps that allow them to interwork with the jurisdiction's LMR system, further enhancing the ability of responders to communicate with each other during an event.

The FirstNet App Catalog is a good resource for identifying apps relevant to your mission. See the latest apps at **FirstNet.com/Apps** or see **Section 5: Mission Critical Services**.

Enabling mutual aid during an emergency

Mutual aid forces may include agencies that are not regular partners of the affected jurisdiction. With a cache of FirstNet Ready devices on hand, agencies can rapidly deploy devices when these mutual aid forces arrive on scene, speeding up the ability to communicate and coordinate. Devices that are pre-configured and registered on compatible systems and applications will work together and share information easily with other responders. FirstNet priority and preemption services will ensure that mutual aid partners can communicate on a level playing field with local forces.

It is important to note that when a FirstNet deployable asset has been requested, only FirstNet Ready (Band 14-enabled)

There are many software apps developed to specifically take advantage of FirstNet's public-safety-focused capabilities. To drive innovation for first responders, FirstNet has a first-of-its-kind developer portal for public safety apps.

devices will be able to connect to the deployable and benefit from its provided coverage. Mutual aid partners that are not on FirstNet may need to be given a device from the agency's cache to be able to communicate using the deployable. FirstNet deployables **do not** come with a cache of devices on board for agency use. If you anticipate distributing devices to mutual aid partners, develop a process for tracking those devices and ensure the devices are returned after an event has concluded.

Building a device cache

The first step to building a device cache is identifying the purpose of the cache. Agencies should evaluate which key personnel should be provided with devices and what types of capabilities and functionalities are critical to a successful operation, today and in the future. By understanding where and how their responders operate, agencies can identify technological platforms that meet those needs.

Additional considerations when developing a device cache:

- Device types
  - Determine whether commercial or ruggedized devices are needed to align with personnel operations.
    - What types of working environments do you encounter in your response area?
    - Do law enforcement agents need covert/undercover equipment?
  - Select devices designated as **FirstNet Ready**.
  - Ensure devices are compatible with technology being used by mutual aid partners (e.g., push-to-talk-capable devices and accessories).
  - Ensure devices can connect to other public safety technology used by your agency (e.g., drones, body-worn cameras).
  - Determine whether data-only devices are needed, or if all devices should also have voice capability.
  - Determine what types of data sharing will be required (e.g., video streaming).
- Applications
  - Install apps used by the jurisdiction's agencies.
    - General apps may include those related to mapping, translation, weather, etc.
    - Agency/operational-specific apps may include those related to situational awareness, location services, file sharing, etc.

- Consider specialty apps and/or apps used by mutual aid partners.
- Consider sign-on/access requirements for devices that are not permanently assigned to staff (e.g., distributed to partners/volunteers).

- Methods of communication needed for response
  - Determine voice/text/data capabilities required.
  - Determine push-to-talk applications needed.
  - Determine LMR interconnection required.
  - Conduct signal tests to know how many and what types of devices may be needed, based on data usage and number of connecting devices (e.g., hotspots, larger access points such as mobile routers or in-building devices, CRDs).
- Training on devices/applications that may not be familiar or regularly used
- Cache maintenance and use
  - Identify costs to develop and maintain the cache.
  - Identify the cache storage location.
  - Determine appropriate Point(s) of Contact for access to the cache.
  - Establish a method to track the assignment of cache devices for accountability and demobilization.
  - Maintain and regularly refresh devices.
    - Activate devices prior to an event (e.g., FirstNet Customer Care).
    - If applicable, add cache device numbers to the FirstNet Uplift contact list.
  - Maintain and update apps loaded on devices (e.g., feature updates, security patches)
  - Develop credentialing and access management policies and procedures to ensure users can log into devices that are distributed from the cache.
  - Establish processes to transport the cache.
  - Train with cache devices.

Pro Tip:
Cache Database

We recommend that Emergency Managers create and maintain a database or listing of all available caches in their area for easy reference during an emergency. Pre-plan who you will call to ask for devices, and in what order.

Using FirstNet Ready® devices helps ensure that responders can access FirstNet deployables when they are mobilized in an emergency. FirstNet deployables provide service on Band 14 and FirstNet Ready® devices have built-in access to this spectrum.

PUSH-TO-TALK FOR VOICE AND DATA

Push-to-Talk

PTT applications offer many benefits to FirstNet users, equipping them with real-time data and voice communications capabilities. Public safety can use PTT applications to communicate and track the location of responders in the field from the EOC or the ECC. They can connect with individuals or entire talk groups to share critical information, such as voice communication, pictures, and video. They can scale the applications based on each incident, creating or expanding talk groups as needed to develop a shared common operating picture of an incident. With access to the FirstNet network, groups and users can be configured over the air within seconds of the administrator making changes, enabling swift operations and response.

With the ability to connect to LMR radio networks, PTT applications further extend and enhance communication capabilities, especially when responders are outside their normal LMR footprint or are working on Wi-Fi within a building or structure.

Several vendors have developed FirstNet Ready™ devices that are dedicated to PTT and have physical PTT buttons, some even with knobs and a look and feel like an LMR radio. These devices can be loaded with MCS applications and have lower monthly cost plans than smartphones. Users can be quickly trained and learn to operate devices that are dedicated to PTT, making them a solid choice for cache devices that may be on hand for events or disaster response.

Additionally, smartphone devices are available with physical PTT and emergency buttons that also allow for easier operations. Many are rugged or semi-rugged and offer accessories such as remote speaker mics. PTT apps are also available on these devices.

Push-to-Talk solutions have many benefits for daily and large-scale incidents:

- **Large-Scale Mutual Aid Connectivity:** Talk groups established among agencies and disciplines can help address common communication challenges mentioned in After-Action Reports (AARs). MCPTT Task force operations can benefit from this communication when their agencies may use different communication

solutions. For example, a leadership group across public safety and a municipality (e.g., police chief, fire chief, mayor) can maintain quick and direct contact, even allowing seamless communication when traveling outside the area. In some cases, jurisdiction leadership may not require a hardened, public safety-grade communication device when a simple smartphone with PTT would suffice.

- **LMR-Broadband Integration:** PTT can integrate with traditional LMR to maintain a critical connection across a public safety organization, with dispatch and other public safety organizations, and with partners like schools and power and utility companies. It allows command staff, supervisors, and responders to communicate directly to their current LMR talk groups and channels, allowing for smoother incident management. It can also free up LMR capacity.
- **Extended Operational Reach:** Agencies have reported extended coverage and reach of the FirstNet network, especially in areas known to have connectivity challenges. PTT can also help responders keep in touch even when LMR might not have coverage, for example inside buildings or in the basement of a parking garage where LMR signals have difficulty reaching. PTT over Wi-Fi can enable communications from beyond the agency's geographic LMR footprint, literally providing the ability to communicate from anywhere in the world where Wi-Fi is available.
- **Specialized Team Applicability:** There are many teams or job functions that can achieve special benefits from PTT talk group solutions, such as tactical teams, undercover officers (who cannot carry radios), and task forces. Additionally, other support teams, like facilities and fleet management, can be better integrated in communications even when radio access is unnecessary or financially not feasible.
- **Web Dispatch:** A PTT web dispatch client ensures the ECC stays integrated with on-going PTT operations. Like LMR-type consoles, the web dispatch offers telecommunicators call recording, playback, and multiple talk group modules that have separate volume controls and can be routed to different speakers. In addition to traditional features, the web dispatch console includes video streaming, location tracking, and geofence capabilities. Geofences can be used to monitor users crossing into or out of the geofence, along with defining area-based talk groups. The web dispatch client can be used in any environment, including on-the-go, in a communications vehicle, in an EOC, or in incident command.

Cellular – LMR Interworking

As MCS applications have evolved, public safety agencies have been vocal about the ability to integrate MCPTT into their current LMR systems. Integrating broadband into LMR provides flexibility and interworking for operations.

The benefits include:

- **Expanded coverage:** Users benefit by having both LMR and broadband coverage. Devices connected to Wi-Fi can also communicate to an LMR network.
- **Optimization of LMR resources:** Non-emergency talk groups can utilize broadband, leaving LMR capacity for critical communications.
- **Over-the-air programming:** Web-based admin portals allow for easy user and talk group configuration, including the ability to rapidly add users to LMR connected talk groups.
- **Streamlining of devices:** LMR-broadband integration utilizes the smartphones carried by nearly every responder, reducing the need for large caches of expensive LMR devices for mutual aid events.

