EMERGENCY MANAGEMENT RESOURCE GUIDE

September 2024

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**.

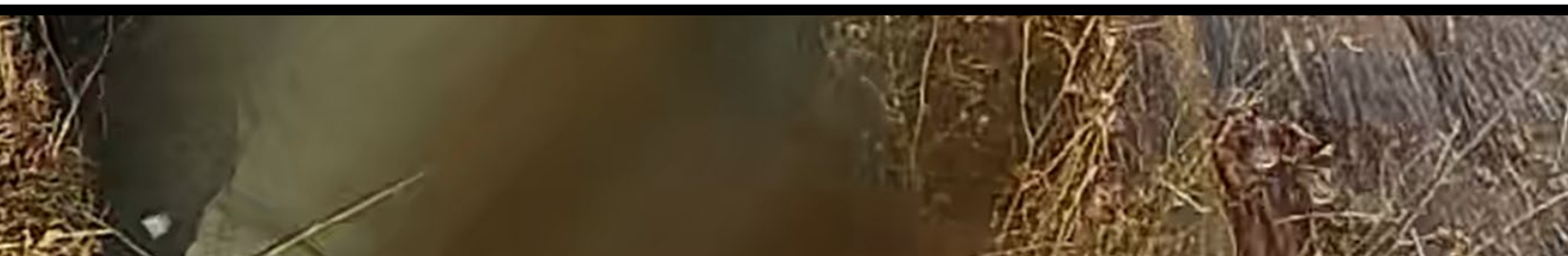
GUIDE CHANGE LOG

Section	Change	Last Update
What is FirstNet?	Added FirstNet categories: Primary, Extended Primary, Agency Paid, Subscriber Paid; Added 5G description	September 2023
What is FirstNet?	Added information about investments	September 2024
Section 1	Updated content on Wireless Priority Service (WPS)	September 2023
Section 2	Updated guidance on how to request a deployable	June 2022
Section 2	Major update	September 2024
Section 3	Updated language regarding Advanced Network Status Tool capabilities	June 2022
Section 4	Updated descriptions of Uplift and Uplift Request Tool	June 2022
Section 5	Added language on 5G and FirstNet	September 2023
Section 7	Added planning considerations	June 2022
Section 10	Add information about Boulder FirstNet Lab	September 2024
Appendix B	Added new definitions	September 2023
Appendix C	Re-formatted deployables best practices guide	June 2022

The New Hampshire Department of Safety worked with private healthcare organizations and state and local agencies to set up large testing and vaccination sites. "Go-kits" with cameras, battery packs, routers with FirstNet SIM cards, and other internet-based devices were used to oversee and coordinate the operation. The ability to stream video footage to unified command was critical to decision-making.

CONTENTS

The City of Boulder used its FirstNet Compact Rapid Deployable to respond to the 2022 NCAR Fire in Colorado. In an area where they normally don't have great coverage, in fifteen minutes they were up and running, coordinating evacuations on their phones and laptops.



PURPOSE

This Emergency Management Resource Guide is intended to be a reference for Emergency Managers to use the products, services, and capabilities of the Nationwide Public Safety Broadband Network (NPSBN) or "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. Our mission, as mandated by Congress, is to ensure the buildout, 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**.

With increasing numbers of emergency management agencies (EMAs), law enforcement, fire service, emergency medical services (EMS), emergency communications, and other partners in public safety response using FirstNet, this guide provides an overview of certain features and functions that Emergency Managers might use in their daily and emergency response roles. Many of the topics covered in this guide are applicable for coordinating response in the field or when an Emergency Operations Center (EOC) has been activated.

Where practical, the guide includes reference links and suggestions for Emergency Managers 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 can be contacted at **FirstNet.gov/advisor**.

For more information about Emergency Management and FirstNet, visit FirstNet.gov/EM.

The Chesapeake Fire Department's Office of Emergency Management in Virginia uses FirstNet-enabled tablets to support their emergency management damage assessments in the field.

WHAT IS FIRSTNET?

The Middle Class Tax Relief and Job Creation Act of 2012 created the FirstNet Authority, an independent agency within the U.S. Department of Commerce's National Telecommunications and Information Administration. The FirstNet Authority's mission is to ensure the establishment and continuing operation and improvement of the NPSBN, and in 2017, the FirstNet Authority contracted with AT&T to build, operate, and maintain the network. The legislation creating FirstNet also allocated 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.

Today, FirstNet provides a reliable broadband communications network that is available in all 50 states, 5 territories, and the District of Columbia, including Tribal lands. For Emergency Managers as well as front-line first responders, the availability of the FirstNet network provides secure, prioritized communications before, during, and after incidents, whether they are routine responses, major disasters, or pre-planned events and exercises.

In February 2024, the FirstNet Authority and AT&T announced an $8 billion investment initiative that will evolve and expand the FirstNet public safety communications network. The FirstNet Authority will invest $6.3 billion through its network contract with AT&T and anticipates an additional $2 billion for ongoing investments in coverage enhancements for public safety. These strategic investments will expand and evolve FirstNet so public safety stays at the forefront of innovative, lifesaving technologies.

With the **initial buildout of FirstNet completed and validated as of December 2023**, this investment initiative will continue to expand access to public safety's Band 14 spectrum in the near term, with plans for additional coverage enhancements on a recurring basis. The FirstNet Authority will work closely with public safety across the states, territories, and tribal lands to ensure future coverage enhancements maximize investment dollars and make the biggest impact to public safety operations.

Broadband Technologies for Public Safety

As public safety's role continues to evolve — from natural and man-made emergencies to civil unrest, protests, and pandemic response — agencies have had to adapt to these new challenges. In doing so, the technology supporting responders through preparedness, response, recovery, and mitigation has matured, allowing for enhanced awareness and collaboration.

As wireless broadband technologies have become more ubiquitous, more agencies are choosing to use tools and resources powered by the FirstNet network. Tens of thousands of public safety agencies across the country use the FirstNet network for their critical communications needs, transmitting voice calls, text messages, and secure data over the only dedicated public safety network built specifically for first responders. Law enforcement agencies, fire departments, emergency medical services, emergency communications centers (ECCs), and emergency management agencies all rely on FirstNet for their daily and emergency operations.

No matter if the response is to a local mutual aid event or an Emergency Management Assistance Compact (EMAC) deployment assisting in a national emergency, FirstNet is the means by which responders in the field can communicate with each other and share situational awareness with Emergency Management Coordinators in their EOCs.

Who Can Use FirstNet

FirstNet is available to traditional public safety agencies and to many of their partners who assist in emergency response.

Primary users are public safety entities that serve as first responders — the agencies 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 non-profit or for-profit companies that provide public safety services in support of Primary users.

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.

These broad categories of eligibility provide many options for public safety agencies and their partners to take advantage of FirstNet service. The tools outlined in this Resource Guide are intended to help Emergency Managers get the most out of FirstNet's capabilities for communicating efficiently and effectively with all agencies that are part of an emergency response.

FirstNet and 5G

Wireless networks continually evolve, as we see 4G LTE give way to newer 5G communication technologies.

The FirstNet Authority recognized the need to address 5G evolution and approved network investments to support initial generational upgrades to enable 5G network capabilities. These initial investments have supported AT&T's upgrades to the dedicated FirstNet network core to enable reliable 5G connectivity, resulting in access to 5G spectrum bands. Today, FirstNet users in select cities can access high-band 5G+ spectrum, mid-band 5G+, or low-band 5G. Mid-band 5G+ offers ultra-fast speeds and wide geographic coverage. Low-band 5G can travel farther and penetrate buildings and infrastructure better than high-band 5G+.

The investment announced by FirstNet Authority in February 2024 marked the start of the transition to a full 5G network, enabling FirstNet to keep pace with current evolutions in technology and 3GPP standards-based mission critical advancements. The planned 5G network upgrades will generate faster speeds, increase capacity, enhance the quality of service for FirstNet users, and drive innovations in 5G mission critical services. Throughout this multi-year transition to a full 5G network, the existing FirstNet 4G LTE network will remain fully operational and maintain the high level of service that first responders have come to rely on.

5G's ability to handle large amounts of data and connect more devices at once is essential to enabling the future of emergency response. From using drones to transmit high-definition video during search and rescue operations to opening the door to an influx of Internet of Things (IoT) data that will enhance situational awareness and improve emergency patient care, 5G is the foundation for the future of first responder-centric technologies.

Plus, by integrating 5G on FirstNet with **9-1-1**, public safety will be able to leverage the full potential of this technology, allowing for a more informed and rapid response to emergencies.

For more information on 5G devices and connectivity, see **Section 7**.

How FirstNet Can Support Emergency Managers

One of the key teachings for Emergency Managers is that "all disasters are local." So how does FirstNet specifically help Emergency Managers do their jobs during a planned event, a no-notice event, or a major disaster?

Whether they are standing up an EOC or operating in the field from an incident command post, Emergency Managers are focused on coordinating resources and partner agencies. The EOC needs to know where response forces and equipment are located, when and where they might arrive to their deployed locations, and which forces are in standby or recovery mode waiting to be dispatched again.

Emergency Managers are also responsible for sharing situational awareness through a common operating picture (COP). Building a COP relies on gathering and quickly analyzing large volumes of data, such as sensor data, weather and environmental conditions, video feeds from fixed cameras and new platforms such as drones, and more.

By providing multi-faceted situational awareness, FirstNet helps EOC staff to effectively respond to current conditions as well as to plan for the assets and personnel that might be needed in the next operational period.

In this resource guide, you will learn more about how FirstNet capabilities can support your agency before, during, and after an emergency.

A convoy of response vehicles from Missouri travel with AT&T FirstNet deployable vehicles to provide mutual aid assistance in Florida after a hurricane.

SECTION 1: RESPONDING WITH FIRSTNET

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 a 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 deploy the FirstNet network to meet the needs of their responders.

Nationwide Available Network

In any situation, 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 ECC or EOC, even when the general public is trying to communicate at the same time. Apps such as **FirstNet Push-to-Talk** or FirstNet Rapid Response can 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, 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 public safety broadband network, EMAC deployment teams can count on being able to use their FirstNet mobile devices, including phones, tablets, and hotspots, to communicate and share situational awareness — regardless of what state

they are operating in. They can access databases, reference materials, and share planning documents. Real-time location data, sensor data, and video can be shared with responders and EOCs to keep everyone informed and working from the same common operating picture.

Deployable Assets

In many instances, responders are forced to operate in remote or challenging environments where communication networks may be strained or damaged. To support operations, FirstNet users can request and use temporary deployable communications assets. Depending on mission requirements, these assets could include Cells on Wheels (COWs) and Satellite Cell on Light Trucks (SatCOLTs), Compact Rapid Deployables (CRDs), or 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 to no communications and enabling responders to transmit voice and data communications from the field to the EOC. 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 3**.

"Now that there's a public safety broadband network across the country, my communications system goes ocean to ocean, Canada to Mexico, and everything in between. We had responders from here [Iowa] that went down to the aftermath of Katrina. Communications were a nightmare. If we're all on the same network and all singing off the same sheet of music, stuff like that where we go a thousand miles away to help somebody, that's going to be a lot better. Not only locally, but large distances, we're going to be able to communicate."

ROB DEHNERT
WEST DES MOINES EMS, IOWA

FirstNet.gov/WestDesMoines

Pro Tips: Agency-Owned and Managed 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.

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 Mini CRDs™, Rapid Deployable Kits, Mobile Broadband Kits, and satellite-enabled systems. These platforms can allow for quick, nimble deployment of FirstNet availability in the critical minutes and hours after an event or incident begins. Agencies now have the ability to extend the FirstNet network to remote, damaged, or even congested areas and provide secure field-to-EOC communication, at their own direction and on their own timeline.

In addition, 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, or helicopter into remote areas or high terrain to provide responders with a temporary signal during search-and-rescue operations. For EOCs and command posts, there are solutions such as the Cell Booster Pro 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, 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.

Agency-owned assets provide responders with the ability to communicate back to the EOC, 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.

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 on 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 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 other wireless users outside of FirstNet. 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**.

Cached Devices: Mobile Handsets, Tablets, and Hotspots

Many agencies maintain a cache of mobile devices that can be quickly distributed in an emergency to augment the communications tools used by responders. These devices may be handed out to mutual aid partners who are not tied into the local responders' networks or allow for a surge in the number of responders at an incident. Providing responders with a common communications platform ensures all are able to maintain a common operating picture, situational awareness, and access to plans and resource documents.

It is important to note that when a FirstNet SatCOLT is deployed to assist with on-scene communications, it will only be available to FirstNet devices. Maintaining a local cache of FirstNet devices that can be handed out quickly to those without their own FirstNet device ensures that all responders can benefit from the SatCOLT's coverage enhancements.

For more suggestions on using devices and apps, see **Section 7: FirstNet Devices and Applications for Everyday Use**.

For more suggestions on using caches of devices, see **Section 8: Using a FirstNet Device Cache**.

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 adopted FirstNet can be found at **FirstNet.gov/FirstNetInAction**.

Every year, the city of St. Augustine, Florida, is transformed during Nights of Lights. As visitors marvel, St. Augustine's officials use FirstNet to coordinate with partners like the state highway patrol, the county sheriff's office, county motor units, and the beach bike patrol.

SECTION 2: MISSION CRITICAL SOLUTIONS

What is mission critical?

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 are included in the standards development process and resulting 3GPP standards reflect the actual requirements of public safety users. The FirstNet Authority also works to ensure the FirstNet network meets 3GPP standards.

Mission Critical

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

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 Land Mobile Radio (LMR) system and help to fill indoor and outdoor coverage gaps, creating a more robust communications capability for public safety users.

MCS on FirstNet

Offerings based on the 3GPP MCS Standard are evolving and maturing. They are also expanding thanks, in part, to the **FirstNet Authority's 10-year, $8 billion investment initiative**, which aims to enhance MCS. Additional features, along with expanding device and accessory compatibility will continue to become available in the marketplace. There are several benefits to adopting MCS solutions:

- Expand the agency's communications "footprint" with nationwide-available PTT solutions and the ability to connect LMR networks for improved capabilities outside of the normal LMR geography
- Save money by determining which devices agency staff need based on their roles and responsibilities (i.e., LMR radios vs. commercial LTE devices using MCS PTT)
- Reduce radio traffic loads by moving some voice traffic off the LMR system and onto an MCS (data) exchange
- Leverage the capabilities of LTE devices to communicate with voice, MCData, MCVideo, location information, and more.

We recommend working with your AT&T FirstNet Solution Consultant to find the best solution for your agency's communications needs.

There are currently two mission critical services to choose from on FirstNet: FirstNet Push-to-Talk (FNPTT) and FirstNet Rapid Response (FNRR).

They are both integrated into the FirstNet Core and have the highest priority for applications on the network. Both support secure, encrypted mission critical services nationwide over the FirstNet network. Beyond voice communications, other features such as location services to identify responder positions, geofencing, mapping, ability to send text messages/broadcasts, ability to share documents, images, and video may be available, depending on the devices being used.

Both FNPTT and FNRR support MCPTT, MCData, and MCVideo along with mission critical Quality of Service (QoS) for all communications. Both support Push-to-Talk over Wi-Fi as well as the FirstNet network, and both applications can be set up for LMR interworking through a Radio-over-IP setup. The FNRR application can also support Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) interconnections. Both solutions provide the following dispatch clients:

FirstNet PTT Console: The FirstNet PTT Console provides one dispatch solution for both LMR and FirstNet PTT users and allows for the ability to multiselect or patch LMR groups to FirstNet groups. FirstNet PTT interface to the console is the native 3GPP client interface so the console has all of the normal client capabilities plus typical dispatcher features. The console is provided by a third-party partner and is a mature EOC dispatch solution with APCO Project-25 (P25) CSSI, telephony, and logging recorder interfaces along with many of the other dispatch features you would expect.