FirstNet supports LMR-broadband interoperability through:

- **Radio over IP (RoIP) gateway technology:** This is a lower cost option to extend agency communications. It allows users to remain in contact with personnel who travel outside the agency's LMR footprint and frees up capacity on the LMR network. This functionality can be achieved with as little as a single LMR radio connected to the RoIP gateway device.
- **Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI):** These P25 standards-based solutions have more features. For example, they support the ability to pass through "emergency button" activations, to see the unit ID/alias of a user, and to map multiple talk groups between an MCS service on FirstNet and an LMR network. These methods are more complicated and costly, however.

Interworking solutions are evolving and expected to continue to add capabilities in the coming years.

Interoperability with other Agencies and Carriers

Working within your region to standardize your use of FirstNet, determining MCS solutions/applications to integrate, and establishing regional governance agreements will ensure stronger communications among agencies. You will find the same benefits with a regional MCS solution. Because FirstNet is available nationwide, there are no restrictions on how small or large your region is. FirstNet MCS solutions allow calls between all users and talk groups across agencies.

Most agencies already have interoperability with their neighboring agencies via their existing LMR systems. When adding MCS PTT to your existing LMR system, your agency enhances the interoperability you have already established with your neighboring agencies.

If your neighboring agencies have not yet moved to FirstNet, there are ways to communicate in the interim. Cross-carrier licenses allow users that are operating on other carriers to be part of the FirstNet Rapid Response MCS solution. Cross-carrier users will have access to the same talk groups, but the priority of their calls will be based on the level of service their carrier is providing.

When the network is at the highest traffic level during a response, MCS communications have the highest priority. A mutual aid talk group framework can be put in place, allowing incident command and users to easily identify talk groups and use MCS communications during incident response. Listing easily identified talk groups that all responders can utilize in the Incident Communications Plan (e.g., ICS 205) is crucial for an efficient response. DHS/CISA's SAFECOM program and the National Council of Statewide Interoperability Coordinators (NCSWIC), working with the FirstNet Authority, recently published a framework for naming MCPTT talk groups. Read more here: insert link when available

For public safety users, these functions can be critical to incorporating mutual aid resources, especially from outside the area through EMAC. For example, responses to wildfires, major flooding, tornadoes, or hurricanes often involve responders deploying from far away states. Because FirstNet is available nationwide, these responders can hit the ground running with their regular communication methods and quickly be integrated into the host state/agency's communications systems.

Devices, Accessories, and Ecosystem for MCS

Devices and accessories with the MCS service can be just as important as the service itself. Frontline users want to use devices and accessories that can be manipulated with muscle memory. Those devices allow them to keep their heads up and focused on the mission, while communication is second nature (e.g., turning a knob, pushing a button). Typically, these are LMRs with FirstNet capability or devices with knobs and buttons that are dedicated to PTT. Command staff and other responders may use MCS in an application on a smartphone, especially when paired with a remote speaker mic.

It is recommended to allot adequate and appropriate time for trying out device and accessory options. It is also recommended to spend time assessing the configuration and applications being used with the MCS solution selected so you can ensure the combined solution meets the users' mission for PTT communications.

Hybrid LMR FirstNet Devices

Hybrid LMR FirstNet devices are LMRs with FirstNet capabilities built in. Responders may prefer these devices because they can be controlled with muscle memory, allowing the responder to focus on the mission.

Both leading P25 LMR vendors offer proprietary solutions that allow their LMRs to be leveraged on FirstNet with direct connections to the P25 network. One vendor offers a line of devices that are compatible with PTT applications. While using these devices in MCS mode on FirstNet, their communications have higher priority just like other MCS devices on FirstNet. They are purpose-built for public safety with a full line of accessories and installation options for all types of use cases.

Smartphones

MCS client applications can be downloaded from the device's own app store and through the FirstNet App Catalog. This enables you to communicate on your existing device.

Make sure that the MCS app(s) work well with other applications in meeting your mission. We recommend a mobile device management (MDM) solution when using a smartphone to ensure MCS and relevant settings are updated when a new MCS version, device, or accessory is available.

Prioritized service enables first responders to access network resources during times of high network congestion. When hundreds of thousands of people gathered in Times Square on New Year's Eve, FirstNet gave first responders the resources they needed.

Accessories

Accessories can be just as important to the operation as the service and device. For example, if responders require in-ear accessories for privacy or loud noise environments, choose a service/device combination that works with in-ear accessories. Take into consideration the operational environments your team faces when selecting appropriate accessories.

Ecosystem

Understanding what is needed and works best for your mission is an important step in choosing an MCS solution. When considering MCS, evaluate your operational needs, such as vehicle solutions and logging/recording, and specific accessories your team will need, like vehicle docking stations and multi-bay charger.

If your MCS solution is connected to LMR, the LMR system will typically record your calls. If talkgroups are not tied to the LMR system, you can use RoIP for an analog interface to your logging recorder.

Devices, accessories, and the ecosystem to support MCS are continually evolving. As more users adopt MCS, more vendors and solutions will be offered in the marketplace.

During the pandemic, Alexandria, Virginia, 9-1-1 dispatchers and call takers began using FirstNet hotspots and devices to work from home. These practices have been permanently adopted, allowing staff to quickly set up and support operations.

DATA MANAGEMENT

The FirstNet network allows public safety to send information to the field, access Department of Justice information sources, and capture information from the field that otherwise may not be documented.

Secure Exchange of Data and Justice Data

When an officer approaches a car at a traffic stop or knocks on a house door, having information is helpful. Is the car stolen? Does the person on the other side have a history of fighting with police or have firearm violations? Having the information in a matter of seconds helps officers perform their jobs more effectively while staying safe.

The smartphone carried by most officers is becoming a real-time crime center with vital information. Through a partnership between FirstNet Authority and the FBI and years of collaboration with the Criminal Justice Information System (CJIS), public safety at all levels (federal, state, local and tribal) have access to critical data sets through mobile devices. Responders can pull or submit information to the FBI or state and local agencies' data sets for response and investigations. Connectivity in the field is vital to help public safety officials capture information that might otherwise be missed, such as images of important items, threats to public safety, the individual, or members of the public, medical information, and so on.

As agencies continue to integrate broadband devices and capabilities into operations, they must also adapt to managing evidence collected in the field by mobile devices. Using FirstNet-connected devices, responders can collect and process evidence such as crime scene photos, digital information obtained from other sources (e.g., private video cameras, paper photographs and documents at the scene, witness smartphones), infrared and night-vision images, and aerial drone data. Agencies must be prepared to preserve the chain of evidence for investigation and prosecution.

Analytics and AI

Public safety has been using analytics for many years. Artificial intelligence (AI) is accelerating and changing the ways in which public safety can utilize large and disparate sets of data to improve their operations. By using AI, public safety can analyze vast amounts of data into actionable insights, thereby

enhancing decision-making and operational effectiveness. We are just starting to see the future that will allow for real-time integration and analysis of information to enable a complete picture to be pushed to the first responder in the field. Today, we have smartphones, tablets, IoT devices, cameras (e.g., closed circuit television [CCTV], security, body-worn cameras [BWCs], traffic, drones, dashboard), and acoustic detection devices that can be pulled in for AI and analytics. In the future there may be additional data from smart city grids, connected sensors, and more.

Analytics and AI present an opportunity to deliver the information you need in the moment — whether on a daily patrol or responding to an emergency incident. This information can help you make critical decisions and send alerts to supervisors and responders when a dangerous situation emerges.

By leveraging the robust capabilities of the FirstNet network, public safety agencies can access real-time data from various sources, including sensors, cameras, and communication systems, allowing for advanced analytics that identify patterns, predict incidents, and optimize resource allocation. For example, predictive analytics can forecast potential crime hotspots or assess the likelihood of emergencies based on historical data, enabling agencies to allocate personnel and resources more strategically. AI-driven tools can analyze video footage for real-time threat detection or automate reporting processes through speech-to-text reporting or voice-annotated video from a BWC, freeing responders to focus on critical tasks.

To effectively operationalize analytics and AI, public safety agencies should invest in training personnel on data interpretation and AI technologies, establish cross-agency collaboration for data sharing, and implement robust data governance frameworks. By embracing these technologies, public safety organizations can enhance their situational awareness, improve community safety, and foster a proactive approach to public safety operations.

Real-Time Crime Centers

Real-time crime centers (RTCCs) serve as a hub for data exchange with the field and decision-makers operating out of a command post or headquarters location. RTCCs are often established by law enforcement but frequently bring in other public safety disciplines to share situational awareness and to help create a common operating picture. They rely on various data sources coming from devices carried by officers, in vehicles, and around the community that often rely on a broadband connection to fast track that information to the crime center or responder in the field. Examples of devices and data include CCTV, BWC, geolocation data, and automated license plate readers, which are used to help identify crime patterns and aid investigations.