FirstNet Rapid Response Web Dispatch: The FirstNet Rapid Response dispatch console provides typical dispatch features including call recording/playback and multiple talkgroup 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, a map that tracks users that can be popped out to a second screen, and geofences. Geofences can be used to monitor users crossing into or out of the geofence, along with defining area-based talkgroups.

FNPTT and FNRR offer many benefits to emergency managers by equipping them with real-time data and voice communications capabilities. With access to the FirstNet network, mission critical services have significant advantages in that configuration of groups and users can be accomplished over the air within seconds of the administrator making changes. These offerings enable emergency managers to communicate and track the location of responders in the field from the EOC. They can connect with individuals or entire talk groups to share critical information, such as voice communications, pictures, and video. They can scale the applications based on each

Use Case: LMR-to-LTE in Indiana

"Embracing LMR-to-LTE has helped Indiana first responders save money and save lives. While Indiana responders have access to a very robust statewide LMR system, in-building coverage such as inside school buildings, hospitals, and correctional facilities, presented a challenge. Today, we can put a SIM card in an LTE-capable radio — which means a responder can stay connected when it counts. In addition to this improved coverage, we are also seeing a cost savings. The broadband connection to our LMR system is giving volunteer fire departments the option of a using a push-to-talk app on a low-cost device — saving money and possibly saving a life."

KELLY S. DIGNIN
EXECUTIVE DIRECTOR (RET.), INTEGRATED PUBLIC SAFETY COMMISSION

incident, creating or expanding talk groups as needed to develop a shared common operating picture of an incident.

With the ability to connect to LMR radio networks, FNPTT and FNNR 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.

Integration between LMR and LTE

As MCS applications have evolved, public safety agencies have been vocal about the ability to integrate MCPTT into their current LMR systems. Integrating LTE into LMR provides flexibility and interworking for operations. There are several ways to do that today and we expect more in the future.

There are several benefits to integrating LMR and LTE communications, including:

- **Expanded coverage:** Users benefit by having both LMR and LTE coverage. Devices connected to Wi-Fi can also communicate to an LMR network.
- **Optimization of LMR resources**: Non-first responder groups can utilize LTE, leaving LMR capacity for first responders.
- **Over-the-air programming:** The MCS admin portals allow for easy user and talkgroup configuration, including the ability to add users to LMR connected talkgroups and have them available for users in seconds.
- **Streamlining of devices:** LMR-LTE integration reduces the need for large caches of LMR devices for large mutual aid events.

FirstNet supports LMR-LTE interoperability through several methods:

- **Radio over IP (RoIP) gateway technology:** This is a lower cost option to extend agency communications. It also provides the ability to remain in contact with personnel who travel outside the agency's LMR footprint and the option to free up capacity on an LMR network that is nearing its limits. This functionality can be achieved with as little as a single LMR portable or mobile radio connected to the RoIP gateway device.
- **Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI):** These P25 standards-based solutions provide a greater feature set. 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.

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

Interoperability with other Agencies and Carriers

Like LMR, CAD, and other communications tools, working within your region to standardize on the same application/solution and establish regional governance agreements will provide the best seamless communications between 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 can extend. Both FirstNet MCS solutions allow for calls between all users and methods for users across agencies to join the same talkgroup.

Most agencies already have interoperability with their neighboring agencies via their existing LMR systems. Therefore, when adding MCS PTT to your existing LMR system via one of the methods described in the previous section, 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 solutions that can be leveraged in the interim. Cross-carrier licenses allow for users that are leveraging other carriers to be part of the FirstNet Rapid Response MCS solution. Cross-carrier users will have access to the same talkgroups, except priority of their calls will be based on the level of service their carrier is providing. If your neighboring agency has a different broadband PTT solution from another carrier, then the same methods as described above for other PTT solutions on FirstNet can be leveraged. The wireline interfaces still can be leveraged, even when using RoIP as FirstNet coverage is available nationwide.

FirstNet offers a unique opportunity for incident response communications. The coverage footprint is nationwide, public safety has priority on the network, and there is Federal Government oversight. Most importantly, when the network is at the highest traffic level during a response, MCS communications have the highest priority. The FirstNet Authority is working to ensure a mutual aid talkgroup framework can be put in place to allow for incident command and users to easily identify talkgroups and leverage MCS communications during incident response. Having easily identified talkgroups that all response users can join included in the Incident Communications Plan (e.g., ICS 205) is crucial for an efficient response. For emergency managers, these functions can be critical elements to incorporating mutual aid resources, especially from outside the area through EMAC. For example, response to wildfires, major flooding, tornadoes, or hurricanes often involves 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 absorbed into the host state/agency's communications systems.

Devices, Accessories, and Ecosystem for MCS

Devices and accessories leveraged with the MCS service can be just as important as the service itself. For frontline users, they want to leverage 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 leverage MCS in an application on a smartphone, especially when paired with a remote speaker mic. Early adopters have cautioned those exploring MCS to limit the applications on smartphones with MCS to only those critical to the mission. Just like early smartphones struggled with transferring data while the user was on the phone, there is still work to be done to ensure MCS, other mission applications, and telephony work seamlessly together.

We strongly recommend that you allot significant time for trying out device and accessory options along with 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.

"Road test it, put it in your hand, see how it works, because that answers a lot of questions without even having to ask them. You need to use FirstNet and have [product representatives] come out, show the operation, show all the pieces. You can walk around with a device in your hand, try PTT, see how your agency can integrate, and you'll probably think of way more solutions than you realized until you have it in your hands. … [To really understand what the technology can do,] I need to know how it works in my specific area. Just test it, figure it out, and then everybody can start talking about your specific needs in your area."

CODY SNOW

President, Prevent Medical Solutions, Bloomington, California

Hybrid LMR FirstNet Devices

Hybrid LMR FirstNet devices are LMRs with FirstNet capabilities built in. As noted previously, responders leverage hybrid LMR FirstNet devices in their mission and use muscle memory to control them, which allows them 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 mobiles and portables that are compatible with FNPTT. While using these devices in MCS mode on FirstNet, their communications have higher priority just like other MCS devices on FirstNet. An advantage to these devices is that they are purpose-built for public safety with a full line of accessories and installation options for all types of use cases.

PTT-focused devices

Several vendors have developed 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 packaged with MCS and have lower cost monthly plans than smartphones. They are typically easier to pick up quickly and operate by users, 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 operation of MCS. Many are rugged or semi rugged and offer accessories such as remote speaker mics.

Smartphones

MCS offers client applications that can be downloaded from the app store on the smartphone just like other applications. This enables users to communicate without taking an extra device with them, or to communicate on an existing user's device. Care needs to be taken to make sure that the combination of MCS and other user applications work well together to meet the responders' mission. In most cases a mobile device management (MDM) solution is recommended when using a smartphone device to ensure MCS and relevant settings are updated when a new MCS version, device, or accessory is available.

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 the accessories needed for your operation.

Ecosystem

Understanding what is needed and works best for your users' mission is an important step in choosing an MCS solution. When considering MCS, operational needs, such as vehicle solutions, specific accessories like vehicle docking stations, multi-bay chargers, and logging/recording, should also be evaluated.

For logging/recording, if your MCS solution is connected to LMR, your recording of calls is typically taken care of on the LMR system. If talkgroups are not tied to the LMR system, RoIP can be leveraged to provide an analog interface to your logging recorder. Further, with FNPTT console, you can leverage logging/recording interfaces built into the console.

Devices, accessories, and the ecosystem to support MCS are evolving and expected to continue to add capabilities in the coming years. As more users adopt MCS, more vendors and solutions will be offered in the marketplace.

Location-based services (including Z-axis location)

Location-based services (LBS) refers 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.

LBS applies to both indoor and outdoor environments and has 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.

Today, with FirstNet and the **Response for FirstNet** application, 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" (HAT). 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.

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.

SECTION 3: UNDERSTANDING THE FIRSTNET DEPLOYABLE PROGRAM

What is provided to FirstNet users?

There are more than 150 deployable network assets dedicated to FirstNet users. Agencies can request a deployable to support critical incidents, disasters, planned events, and exercises. These assets are provided at no cost to subscribing agencies and do not include any fees for fuel, personnel, or satellite airtime for as long as they are deployed. The FirstNet deployable assets are stationed strategically throughout the county and available to subscribers 24/7/365. AT&T also has a Network Disaster Recovery (NDR) program with hundreds of 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 the Starlink 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.

How does it work?

The deployable assets can provide up to several miles of Band 14 coverage exclusively for public safety use. Range is often dependent on the terrain in which the deployables are set up. These assets are intended to support FirstNet users with

FirstNet-capable devices which have a black FirstNet SIM card or a FirstNet eSIM, to ensure network availability and effective assistance to public safety. They are not intended to support commercial cellular traffic.

Different assets have different capabilities to best support the public safety operational need, and the FirstNet Response Operations Group (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.

"In rural America, we do not have communication. When we initially set up our incident command, we had no phone connectivity. We had no internet connectivity. We had no way of sending data or photos. And unfortunately, many of our tribal nations had no way of contacting us to let us know what they needed. We made a simple phone call to AT&T FirstNet to request a deployable and within 24 hours they established communications for us. We were able to start communicating with our most critical partners — our first responders, our management team, and those working to distribute resources — to respond to COVID-19."

LYNDA ZAMBRANO
EXECUTIVE DIRECTOR, NATIONAL TRIBAL EMERGENCY MANAGEMENT COUNCIL

FirstNet.gov/NTEMC

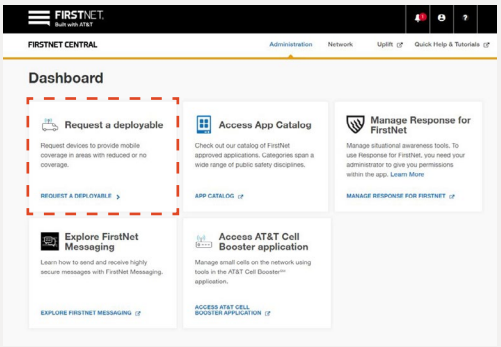
How do you request a deployable solution?

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 agency account managers 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.

Not every request for support will result in a deployable asset being sent by AT&T. With evolutions in deployable technologies and network optimization capabilities, AT&T has new options to provide support to public safety agencies beyond the original SatCOLT vehicles. Once you submit your request using the online tool, you will receive an email confirming your request as well as update emails as your request goes through the triage process and a solution is implemented.

Pro Tips: Access Deployable Request Tile

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



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

When calling FirstNet Customer Care, the requester should be prepared to provide the agency's Foundation Account Number (FAN).

Regardless of how you make the request, the FirstNet ROG will process the request and identify the best solution to deploy for the support request. 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 Account Administrators and Uplift Managers can request deployable assets. Agency Account Administrators can create multiple Account Administrator and Uplift Manager accounts to ensure that personnel are available during emergencies.

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?

Whether you use the online Deployable Request Tool in FirstNet Central or call the FirstNet Customer Care number, 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, wash-outs 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 or weight restrictions, turning radius, and other logistics information when making the request.

For more suggested best practices related to using FirstNet deployables, refer to **Appendix C**.

To review the Deployable Request Form, see **Appendix D**.

Use Case: Hurricane Ian

In September 2022, Hurricane Ian hit the Florida Keys, southwest and central Florida, and coastal cities in North and South Carolina. The Category 4 storm brough high winds and storm surges that presented new communications challenges for first responders. In advance of the storm, FirstNet deployables, including SatCOLTs, CRDs, and a response communications vehicle, were staged in forward operation locations. In the aftermath of the storm, the FirstNet ROG used an amphibious vehicle to deliver a CRD to Sanibel Island when Hurricane Ian destroyed portions of the Sanibel Causeway. A National Guard helicopter delivered a FirstNet CRD to Pine Island where it established immediate connectivity while other networks were still down.

Using the deployable

Every SatCOLT deployable must have a minimum 100-foot safety perimeter and should be placed at least 500 feet away from a command post or other area with heavy responder radio traffic. The asset needs a clear, level, unobstructed view of the southern sky and must be staged in a secure area. The deployable 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. Smaller deployables such as the CRD do not require such a large footprint, but the same basic conditions for parking, securing and operating the assets are still needed.

AT&T technicians are responsible for transporting, setting up, and breaking down the deployable asset. During operation of the asset, they may need access to the deployable to refuel generators, but otherwise the asset will be managed remotely from AT&T's global network operations center (GNOC).

These assets are dependent upon satellite backhaul to connect to the network, which is an important feature to have during emergencies when terrestrial infrastructure may be damaged. While terrestrial connections such as fiber provide the most bandwidth, satellite backhaul is a more limited resource. In some instances, it may be helpful to coordinate and consolidate the use of apps and capabilities that are necessary to the mission to help manage satellite bandwidth.

As part of the FirstNet Authority's in-building investment, agencies can install up to 50 Cell Booster Pro devices across multiple public safety facilities — at no cost to the agency — to boost FirstNet inside the buildings where they work if there's insufficient coverage.

SECTION 4: NETWORK ENHANCEMENTS UNIQUE TO FIRSTNET

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 and in 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, emergency managers now have several options to stay connected from their EOCs to responders in the field.

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 use their devices and communicate with dispatch, the EOC, or field command posts. FirstNet provides a unique technology for keeping responders connected in areas with challenging coverage.

In accordance with the FirstNet Authority's Federal Communications Commission 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. This allows those devices 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 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.

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 injector and a wall adapter for AC power sources.

In urban environments, MegaRange™ can help improve connectivity and data throughput where 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, or operating in rural areas.

"In fringe network areas, HPUE allows us to stay connected with a higher level of reliability. There were still areas that had issues because of geography, and once we brought in HPUE, it helped to fill in those gaps because we can transmit at a higher power. Leveraging HPUE allows us to maintain connections not just for dispatch information but also for connecting our cardiac monitors to send 12-leads from the field,"

LIEUTENANT HUMZA SHAMSUDDIN
TECHNOLOGY DIRECTOR, BRISTOL KENDALL FIRE DEPARTMENT, ILLINOIS

FirstNet.gov/BristolHPUE

In-building solutions

Emergency managers typically work in an EOC, which is usually 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. As a result, EOCs can benefit greatly from FirstNet technologies that help improve indoor cell coverage and provide improved connectivity for emergency managers responding to an incident.

FirstNet Authority Re-investment Supports In-building Coverage Enhancements:

In May 2022, based on feedback received from public safety agencies across the country, the FirstNet Authority Board approved a multi-million dollar investment to address a critical communication priority — enhancing FirstNet coverage in key public safety buildings. The AT&T Cell Booster Pro is a device that acts as a miniature cell tower and improves the quality of indoor FirstNet service in locations such as police headquarters, fire stations, ECCs, or EOCs.