USE CASE

Using MCPTT and License Caching During a Wildfire

Scenario:

A rapidly expanding wildfire is impacting the region, causing mutual aid responders to come into the area to assist with response. This scenario highlights the practical application of MCPTT and license caching in a high-stakes emergency, ensuring robust communication and interoperability across diverse agencies and challenging environments.

1. Deployment of PTT using FirstNet Central and Rapid Response

While many responding agencies have FirstNet-compatible devices, some have devices from other carriers provisioned with FirstNet SIMs or other carrier SIMS. The PTT application may be pre-installed from prior events or configured on the scene by downloading the mission-critical application from their device's app store. Coordinating agencies can purchase and maintain a cache of prepaid cross-carrier licenses ready for issuance to individual responders for the event.

Benefits:

- End-to-end encryption for secure communications
- Everyone has a cell phone (either personal or issued by their department or agency)
- Group calls for coordinating across agencies/functions (e.g., fire command, law enforcement, logistics)
- One-to-one calls for direct communication between incident commanders
- Integration with dispatch consoles for real-time updates to the command center
- LMR-LTE integration into the communication application among agencies with a radio channel established for the event

2. Cached License Model for Interoperability

A cached license management system is implemented to address interoperability. This system allows devices to operate PTT functions regardless of carrier, creating instant interoperability with LTE and LMR if desired.

How It Works:

- Each agency's devices are set up with a temporary, locally cached PTT license managed by a FirstNet Central Administrator; this can be preloaded or installed on scene. These licenses can be assigned for a set period (e.g., 72 hours). They allow access to PTT services without continuous authentication to the FirstNet core network, enabling devices from other carriers to participate in the PTT talkgroups with FirstNet users.
- Licenses are pre-distributed to devices via a secure onboarding process at a staging area with reliable connectivity (e.g., a mobile command post)

- Interoperability is achieved by mapping agency-specific talk groups to a unified PTT group structure. For example, a local fire department's LMR talk group is bridged to a FirstNet PTT LTE group via an Inter-RF Subsystem Interface (ISSI or ROIP), allowing seamless communication with everyone on LTE devices.

Benefits:

- Agencies with different radio systems (e.g., P25 LMR for fire), can join the same PTT groups, reducing silos.
- Additional responders (e.g., mutual aid) can be onboarded quickly by issuing cached licenses at the staging area.
- Talk groups can be created quickly if more are needed.
- Responders can use cell phones to communicate with LMR devices.

3. Operational Execution

Incident Command Setup:

A unified incident command post (ICP) is established near the fire perimeter, equipped with a FirstNet deployable asset (i.e., Cell on Wheels, or COW) to provide Band 14 LTE coverage. The ICP serves as the hub for license distribution and PTT group management. In the case of good Macro coverage, the COW may be on standby in case it is needed.

Initial Response:

- Firefighters on the front lines use FirstNet PTT to coordinate containment efforts. Their devices, pre-loaded with cached licenses, are sent to the command center to obtain a license from the FirstNet Central Administrator in less than 10 minutes for each device.
- The sheriff's office, patrolling evacuation routes, joins the same PTT group as firefighters, receiving real-time updates on fire spread and road closures.
- National Guard units deployed for logistics and medical evacuation use PTT to communicate with FEMA teams coordinating federal aid.

Connectivity Challenges:

- In a remote valley without cellular coverage, firefighters rely on LMR to maintain communication within their team. A portable FirstNet Satellite Cell on Light Truck (SatCOLT) is later deployed to restore connectivity, syncing licenses with the FirstNet core network.
- Legacy LMR users (e.g., a rural fire department) are integrated via a gateway device that bridges their P25 radios to the FirstNet PTT network, allowing them to join the unified talk group.

Dynamic Scaling:

- As the fire grows, mutual aid arrives from neighboring counties. New responders are issued compatible devices at the ICP, where cached licenses are provisioned in minutes, enabling immediate integration into the PTT network.

4. Outcome

The use of FirstNet PTT with cached licenses ensures uninterrupted, interoperable communications. Key successes:

- **Rapid Coordination:** Real-time PTT communication enables firefighters to contain the spread of fire, while law enforcement safely evacuates residents.
- **Resilience:** Cached licenses allow responders to operate using cellular devices if LMR radios are unavailable.
- **Interoperability:** Bridging LMR and LTE systems via PTT eliminates communication barriers.
- **Scalability:** The ability to quickly onboard additional responders ensures the operation adapts to the fire's escalation.
- **Just-in-time management:** Licenses are deactivated after the event concludes and made available for the next event.
- **Accountability management:** Agencies do not need to gather issued devices after the event.

By leveraging MCPTT capabilities and a cached license model, the multi-agency task force effectively mitigates the wildfire, protecting lives and property while demonstrating the power of modern, interoperable public safety communications.

PEOPLE AND ASSET MANAGEMENT

SECTION 6

The Hyannis Fire Department turned to FirstNet to connect personnel. FirstNet supports the department through hotspots, agency cell phones, tablets, and wireless routers on fire apparatus.

PEOPLE AND ASSET MANAGEMENT

Sensors

Many sensors deployed by public safety agencies can be operated as FirstNet IoT devices, enabling agencies to gather and analyze real-time data. These sensors can include a wide range of technologies such as environmental monitors, shot detection systems, and biometric sensors, each providing critical information that can be transmitted securely over the FirstNet network. By integrating these sensors into operations, public safety agencies can create a comprehensive data-driven network that enhances their situational awareness, resource allocation, and decision making; ultimately, this leads to better outcomes for the communities they serve.

Shot Detection

ECCs and RTCCs can monitor alerts and video footage from shot detection devices in their operations centers. FirstNet enables public safety officers in the field to view this same information from their mobile devices. With reliable connectivity on mobile devices, this data is shared in real time, enabling faster response times.

This allows for greater success in apprehending suspects, collecting bullet casings and other evidence, and interviewing witnesses to result in more successful investigations. Ultimately, this helps to reduce gun crimes and violent crimes in communities.

Air Monitors

Air monitors provide real-time data on air quality and environmental conditions. These monitors can detect harmful pollutants, particulate matter, and other hazardous substances, offering critical insights that inform emergency responders about potential health risks during incidents such

as natural disasters, industrial accidents, or chemical spills. Leveraging the FirstNet network, air monitors can securely transmit data to command centers and field personnel, enabling timely assessments and informed decision making. With these technologies, public safety agencies can safeguard the health of their community and responders, as well as enhance their preparedness and response strategies.

Biometric Sensors

Biometric sensors can monitor vital signs such as heart rate, blood pressure, and oxygen levels. They can also detect falls, enabling first responders to assess the health status of individuals in real-time, particularly in emergency medical scenarios. By integrating FirstNet with biometric sensors, agencies can ensure that critical health information is securely transmitted to medical personnel and incident commanders, allowing for timely medical interventions and resource allocation.

Additionally, biometric sensors can be employed to enhance situational awareness during high-stress incidents, providing valuable insights into the physiological responses of both responders and individuals in distress.

Equipment Monitors

Equipment monitors provide real-time data on the status and performance of critical equipment and resources. These monitors can track various metrics, such as operational efficiency, maintenance needs, and environmental conditions affecting equipment, ensuring that responders' tools are functioning correctly. By utilizing the secure and prioritized communications capabilities of the FirstNet network, equipment monitors facilitate the seamless transmission of data to command centers, enabling proactive maintenance and timely repairs before equipment failures occur. This capability is especially crucial during emergencies, where the reliability of equipment can significantly impact response effectiveness.

Location-Based Services/Mapping

Location-based services refer to the ability to accurately locate people, vehicles, or other resources. Determining and visualizing the location of responders in near real time is a key component of situational awareness that can enhance personnel safety and accountability, improve the effectiveness of incident management, and potentially reduce response times.

Location-based services can be used in both indoor and outdoor environments and have the potential to identify locations in both 2D (horizontal, or X and Y axes) and 3D (vertical, or Z-axis). Indoor locations present unique challenges when it comes to mapping and determining the accurate location of a resource. The FirstNet network supports a variety of solutions and applications capable of delivering location information.

With FirstNet and applications such as **Response for FirstNet** or **Team Awareness Kit** (TAK), users can view the vertical location of a first responder. The information can be displayed and shared on mobile devices and through web browsers.