AT&T began offering the devices in September 2022. Through the FirstNet Authority's investment program, up to three devices are available for a single location, and up to 50 devices across multiple locations in a jurisdiction are available, all free to FirstNet subscribing agencies. Agencies can also receive professional installation of the Cell Booster Pros for free under this program. The FirstNet Authority often conducts follow-up interviews with agencies to assess how the program is working. For more information, please visit **AT&T's website.**

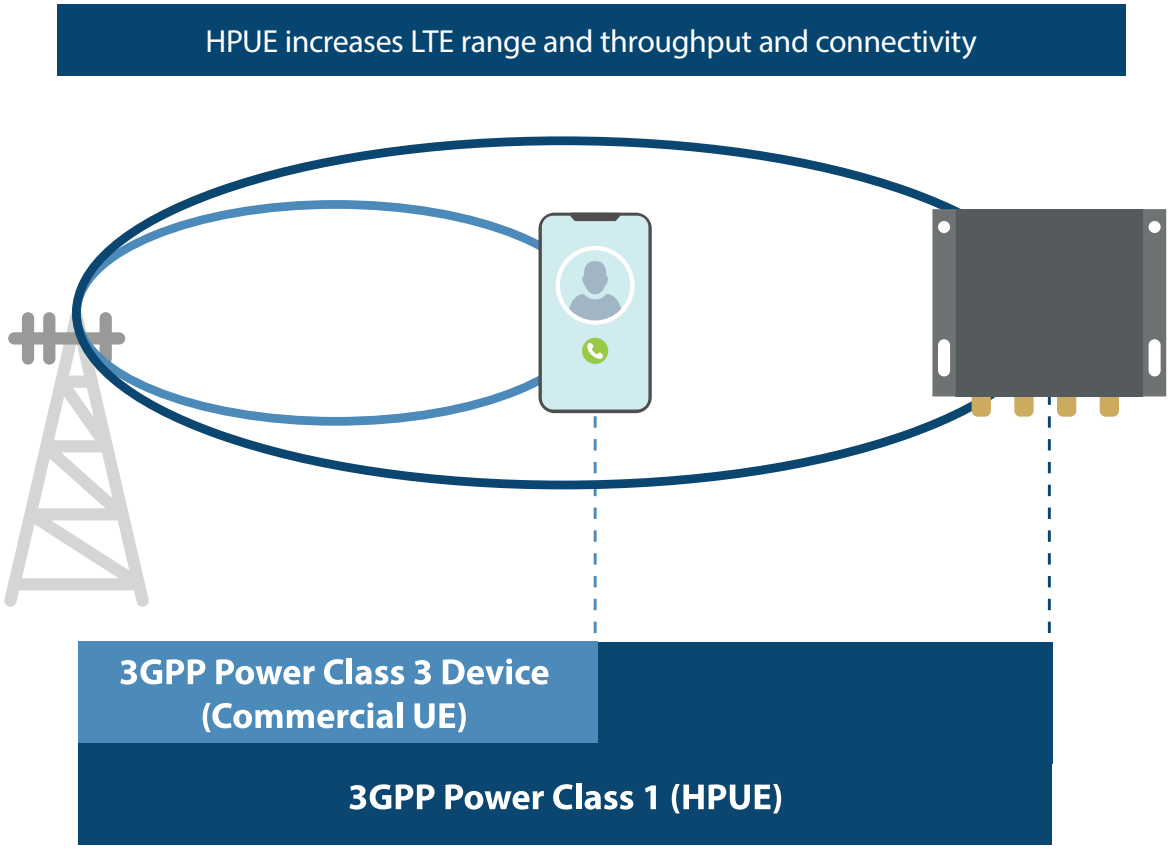
"Everybody has FirstNet for their work phones. This building is an old factory with a lot of masonry inside and around the perimeter of the building. So not only does cell service not get in here very well, but also, radio service doesn't get in here well either. We were missing some of that contact with the EMS supervisors and administration who were in the building. Indoor coverage is much better now. We haven't hit any areas inside the building where we have issues."

JIM GUSLER
EMS DIRECTOR, FRANKLIN COUNTY, NORTH CAROLINA

FirstNet.gov/IndoorEMS

One option for EOCs, either permanent or set up rapidly to respond to an incident, is the MegaFixed HPUE device mentioned above.

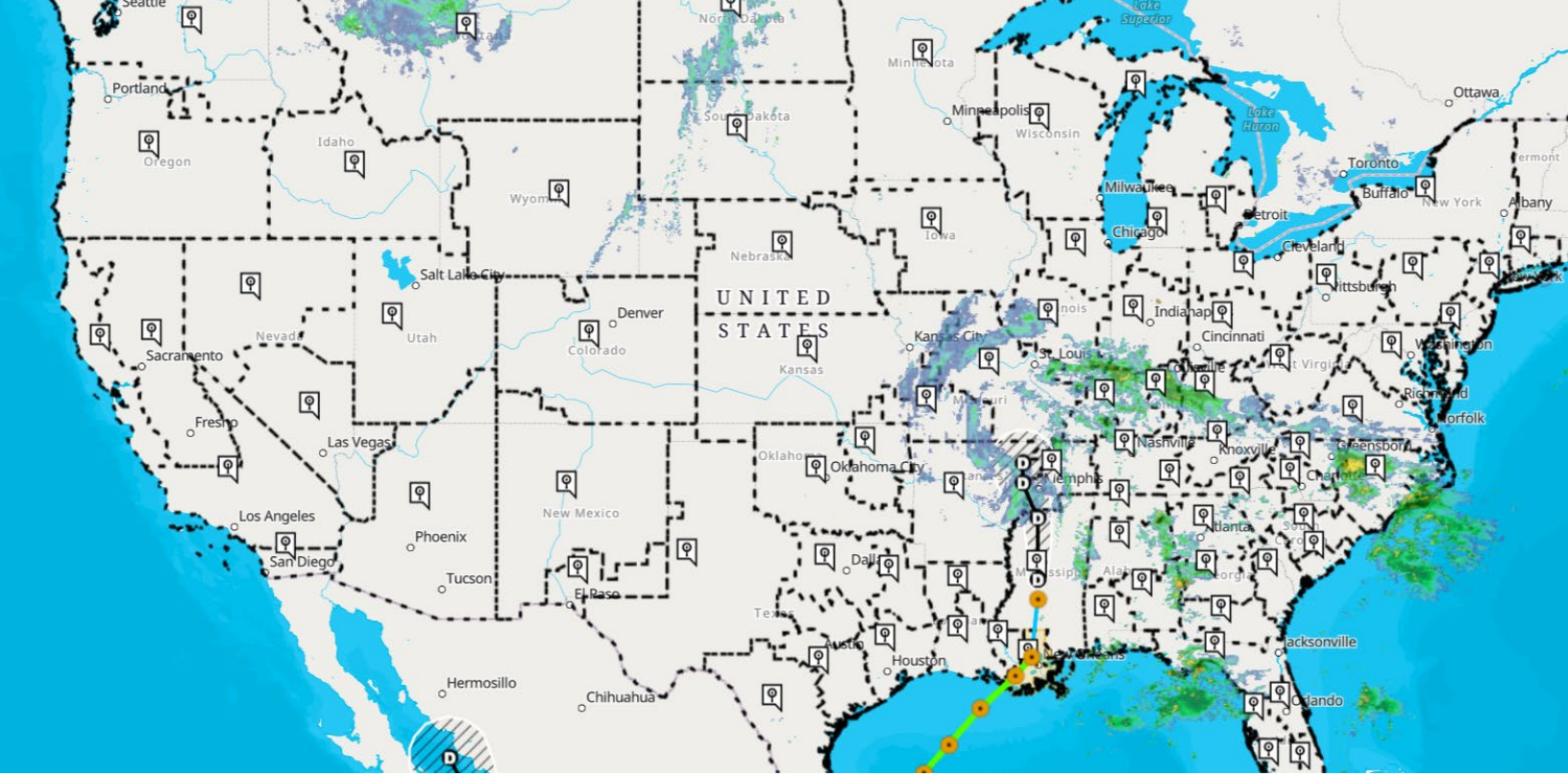
Figure 1: HPUE range information



	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

Another option for permanent EOC 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 three CBPs can be connected in a building to provide up to 45,000 square feet of improved 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.

The **Cel-Fi GO RED** smart signal booster is another in-building enhancement tool that Emergency Managers can quickly deploy to improve indoor coverage when establishing a temporary EOC or command post. The GO RED helps to 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 EOCs where there may not be a wired internet connection, but there is strong FirstNet LTE service outside the facility.



The FirstNet Central portal provides users with access to the Uplift Request Tool, network status information, and other data.

SECTION 5: USING THE NETWORK STATUS TOOL

What is FirstNet Central?

Agencies using FirstNet have access to FirstNet Central, an online system that can be especially useful to Emergency Managers. The tools provided in FirstNet Central can be advantageous for Emergency Managers as they prepare for incidents as well as during response operations. FirstNet Central is available through a **browser-based portal**, meaning it can be accessed from an EOC or from a mobile incident command post with a network connection. It can also be accessed from mobile devices such as smartphones and tablets.

FirstNet Central can be accessed through the FirstNet website: **www.FirstNet.com** and by clicking the "Account" link in the upper right corner of the page; there will be an icon that looks like a person next to it.

The information displayed in this system, particularly the network status maps, is highly confidential and contains sensitive information belonging to AT&T. For these reasons, every time users log in and select the Network Status option, they are asked to agree to use the provided information only for the purpose of assisting first responders in the performance of their official duties. The information presented in the Network Status Tool is not intended to be a source for public safety to make public announcements about the availability (or non-availability) of cellular service in a particular area. In fact, making public announcements based on Network Status Tool alerts may violate the user agreement and preclude future use of the tool by account holders.

FirstNet Central serves two core user groups: administrative and operational. At least one FirstNet Central Administrator is designated for each agency, after which the Administrator can create additional Administrators and user accounts with various roles and permissions. Some users are administrative (general account management, bill paying, ordering equipment, etc.). Other roles include access to FirstNet Central's operational resources, such as the Advanced Network Status Tool, Uplift Request Tool, and Deployable Request Tool.

Pro Tips:
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.

For more help using FirstNet Central, contact your AT&T FirstNet Solution Consultant or consult the Quick Help & Tutorials section on the FirstNet Central portal.

Network Status Tool

The Network Status Tool is designed to increase situational awareness of the status of the FirstNet network and can be accessed via FirstNet Central. This tool enables public safety agencies to assess 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.

Emergency Managers may find this tool useful in their EOC operations 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 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 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 the outage is occurring somewhere within the yellow shaded area. Clicking in the shaded area will display a window with available details regarding the outage.

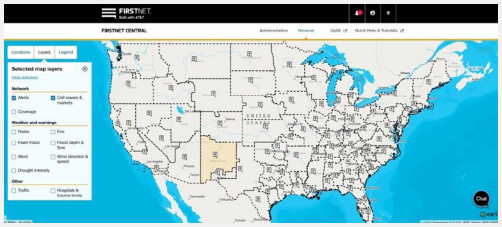
B. Allows users to view on-demand reports on locations scheduled for planned maintenance.

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.

Pro Tips:
Outages in Network Status Tool

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



Advanced Network View

The Advanced Network View provides critical information for Communications Leads, Emergency Support Function #2 personnel, Communications Coordinators, or equivalent roles who can interpret the information and make necessary decisions or recommendations based on the potential impact to communications or operations.

Access to this view is provided by FirstNet agency administrators for specified users.

This view includes everything from the Standard View and adds the following items:

A. The Advanced Network View provides critical information for Communications Leads, Emergency Support Function #2 personnel, Communications Coordinators, or equivalent roles who can interpret the information and make necessary decisions or recommendations based on the potential impact to communications or operations.

B. Markets experiencing outages will be shaded in yellow. Sites within those markets that are experiencing an outage will be indicated by a red icon. Clicking directly on the red icon allows users to review what type of communication technology or services (e.g., LTE, UMTS) are impacted. Clicking on the icon also displays (if known) the cause of the outage (e.g., power, transport). By zooming down to street level, users will see the estimated geographic impact area of a site's outage, denoted as a red hash-marked area.

Access to Network Status Tool

The Advanced Network View is intended for those personnel who have communications expertise, or who are responsible for managing the communications functions (e.g., daily operations, emergency incidents, planned events).

Public safety agencies have the authority to determine which personnel in their department should have access to the Network Status Tool.

Access to the Network Status Tool is determined and provided by each agency's FirstNet Agency Administrator(s). There could be one or more Agency Administrators within an agency. The initial Agency Administrator(s) within any given agency are established by their AT&T FirstNet Solution Consultant when they are onboarded, but subsequently the Agency Administrators assume responsibility for this function.

It should be noted that a special Terms & Conditions statement must be agreed to **each time** a user opens the Advanced Network View and is watermarked with the user's email address to discourage unauthorized sharing of information.

This is the first time we ever had this invaluable [mapping] tool. When I looked at my [Statewide LMR system] map, I knew where we had P25 [Project 25] LMR coverage and then side-by-side, I could pull up FirstNet's LTE coverage [via FirstNet Central]. That was really important to us and helpful during the decision-making process.

It enabled us to make better decisions about where to send our limited resources."

TRAVIS JOHNSON
FORMER STATEWIDE INTEROPERABILITY COORDINATOR, LOUISIANA GOVERNOR'S OFFICE OF HOMELAND SECURITY & EMERGENCY MANAGEMENT

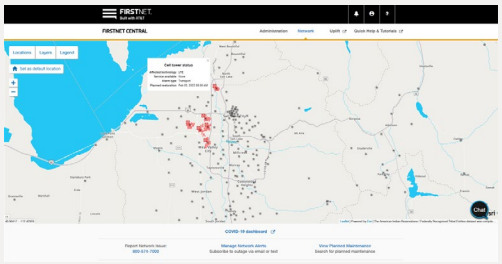
FirstNet.gov/FutureEM

Using the Network Status Tool

Emergency Managers 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.