FirstNet Z-axis is measured as "height above terrain." The application shows the Z-axis location by providing an altitude measurement to X and Y locations using barometric pressure sensors in the user's device. It can help to locate first responders indoors and in multi-storied buildings. The capability is currently **available in over 100** geographic areas across the country.

Video

Internet Protocol (IP)-based cameras provide real-time surveillance capabilities, which can improve incident response. Unlike traditional analog systems, IP-based cameras transmit high-resolution video over a network, allowing for centralized monitoring and easier integration with advanced technologies such as facial recognition, motion detection, and AI analytics. These features enable public safety agencies to identify threats quickly, track suspicious activities, and respond to emergencies more efficiently.

The scalability and flexibility of IP-based systems make them ideal for covering large public areas such as streets, parks, transportation hubs, and event venues. Cameras can be easily installed, repositioned, and monitored remotely, reducing the need for constant physical presence. Additionally, footage can be stored digitally, enabling quick access to historical data for investigations and legal proceedings.

IP-based camera systems can be used to provide real-time situational awareness. Some examples of this include:

- Unmanned Aerial Systems (UAS) devices equipped with this technology can be used in missing person searches, including using infrared technology to locate victims in the dark.
- Remote video of a hazardous materials scene can aid in product identification and status without risking human exposure.
- Identification of perimeters can aid in developing a wildland fire suppression strategy.
- Real-time surveillance of target locations can allow first responders to better monitor crowds for potential criminal activity.

Many jurisdictions have adopted IP-based systems to monitor vehicular traffic, combining video with data collection, for a variety of operational needs. One type of system is

automated license plate readers (ALPRs), which capture and record the license plates of vehicles that pass by. Using high-resolution imaging and infrared sensors, they can work in nearly all light and weather conditions. In addition to the license plate, they can capture other vehicle characteristics such as vehicle make, color, style, time and location of detection, and uniquely identifiable features such as decals or body damage. These systems can take the collected data and make a real-time comparison with existing information sources, such as stolen vehicles or AMBER alert databases, to provide immediate alerts to authorities.

Body-Worn Cameras

BWCs are an important example of "wearable" devices — technology tools we carry on our bodies and uniforms. FirstNet's secure, prioritized network connection is helping provide livestreaming and real-time connectivity for BWCs and other devices.

With BWCs, supervisors can see what is happening before they arrive on the scene. This is especially valuable in chaotic situations when the responding officer has not been able to provide an update. Supervisors can also more effectively deploy their team based on real-time insights. Some agencies are using livestreaming on every call and use their telecommunicators to provide another set of eyes. Agencies are noticing that the livestreaming continues even when other communications become unavailable. Over time, livestreamed video has gained support from many first responders in the field and helped to build trust with communities.

The integration of BWCs with the FirstNet Ready device cache significantly enhances the operational capabilities of public safety agencies. By maintaining a cache of FirstNet Ready BWCs, agencies ensure that their responders have immediate access to reliable, high-quality video recording devices that are optimized for use on the FirstNet network. These cameras not only provide vital real-time situational awareness but also allow for secure video transmission over FirstNet, ensuring that footage can be shared instantly with command centers and other responders. Furthermore, by pre-loading these devices with essential applications, agencies can streamline the deployment process during emergencies, enabling first responders to focus on their critical tasks with confidence in their equipment's capabilities. This proactive approach to technology integration supports enhanced accountability, transparency, and operational effectiveness in public safety responses.

BWCs require more network resources than voice and data transmissions, and so it's a best practice to manage the use of BWCs in large-scale events to make the best utilization of the bandwidth and providing the needed situational awareness. This balance of providing operational

Livestreamed video feeds over FirstNet

Livestreamed video feeds over FirstNet have enabled many benefits to using BWCs for responder safety across all disciplines, including:

Team Coordination:

With BWCs, 9-1-1 telecommunicators can better participate in the response taking place in the field and may improve their understanding of the situation.

Officer Safety:

Video images of the surroundings can help determine the location of the officer. For example, an officer may be in an altercation, but unable to communicate their location. By livestreaming their BWC, their team can identify the officer inside a parking structure and use the footage to look for signs with the floor and position. With that visual information, the team can send help faster.

Hands-Free and Unseen Assistance:

The telecommunicators and supervisors watching the live feeds can provide another set of eyes. When the officer may be focused on the primary subject, the telecommunicator might see a threat, such as a weapon in the back seat or a car passenger reaching for a weapon. Additionally, the telecommunicators can verbally communicate valuable information to the officer without the subject knowing. They can view a driver's license if the officer holds it close to the BWC and reference information to provide further information on the individual and report it back. All of this happens without the officers taking their focus away from the situation and without the subject's awareness of the information being provided.

Location Tracking:

If you know where your officers are located, you can know where to send additional resources or get them help.

FirstNet Compact Rapid Deployables (CRDs) are built to be easily transported and quickly set up. When Hurricane Ian hit Florida, roadways to Sanibel Island were destroyed, so a CRD was brought to the island via boat — providing responders with critical connectivity.

visibility and bandwidth utilization will ensure an optimal user experience and operational outcome during these infrequent large-scale emergencies.

Automatic License Plate Readers

The use of automatic license plate readers (ALPRs) and security cameras is rapidly expanding as communities look for solutions to combat crime with reduced law enforcement staffing. These cameras can be fixed or mobile assets. When they are mobile, like in a vehicle or as a portable kit, they rely on a broadband connection to relay their video feed. The ALPR cameras are also being used by private facilities. In some cases, these private facilities sign agreements to provide law enforcement access to that video for individual incidents or in a live feed.

The real-time transmission of data allows for better, more informed response and faster investigations, but it also enables the ALPR solutions to scan license plate numbers in real time and compare the data against databases to rapidly identify vehicles of concern (e.g., stolen, associated with a crime). Some communities are now using ALPR systems to monitor traffic flows and congestion, which can be a significant advantage for managing numbers of travelers in compact areas, during major events, or when managing evacuation of a geographic area.

Unmanned Aerial Systems

Uncrewed aerial systems (UASs), or "drones," offer public safety a powerful tool for enhancing situational awareness and operational efficiency during emergency response. FirstNet enabled drone systems provide access to advanced aerial capabilities that allow first responders to quickly and effectively assess a situation from the air, sometimes resolving the emergency call without having to send a responder on the ground. These drones provide real-time video feeds, aerial imagery, and data collection during critical incidents, allowing for better decision-making and resource allocation. The integration with FirstNet ensures that the drone's data transmission is secure and prioritized, so that aerial units can seamlessly communicate with ground personnel. By pre-configuring these drones for quick deployment and equipping them with essential applications, agencies can effectively use this technology to assess disaster scenes, conduct search and rescue operations, and monitor large events. Utilizing drone programs, agencies can gather critical information from hard-to-reach or hazardous areas, providing real-time data to incident commanders

As with BWCs, drones transmitting video also require a significant amount of network resources. Therefore, at large-scale events drone video feeds should be managed closely. One recommendation is to develop drone management

Drones as a First Responder programs enable rapid assessment of situations, provide advance situational awareness, and in some cases allow the incident to be resolved without having to dispatch a field responder at all.

tactics as a part of mutual aid agreements to ensure all agencies have a complete understanding of how drone deployments will be managed during these incidents.

Drones as a First Responder

Drones as a First Responder (DFR) programs can significantly enhance emergency response to a 9-1-1 call. Agencies are creating DFR programs to enable rapid assessment of emergency situations, providing advance situational awareness to responders en route to the incident, and in some cases allowing the incident to be resolved without having to dispatch a field responder at all. These programs often rely on broadband connectivity for real-time command and control and camera feeds.

When instituting a DFR program, agencies should focus on training first teleoperators to operate drones effectively, so they can leverage aerial technology for applications, such as incident assessment, coordination with dispatched resources, search and rescue missions, and crowd management during large events. Through DFR programs, agencies can gather and disseminate real time video so responders have advanced situational awareness to be more readily able to respond to a call for service. Furthermore, these programs can foster collaboration among various public safety agencies and disciplines, allowing for coordinated drone operations that enhance mutual aid efforts during large-scale incidents. Implementing a DFR program not only optimizes resource allocation but also establishes a forward-thinking approach to public safety that embraces innovative technology for improved community safety and resilience.

Additional ways that drones are being used by public safety teams include:

- **Tactical Crisis Response:** Drones can be sent into homes, businesses, and other buildings and tight spaces to gain better situational awareness before officers put themselves at risk. There are many examples of barricaded individuals surrendering to drones. Additionally, there are drones outfitted with capabilities to break through windows or doors or to breech buildings.
- **Covering Territory:** For rural areas, drones can act as a force multiplier when responders must cover miles of territory. In border areas, drones can help respond to sensor alerts and identify smuggling routes. For a major metro area drones can aid in surveying large areas like parks where it is hard to provide adequate ground patrol but can be a crime hot spot.
- **Identifying Suspicious Activity:** With real-time video analytics, infrared, and other visual detection systems, drone video can identify where activities are outside the

normal, where activities appear to be criminal, where people might be hiding or seeking shelter, and even identifying when there are concerning contents (e.g., drugs, trafficked people, weapons, explosive devices) in containers, backpacks, luggage, or vehicles.

- **Pursuit Options:** Drones can allow criminals to be identified and followed without high-speed pursuits and without the awareness of criminals. This can increase safety for officers and the community and increase successful identification and apprehension.
- **Patrol:** With drones on continuing patrol, they might identify a crime before anyone calls 9-1-1, including intoxicated driving, carjacking, break-ins, and robberies. They can even create opportunities to stop a crime in progress.
- **Transport of Critical Life-Saving Supplies:** Blood, medications, defibrillators, and other supplies can be delivered where they are needed and with a faster response time than other ground transportation options.
- **Finding Missing People:** Drones can more easily navigate across difficult terrain and survey a larger amount of territory. They can also be outfitted with additional detection technologies (e.g., infrared, night vision, heat sensors), including those that can ping for broadband devices on the missing person. Additionally, they can be a forward observer before rescuers navigate into difficult terrain.
- **Crowd Management:** Drones can aid in the dispersal of a large crowd and by monitoring a large event to quickly identify troubling situations.

USE CASE:

Coordinated Pursuit of Armed Suspect Using TAK for Shared Situational Awareness

Scenario

An armed suspect flees on foot into a suburban neighborhood following a violent incident. Multiple law enforcement officers are deployed to locate and apprehend the suspect. To coordinate the operation, the agency uses the **Team Awareness Kit (TAK)** platform, enhanced by two key plugins:

- The **Wide Area Search Plugin (WASP)** to coordinate systematic ground search efforts
- The **UAS Tool Plugin** enables drone operators to deliver real-time full-motion video to the command and search teams.

Objectives

- Safely locate and intercept the suspect while minimizing risk to officers and civilians.
- Coordinate the actions of multiple responding officers across a dynamic environment.
- Leverage aerial support via drones for overwatch and suspect tracking.
- Use WASP to manage search areas and team assignments.
- Enhance drone operator effectiveness through immersive virtual reality overlays of TAK data.

TAK-Inspired Scenario Flow

1. Initial Incident Response

Officers respond and activate TAK on their mobile devices. The **Command Center** places a **Last Known Location** marker where the suspect was last seen. Officers report real-time updates (e.g., visual contact, gunfire, movement), which are immediately reflected across the shared TAK map using standardized markers and chat.

2. WASP-Assisted Ground Search Coordination

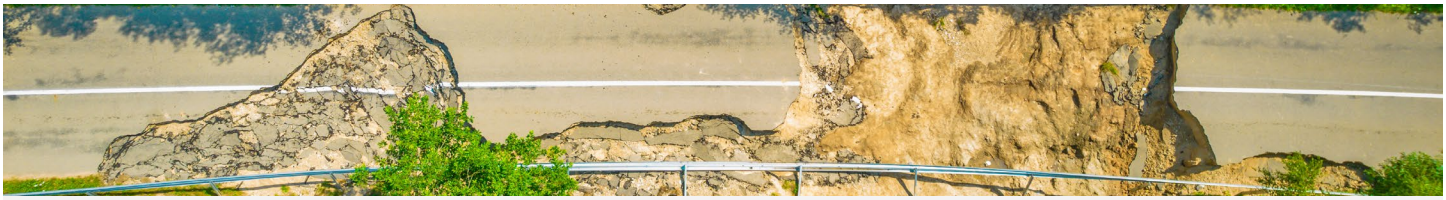
The Command Center uses the **WASP Plugin** to divide the search area into manageable **grids or zones**; this approach is typically used in post-disaster search and rescue operations, but it can be adapted for tactical containment. Officers are assigned to specific grids within TAK. WASP tracks which zones have been cleared, are in progress, or still need attention, minimizing overlap and search gaps. Additional markers are used for known hazards (e.g., civilians, blind spots, potential hiding places).

3. Aerial Surveillance with the UAS Tool Plugin

Drone operators deploy UAS assets and use the **UAS Tool Plugin** to stream video to TAK-connected users and back to command, sharing **live telemetry data** (position, altitude, heading). Drone operators coordinate drone patrols over specific WASP-assigned search zones or dynamic hot zones based on officer reports. Drones assist in covering rooftops, backyards, alleyways, and dense terrain not easily accessible by ground units.

4. Intercept and Containment

A drone operator identifies a suspect moving through a backyard and drops a **"Suspect Spotted"** marker in TAK via the UAS Tool interface. Command reviews the grid status in WASP and reroutes the nearest search team to intercept. Officers use TAK to navigate to the marker via tactical routing. The suspect is successfully intercepted, with the operation captured in the drone's full motion video feed and TAK event log.



USE CASE

Leveraging UAS for Disaster Response

Scenario:

A hurricane makes landfall in Florida travels up the East Coast, settling over western North Carolina as a tropical storm, dropping record levels of rainfall across the region. The unprecedented rainfall causes rivers to overflow isolating communities, destroying portions of the city and homes, as well as impacting infrastructure and basic services. As agencies shift from response to recovery operations, drone teams are deployed to assess roads, rivers, and infrastructure to determine the extent of damages and to develop restoration strategies.

1. Deployment of drones for situational awareness

Drone teams are deployed from local or regional agencies to gather imagery over storm impact and response areas providing near-real time situational awareness to decision makers. Teams may also use other drone sensors, such as LIDAR, to develop photogrammetry to produce 3D images of a scene. The drones can repeat those flights and generate images over time to provide a high level of detail allowing decision makers to see how damage to a bridge or dam may be progressing.

Benefits:

- FirstNet enabled devices provide quality of service, priority, and preemption ensuring connectivity
- Mapping and imagery streaming software transmitted through FirstNet provides the EOC and ECC with situational awareness of flooded rivers, roadways, and impacted bridge systems to identify evacuation and transportation routes.
- Mobile routers using FirstNet enable the sharing of imagery produced in the field between the drone teams and planners to identify areas needing a 3D image. Those images can be used to identify crack propagation in structures and detailed images can be shared over FirstNet across to stakeholders.
- For disaster planning, images taken of critical infrastructure prior to the incident can be compared to post incident imagery to better understand the scale and impact.

2. Information sharing in remote operational areas

Teams in the field require multiple portable options for voice communication, sharing imagery and data, and coordinating operations. FirstNet provides solutions for teams working in comms challenged, austere environments. FirstNet agencies can request the support of the Response Operations Group (ROG), at no cost to the agency, to bring in assets that provide satellite backhaul.

- If an agency owns a CRD or miniCRD, they can deploy those assets anytime and anywhere using the satellite backhaul (LEO or GEO) to connect teams in the field.
- Responders can be provisioned with FirstNet smartphones, hotspots, or High Powered User Equipment (HPUE) modems to stream imagery and coordinate the search. HPUE devices help to provide better coverage in rural areas and optimize the user experience at the cell edge.
- Drone teams deployed in remote regions where radio connectivity is impacted by mountains or long distances can use push-to-talk providing communication, data sharing, and location services over FirstNet.

3. Information Sharing

Drone imagery can be used to identify what evacuation routes are available to the public and responders, provide damage assessments, and shared with PIOs and Government Officials to give context to their briefing and social media posts.

- Government officials have access to FirstNet, providing them with quality of service (QoS) and priority for information sharing and critical communications.
- FirstNet SatCOLTs and CRDs enable communication and distribution of information from remote base camps such that those communicating with the public have accurate and timely information.