Pro Tips: Tower Status

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



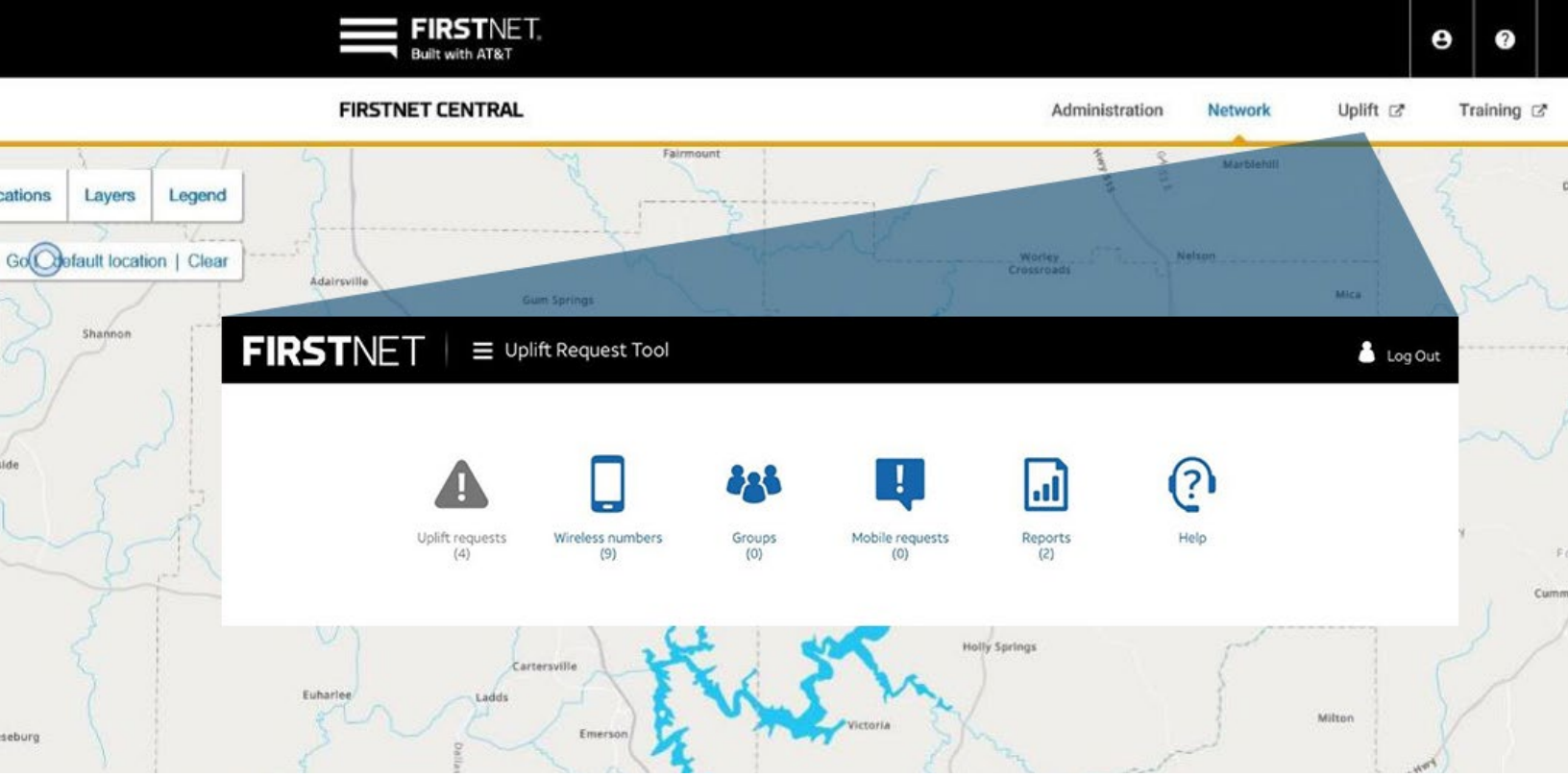
Pre-Planning/Pre-Event Phase:

- 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 EOC 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 & Tutorials link within FirstNet Central.
- Direct designated users to subscribe and receive notification alerts for unplanned network outages within the desired locations via e-mail, 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.

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 Tool periodically until operations are terminated.
- If sending resources, personnel, or teams outside the jurisdiction, check the Network Status Tool for the destination 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 3: Understanding the FirstNet Deployable Program**).
- Depending on circumstances, consider use of the Uplift Request Tool (see **Section 6: Using the Uplift Request Tool**).



The Uplift Request Tool gives the Uplift Request manager(s) the ability to help specified users or groups stay connected when a cell site becomes overloaded during an emergency or planned event.

SECTION 6: USING THE UPLIFT REQUEST TOOL

What is the Uplift Request Tool?

During an incident or planned event, broadband networks can become heavily congested as commercial or consumer 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 of time. Uplift is primarily intended for Extended Primary users that provide support to Primary public safety entities.

The Importance of the Uplift Request Tool

While Primary users have always-on FirstNet priority and preemption for all communications, Extended Primary agencies 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."

Pro Tips: 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**

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 enabled quickly and efficiently for targeted users during an emergency situation.

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

FirstNet Assist Mobile App

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.

When an uplift request is created by an Uplift Request Manager, users with the FirstNet Assist app 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 Manager(s) for the uplift event when users with the FirstNet Assist app submit a request to be added.

When a user with the FirstNet Assist app requests to be added to an uplift event, Uplift Manager(s) for that event will receive information from the requesting user, to include: name of user, user's phone number, agency, job title, alternate contact number, skills, and 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 Manager(s) assigned to the event. Any of the Uplift Managers for the event can either approve or deny the request before it times out. Whether the request is approved or denied, the requesting user and all Uplift Manager(s) will receive a notification. 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.

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

Pro Tips:
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.

Use Case
Indiana Pandemic Response

Tyler Clements, Emergency Response Director for Indiana's Integrated Public Safety Commission, turned to FirstNet to ensure the state's vaccination sites would have the coverage and capacity needed to support multiple federal, state, and local responders. Clements requested a FirstNet SatCOLT to optimize coverage within the two-block area encompassing the vaccination center and relied on the FirstNet Central tool to uplift hundreds of on-site responders to the network, giving them priority access. "Whenever you have that many people in one area, FirstNet is really the only service that's able to deliver to public safety," said Clements.

FirstNet.gov/PandemicDeployables

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.
- Have the Uplift Request Manager(s) 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.

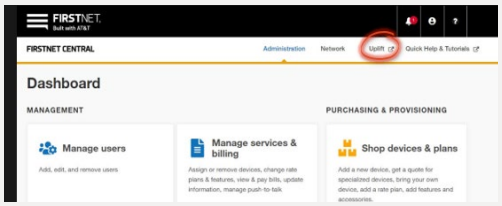
Pre-Event Planning:

- 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 to exclude it from this report. 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.

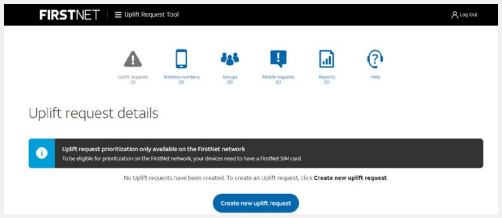
Pro Tips: Finding Uplift

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

FirstNet Central Home Screen



Uplift Request Tool Screen



- 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.
  - In addition to excluding an uplift event from the Nationwide Scheduled Uplift Requests report, if you also 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. However, once the scheduled uplift event goes live, it will then 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.

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.
  - It is recommended to designate at least two Uplift Request Managers, based on the operational period or duration of the incident.
- If an uplift event expires but was needed for a longer period of time, 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 are able to 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, with the exception of 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."

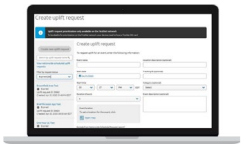
"One of the things we love about working with FirstNet is the fact that not everybody has the same cell phone capabilities. That's how FirstNet works with us – getting together all these community partners and providing the same communication."

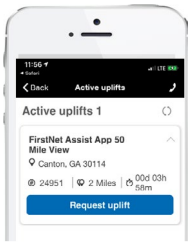
THOMAS MUNOZ
FORMER EMERGENCY MANAGER AND HOMELAND SECURITY DIRECTOR, TEXAS CITY

FirstNet.gov/Hurricane2021

Pro Tips: Uplift Planning

1. Name the uplift event similar to the pre-planned or emergency incident name.
2. Decide whether to make the event private or visible to FirstNet Assist app users, and whether it should appear on a report of future uplift events.
3. Review the uplift request prior to the event by accessing the Uplift Request Tool on a laptop, desktop, or mobile device.





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.

SECTION 7: FIRSTNET DEVICES AND APPLICATIONS FOR EVERYDAY USE

Emergency Managers have many new tools and technologies at their disposal, and this universe of devices and apps will only grow as more solutions are developed to meet public safety's needs. This section will discuss some of the considerations for selecting devices and apps for emergency management in order 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** maintains a list of these devices. The list is accessible at: **www.nist.gov/ctl/pscr/process-document-nist-list-certified-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, including the FirstNet Evolved Packet Core and Band 14. Devices that have a FirstNet Ready® badge support access to Band 14 — FirstNet's public safety spectrum — and are able to work on the FirstNet Evolved Packet Core simply by installing a FirstNet SIM card.

For Emergency Managers 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.

"Combining the technology with usable devices that are ruggedized is very important to what we do in emergency services, because we're not always operating in appropriate conditions. I remember a time when a fire call came in and during the rush to respond, my phone pops out of my pocket and rolls up under the fire truck. The fire truck pulls out and it runs over my phone, but the ruggedized device survived getting run over by a fire truck and it's still usable today! These devices from regular cell phones to tablets to computers to modems and routers and all the things that we need now in our daily operations, come together in one system that provides security and availability when we need it most."