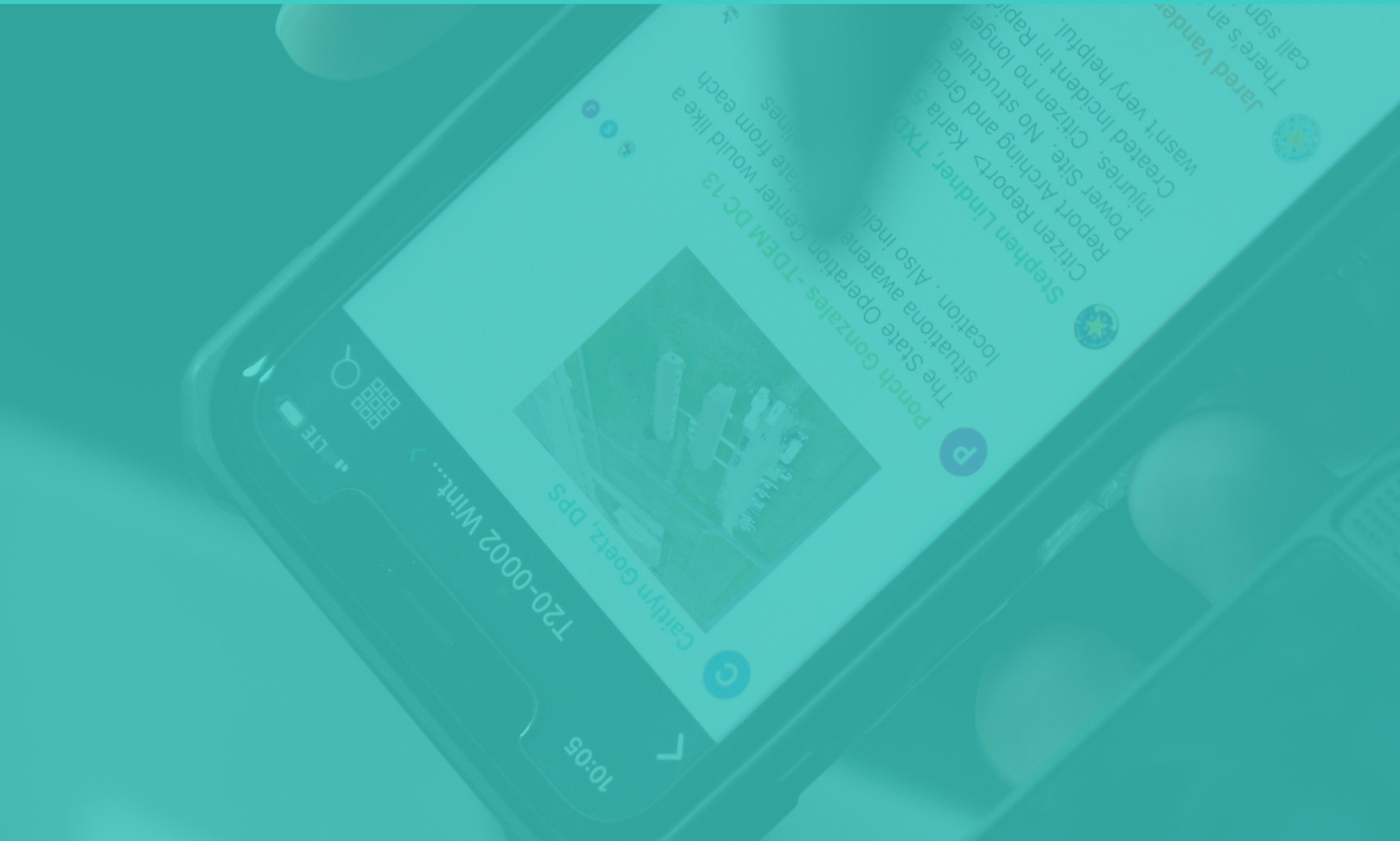
4. Outcome

The use of FirstNet communications solutions (HPUE, CRD, MiniCRD) and services like AT&T's ROG Deployables ensure that field teams have access to broadband communication when operating in remote and disaster environments. When coupled with drone solutions, decision makers and key stakeholders have the information they need to strategize the disaster response.

- **Resilience:** Teams provisioned with FirstNet HPUE devices and CRDs maintain connectivity in the field
- **Communication:** Imagery and data sharing combined with FirstNet push-to-talk services keep field teams connected with decision makers to share critical information and strategize operations

USING FIRSTNET ACROSS PARTNER AGENCIES

SECTION 7



A pickup truck carries a FirstNet Compact Rapid Deployable through snow and mud on the way to the Marshall Fire in Colorado.

USING FIRSTNET ACROSS PARTNER AGENCIES

Telecommunicator Emergency Response Taskforce

A Telecommunicator Emergency Response Taskforce (TERT) from another jurisdiction can provide relief to an impacted ECC by assuming call-taking and dispatching functions remotely. FirstNet has been used by TERT teams to facilitate 9-1-1 operations in the field. When activated, a TERT mobilizes telecommunicators to aid in situations where additional emergency resources are needed. This often occurs during high-priority, low-frequency events, such as a major planned event, an active shooter incident, or following severe weather.

TERTs can be deployed on site to assist or staffed up through remote response, and they may consist of telecommunicators from the requesting agency or from outside agencies. Portable routers and device hotspots with FirstNet SIMs allow telecommunicators to access the impacted agency's CAD and 9-1-1 workstations from anywhere, so they can begin taking calls almost immediately. Volunteer telecommunicators just need the equipment, electricity, and connectivity to provide much needed support to an impacted community. FirstNet can provide the necessary connectivity for TERT teams to facilitate 9-1-1 operations in the field.

Incorporating FirstNet into Your Communications Plans

As public safety users increasingly rely on technological solutions for responding to and managing events, it is critical that communications plans reflect those advances. Emergency planners and communications specialists should incorporate broadband use — including key contacts, processes, and procedures — in plans, emergency training, and exercises, so public safety will have a more effective response when a real emergency or disaster occurs. FirstNet-specific topics to consider incorporating in plans include the utilization of deployable assets (e.g., how to request, who requests), applications used by public safety agencies, procedures and best practices for using FirstNet Central, and managing device caches.

Communications Plans

One way to speed up equipment deployment and reduce the stress of providing robust communication capabilities at an incident scene is through pre-planning. Agencies should consider amending their planning documents, such as the Emergency Support Function (ESF) annex for Communications (ESF-2), Statewide Communications Interoperability Plan (SCIP), and Field Operations Guide, to address how FirstNet will be used during emergencies.

Some questions to ask during this planning process:

- What agencies typically respond to incidents?
  - Primary public safety agencies: law enforcement, fire, EMS, emergency dispatch, emergency management
  - Extended Primary partners: transportation departments, public works, water/wastewater entities, utilities (e.g., gas, telecom, electric)
- How are you currently communicating today?
- What devices and applications are these agencies using?
- How do you track the locations of resources (e.g., people, assets)?
- What information is being shared among partners?
- What can be improved in future planning cycles?

FirstNet-specific planning considerations:

- Who are the Uplift Managers?
- What devices should be uplifted in an emergency?
- Who can request a deployable? (Note, Uplift Managers can access the online Deployable Request Tool on their FirstNet Central landing page.)
- Is there a local or state process to request a deployable?

Emergency Support Function 2

The ESF-2 section of an organization's Emergency Response Plan should include language to define and identify deployable assets that may be required for a response. Specific directions and planning steps should be included to spell out the roles and responsibilities for communications coordinators and the process by which FirstNet deployable assets can be requested, staged, and utilized in the field. Additionally, agencies may work with AT&T in advance to understand the roles and responsibilities associated with requesting a deployable asset or other need.

When compiling Incident Action Plans (IAPs), Situation Reports (SitReps), and other forms as part of the Incident Command System (ICS), the Communications List (ICS 205A) form can be used to identify FirstNet devices being used, phone number, type of device, and if that user is Primary or Extended Primary. This information can be useful when coordinating an uplift (**Section 4: Using the Uplift Request Tool**) or deployable (**Section 2: FirstNet Deployables Fleet and Local Solutions**).

Statewide Communication Interoperability Plan

The SCIP provides actionable steps toward improving emergency communications interoperability within a state or territory. Developed through statewide engagement that involves all jurisdictions and disciplines, the SCIP is a critical reference resource to unify public safety's approach.

Jurisdictions should build FirstNet considerations into their SCIP to have a complete picture of interoperable communications used by public safety. It is important to include how public safety broadband fits into the communications picture for the jurisdiction, including details on how the agency will manage the request and deployment of FirstNet deployables and device caches, who will maintain situational awareness of network status, and when or how FirstNet Uplift will be utilized.

Field Operations Guides

Updating a jurisdiction's Field Operations Guide is an opportunity to incorporate broadband capabilities — specifically FirstNet — into official communications strategy. Statewide Interoperability Executive Committees and Interoperability Coordinators are encouraged to collaborate with the FirstNet Authority to ensure specific capabilities and functionalities are included in these guides.

PACE Plans

Maintaining operability, interoperability, and continuity of communications is critical for public safety during special events and emergency response in all operating conditions. A PACE (Primary, Alternate, Contingency, and Emergency) communications plan establishes predictable and redundant communications capabilities and ensures critical information can reach decision makers in a timely and secure manner. PACE plans should be as simple as possible to support reliable communications during changing operational conditions.

Leveraging FirstNet as one mode in the PACE plan can help emergency managers and their partners stay in communication during emergencies.

- Primary: everyday method of communication
- Alternate: backup methods and work arounds
- Contingent: fallback methods
- Emergency: last resort methods

More on PACE planning: **Leveraging the PACE Plan into the Emergency Communications Ecosystem, 2023 (cisa.gov)**

Fixed Location PACE plan with FirstNet

		Voice	Data
Primary	LE/FD/EMS	LMR with standard talk groups ⁝ LTE phone calls ⁝ MCPTT with standard talk groups	Wired internet and Wi-Fi ⁝ LTE connections in mobile devices ⁝ Indoor LTE boosting devices
	EOC/ECC	Dispatch with standard talk groups ⁝ LTE phone calls ⁝ MCPTT with standard talk groups	Wired internet and Wi-Fi ⁝ LTE connections in mobile devices ⁝ Indoor LTE boosting devices
Alternate	LE/FD/EMS	⁝ LMR or LTE failover (primary method unavailable) ⁝ Alternate LTE carrier ⁝ Alternate PTT applications	⁝ LTE failover
	EOC/ECC	⁝ LMR or LTE failover (primary method unavailable) ⁝ Alternate LTE carrier ⁝ Alternate PTT applications	⁝ LTE failover Re-locate to pre-established backup center
Contingency	LE/FD/EMS	LMR point-to-point (non-repeated) Wi-Fi calling GETS landline calling	Limiting data usage to essential systems (eliminating streaming video, etc) ⁝ COAM Deployable assets (CRDs, miniCRDs, etc)
	EOC/ECC	Wi-Fi calling GETS landline calling ⁝ COAM Deployable assets (CRDs, miniCRDs, etc) ⁝ ESInet failover using LTE connection (if already established)	Limiting data usage to essential systems (eliminating streaming video, etc) ⁝ COAM Deployable assets (CRDs, miniCRDs, etc) ⁝ ESInet failover using LTE connection (if already established)
Emergency	LE/FD/EMS	Non-standard tactical radio (MARS/HAM) ⁝ Satellite comms (SatCOLT, CRD, miniCRD, Satphone) In-person commnunication relays (set locations)	⁝ Satellite comms (SatCOLT, CRD, miniCRD, Satphone) In-person commnunication relays (set locations)
	EOC/ECC	Non-standard tactical radio (MARS/HAM) ⁝ Satellite comms (SatCOLT, CRD, miniCRD, Satphone) In-person commnunication relays (set locations) Re-route calls to non-local ECC	⁝ Satellite comms (SatCOLT, CRD, miniCRD, Satphone) In-person commnunication relays (set locations) Re-route calls to non-local ECC

⁝ *Solutions that can be enabled by FirstNet*

Mobile Location PACE plan with FirstNet

		Voice	Data
Primary	LE/FD/EMS	LMR with standard talk groups ⁝ LTE phone calls ⁝ MCPTT with standard talk groups	⁝ LTE hotspots/mobile routers ⁝ LTE boosting devices (HPUE)
	EOC/ECC	LMR with standard talk groups ⁝ LTE phone calls ⁝ MCPTT with standard talk groups	⁝ LTE hotspots/mobile routers ⁝ LTE boosting devices (HPUE)
Alternate	LE/FD/EMS	⁝ LMR or LTE failover (primary method unavailable) ⁝ Alternate LTE carrier ⁝ Alternate PTT applications	⁝ Alternate LTE carrier
	EOC/ECC	⁝ LMR or LTE failover (primary method unavailable) ⁝ Alternate LTE carrier ⁝ Alternate PTT applications	⁝ LTE failover Re-locate to pre-established backup center
Contingency	LE/FD/EMS	LMR point-to-point (non-repeated) ⁝ COAM Deployable assets (CRDs, miniCRDs, etc)	Limiting data usage to essential systems (eliminating streaming video, etc) ⁝ COAM Deployable assets (CRDs, miniCRDs, etc)
	EOC/ECC	⁝ COAM Deployable assets (CRDs, miniCRDs, etc)	⁝ COAM Deployable assets (CRDs, miniCRDs, etc)
Emergency	LE/FD/EMS	Non-standard tactical radio (MARS/HAM) ⁝ Satellite comms (SatCOLT, CRD, miniCRD, Satphone) In-person commnunication relays (set locations)	⁝ Satellite comms (SatCOLT, CRD, miniCRD, Satphone) In-person commnunication relays (set locations)
	EOC/ECC	Non-standard tactical radio (MARS/HAM) ⁝ Satellite comms (SatCOLT, CRD, miniCRD, Satphone) In-person commnunication relays (set locations)	⁝ Satellite comms (SatCOLT, CRD, miniCRD, Satphone) In-person commnunication relays (set locations)

⁝ *Solutions that can be enabled by FirstNet*

CONCLUSION

This has been a high-level overview of the tools and technologies available to FirstNet users. As more public safety agencies and individuals join FirstNet for their broadband communications needs, this guide will continue to serve as a reference for specific features and functions that all public safety officials may use as they coordinate with field forces and operate in their EOCs and ECCs.

The FirstNet Authority will continue to update this guide on a periodic basis to account for changes to existing features and to provide an overview of new functions that are added to the platform. The FirstNet Authority also wants to hear from stakeholders about their experiences using the resources described in this guide. To share your feedback and find other public safety broadband information and resources, please visit **FirstNet.gov.**

APPENDIX A: CONTACT GUIDE

First Responder Network Authority:

FirstNet.gov

FirstNet.gov/advisor

FirstNet Customer Care:

1-800-574-7000

Calls to FirstNet Customer Care are routed to either technical or billing representatives for assistance. Callers should be prepared with their FirstNet Foundation Account Number (FAN) when calling for assistance.

FirstNet, Built with AT&T:

FirstNet.com

Training.FirstNet.att.com

Your Agency's Information:

AT&T FirstNet representative

Name _____ Phone _____ Email _____

Agency Administrator(s) of FirstNet Account

_____

Agency Uplift Manager(s) for FirstNet Account

_____

Agency Foundation Account Number (FAN) for FirstNet Account

_____

APPENDIX B: ACRONYMS

3GPP	3rd Generation Partnership Project
AAR	After-Action Report
AI	Artificial Intelligence
ALPR	Automated License Plate Reader
AMBER	America's Missing: Broadcast Emergency Response
API	Application Programming Interface
BWC	Body-Worn Cameras
CAD	Computer-Aided Dispatch
CAP	Common Alerting Protocol
CBP	Cell Booster Pro
CISA	Cybersecurity and Infrastructure Security Agency
CJIS	Criminal Justice Information System
COAM	Customer Owned and Managed
COW	Cell on Wheels
CRD	Compact Rapid Deployable
CSSI	Console Subsystem Interface
DFR	Drone as a First Responder Program
DHS	U.S. Department of Homeland Security
ECC	Emergency Communications Center
ECD	Emergency Communications Division
EM	Emergency Management
EMA	Emergency Management Agency
EMAC	Emergency Management Assistance Compact
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EPC	Evolved Packet Core
ESF	Emergency Support Function
FAN	FirstNet Foundation Account Number
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
Flying COWs	Flying Cells On Wings
FMV	Full Motion Video
FNC	FirstNet Central platform
FOG	Field Operations Guide
FSLTT	Federal, State, Local, Territorial, and Tribal
GETS	Government Emergency Telecommunications System
IAP	Incident Action Plans
ICS	Incident Command System
IoT	Internet of Things
IP	Internet Protocol

IPAWS	Integrated Public Alert and Warning System
ISSI	Inter-RF Subsystem Interface
LBS	Location-Based Services
LEO	Low Earth Orbit
LMR	Land Mobile Radio
LPR	License Plate Reader
LTE	Long Term Evolution
MBK	Mobile Broadband Kit
MCData	Mission Critical Data
MCPTT	Mission Critical Push-to-Talk
MCS	Mission Critical Services
MCVideo	Mission Critical Video
MDM	Mobile Device Management
MHz	Megahertz
NCSWIC	National Council of Statewide Interoperability Coordinators
NDR	Network Disaster Recovery
NIST	National Institute of Standards and Technology
NPSBN	Nationwide Public Safety Broadband Network
NTIA	National Telecommunications and Information Administration
PACE	Primary, Alternate, Contingency, and Emergency
PIER	Post-Incident/Event Review
PSAP	Public Safety Answering Point
PSCR	Public Safety Communications Research Division
PTT	Push-to-Talk
RAN	Radio Access Network
RDK	Rapid Deployable Kit
ROG	FirstNet Response Operations Group
RoIP	Radio over IP
RTCC	Real Time Crime Center
SAFECOM	DHS/CISA public safety communications operability program
SatCOLTs	Satellite Cell on Light Trucks
SCIP	Statewide Communication Interoperability Plan
SDK	Single Sign-On Software Development Kit
SIM	Subscriber Identify Module
SitReps	Situation Report
TAK	Team Awareness Kit
UAS	Unmanned Aerial System
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WASP	Wide Area Search Plugin
WEA	Wireless Emergency Alerts
WPS	Wireless Priority Services

APPENDIX C: GLOSSARY

3rd Generation Partnership Project (3GPP):

A global initiative made up of telecommunications professional organizations that sets standards for public safety communications systems. The FirstNet Authority is actively involved in supporting the mission of 3GPP and helping to ensure the FirstNet network meets 3GPP standards. The FirstNet Authority also works to ensure that public safety's needs are included in the standards development process and resulting 3GPP standards reflect the requirements of public safety users.

Agency Paid:

Agency-Paid users are employees and contractors of a qualified public safety entity. The public safety entity pays for FirstNet service for Agency-Paid users.

Band 14:

20 megahertz (MHz) of spectrum in the 700 MHz frequency allocated to the First Responder Network Authority (FirstNet Authority) for the Nationwide Public Safety Broadband Network (NPSBN).

Extended Primary Users:

Extended Primary users are those agencies, organizations, non-profit or for-profit companies that provide public safety services in support of Primary users. They provide mitigation, remediation, overhaul, clean-up, restoration, or other such services during or after an incident.

FirstNet Central:

A portal for FirstNet subscribers to access administrative and operational tools.

FirstNet Deployable:

Network assets available at no cost to FirstNet subscribers to utilize during planned events or emergency situations to support public safety communications. They come in a variety of form factors, such as a Satellite Cell on Light Truck (SatCOLT), Compact Rapid Deployable (CRD), Cell on Wheels (COW), and Flying Cell on Wings (Flying COW™). Deployable solutions can support broadband needs both indoors and outdoors.

FirstNet App Catalog:

Applications relevant to the public safety mission that are reviewed and approved by AT&T and the FirstNet Authority. Applications are divided into two categories: FirstNet Verified™ and FirstNet Certified™.

FirstNet Certified:

A designation for applications that meet the criteria for relevancy, security, and data privacy, and also have increased availability (99.99% available), mobility, resiliency, and scalability.

FirstNet App Priority Application Programming Interface (API):

Extends First Priority service to automatically apply to critical public safety apps sourced from the FirstNet App Catalog. Developers must request permission to use the App Priority API to build in the highest level of priority access to the use of their app.

FirstNet Single Sign-On Software Development Kit (SDK):

Developers creating public safety solutions can integrate FirstNet Single Sign-On directly into their apps.

FirstNet Ready®:

A device has undergone a review by the FirstNet Device Approval Program for certification by AT&T and approval by the FirstNet Authority. A FirstNet Ready® device is compatible with the FirstNet Evolved Packet Core and can utilize Band 14.

FirstNet Verified:

A designation for applications that meet criteria for relevancy to public safety and have gone through a vetting process that includes relevance, security, data privacy, and availability (99.9% available).

High Power User Equipment (HPUE):

Under the FirstNet Authority's Federal Communications Commission (FCC) license for the Band 14 spectrum and standards established by the 3rd Generation Partnership Project (3GPP) organization, certain FirstNet devices are authorized to transmit on Band 14 at a power level significantly higher than normal cellular power.

Homeland Security Exercise and Evaluation Program (HSEEP):

A set of guiding principles for exercise and evaluation programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. This program is developed and maintained by the Federal Emergency Management Agency (FEMA).

Internet of Things (IoT):

A network of devices with processing, connectivity, and intelligence to collect and transmit data. IoT devices may or may not have a traditional user interface or display. IoT devices often run on a limited version of traditional operating system software and firmware. IoT devices may provide connectivity via one or more technologies; for example (but not limited to) wireless broadband, Wi-Fi, Bluetooth, Zigbee, and more. The term "sensor" is often used to refer to such IoT devices.

Mission Critical:

Any factor of a system (equipment, process, procedure, software, etc.) that is critical to the success or failure of mission operations.

Network Status Tool:

Located in FirstNet Central, this tool provides visibility into the status of the FirstNet network to identify areas that may be experiencing outages. It allows users to view on-demand reports on locations scheduled for planned maintenance.

Primary Users:

Primary users are public safety entities that act as first responders, the agencies who are at an emergency scene first. This includes law enforcement, fire protection services, emergency (9-1-1) call dispatching and government ECCs, emergency planning and management offices, and ambulance safety services.

Preemption:

Public safety devices are treated as the most important on the FirstNet network. Network resources cannot be taken from public safety. In severe network congestion, commercial users will be moved to different frequencies or may be momentarily disconnected. End users that have been temporarily uplifted are also protected from preemption.

Priority:

Public safety devices gain access to the network first. Public safety is at the front of the line.

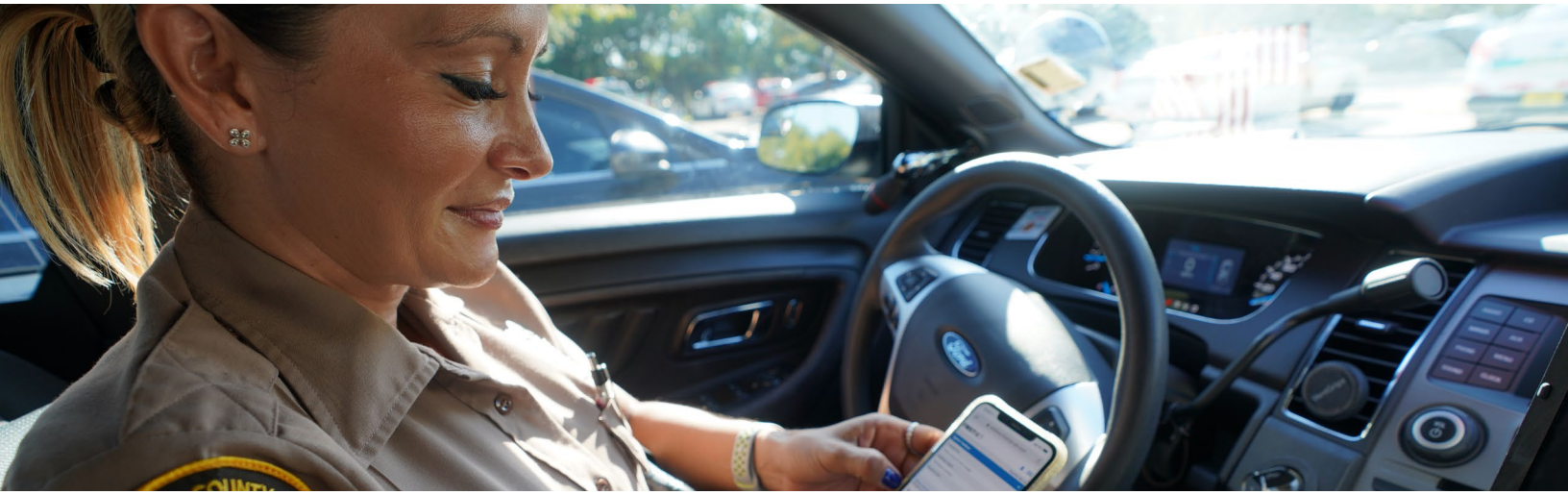
Subscriber Paid:

Subscriber-Paid users are (i) verified current employees/ volunteers of a Primary user public safety entity or (ii) employees of an eligible Extended Primary user public safety entity. The individual user pays their own monthly bill for FirstNet service.

Uplift Request Tool:

Located in FirstNet Central or on the FirstNet Assist app, it elevates the priority of a specific device for a determined amount of time. This can be used for planned events or during emergency situations.


2:28
Search
SB2
00:A0:BC:93:82:54
176.22
AZ
Viasat-1
115.1°
EL
GPS LAT: 39.978



FirstNet® Authority

First Responder Network Authority

info@FirstNet.gov | FirstNet.gov

@firstnetgov