TERRY JOHNSON
EMERGENCY SERVICES DIRECTOR, ESSEX COUNTY, VIRGINIA

FirstNet.gov/Devices

Using FirstNet Devices on 5G

One of the first investments the FirstNet Authority Board approved supported initial generational upgrades to the FirstNet Core. In April 2021, AT&T announced the upgrades to the Core were complete and FirstNet subscribers gained access to AT&T's 5G mmWave spectrum in parts of a growing number of cities and venues.

First responders maintain voice and data communications with priority and preemption on LTE, while the FirstNet network determines the best route for data traffic, whether that's LTE spectrum, 5G, or 5G+, without customer action. 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, there are two courses of action FirstNet users can take, depending on whether the device is provided by their agency (Agency Paid) or they pay for their own device and FirstNet plan (Subscriber Paid).

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.
- Contact the relevant AT&T FirstNet Solution Consultant to better understand specific 5G coverage.
- Visit **FirstNet.com/devices** to determine if your device is 5G capable or if you'll need to acquire a new device.
- Finally, 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.
- Determine if the device is 5G capable.
- Log in to the FirstNet account and modify the rate plan, OR call FirstNet Customer Care or visit a retail store to obtain a 5G-capable device certified for use on FirstNet and move from a 4G to 5G rate plan.

Pro Tips:
FirstNet and IPAWS

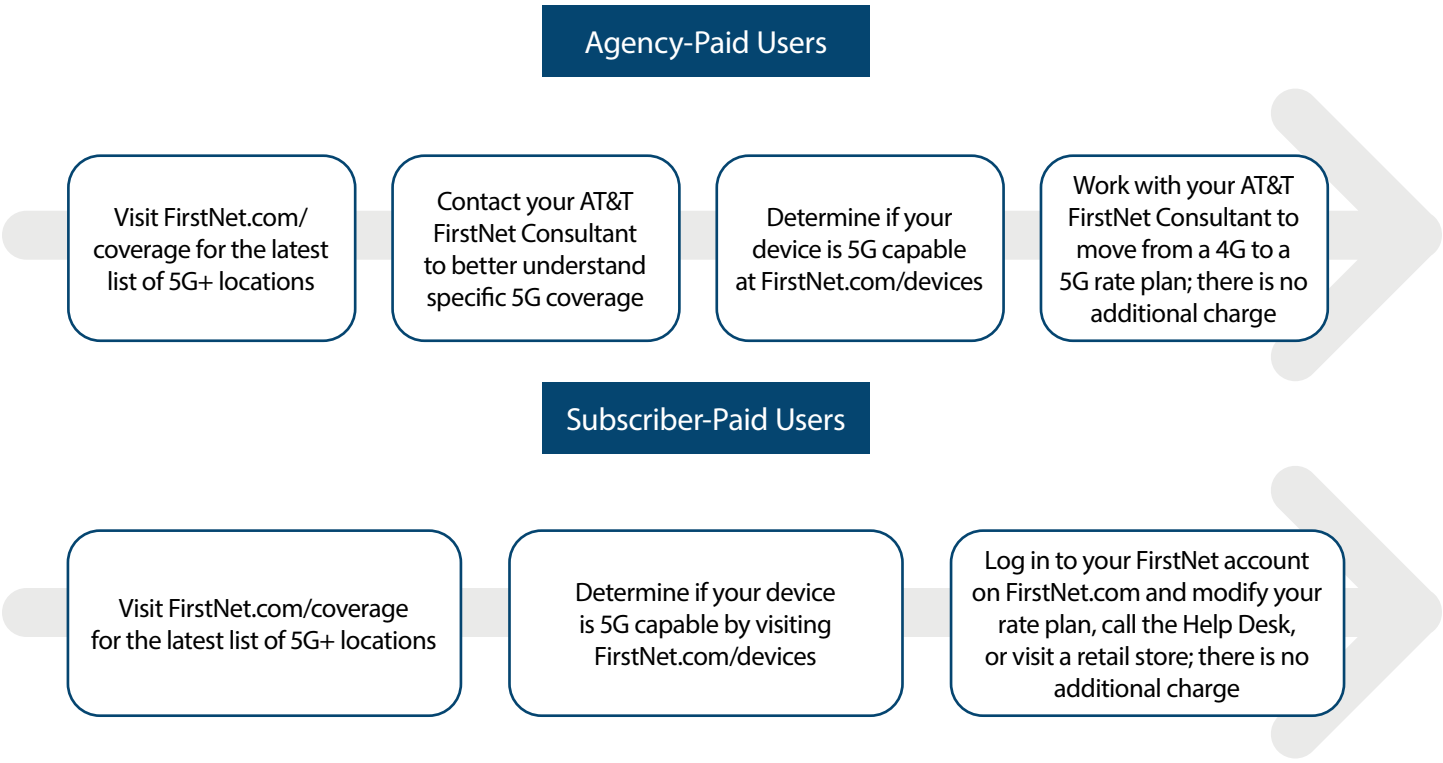
The FirstNet Authority and FEMA's Integrated Public Alert and Warning System (IPAWS) are working together to support alerting authorities and educate and encourage alert and warning software developers to submit their applications to the FirstNet App Developer Portal for testing and certification.

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 (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

Figure 2: Steps to access 5G on FirstNet



(including Wireless Emergency Alerts, or WEAs), Emergency Managers are encouraged to use dual-certified IPAWS and FirstNet alert origination software available to public safety in the FirstNet App Catalog. This software will help 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 App Catalog

FirstNet users have access to the **FirstNet App Catalog**, which identifies pre-evaluated and 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 consisting of members of 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.

Emergency Managers can search for FirstNet Verified™ and FirstNet Certified™ apps in many 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, Emergency Managers 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

Similar to 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**.

By working with FirstNet, mobile app providers can integrate purpose-built and exclusive features. FirstNet provides tools for app developers, including a Single Sign-On Software Development Kit (SDK) and an App Priority™ Application Programming Interface (API). FirstNet apps can include vertical positioning for z-axis mapping, authentication for single sign-on, and device and app uplift for heightened network prioritization. FirstNet app providers can also enhance their solutions with the integration of Mission Critical Push-to-Talk and FirstNet Messaging designed specifically for public safety. The FirstNet App Developer Portal is also the avenue for app developers to submit apps for inclusion in the FirstNet App Catalog. Learn more at **Developer.FirstNet.com/FirstNet**.

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.

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.

SECTION 8: USING A FIRSTNET DEVICE CACHE

There are many preparedness measures that Emergency Managers 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.

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. In addition, 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 for your mission. See the latest apps at **FirstNet.com/Apps** or learn more in **Section 5**.

Enabling mutual aid during an emergency

Maintaining a cache of FirstNet Ready® devices may improve response by enabling the rapid deployment of devices when mutual aid forces that are not regular partners of the affected jurisdiction arrive on scene. 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) 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 for accountability and to ensure the devices are returned after an event has concluded.

"FirstNet has been a great resource. They were there when we've needed them. Whether it was the pandemic, wildfires, or an ice storm, they showed up and helped us improve communications for public safety and emergency management responders. The local FirstNet, Built with AT&T team has also been instrumental in our ability to selectively activate and deploy our Statewide Interoperability Program owned caches of FirstNet devices. Supported by the FirstNet fleet of deployables, these caches have allowed us to get FirstNet service into incident responders' hands, when they needed it most."

WILLIAM CHAPMAN
STATEWIDE INTEROPERABILITY COORDINATOR,
STATE OF OREGON

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)

Pro Tips: 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.

- 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 (hotspots, larger access points such as mobile routers or in-building devices, CRDs, etc.)
- Training on devices/applications that may not be familiar or regularly used
- Cache maintenance and use
  - 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.
  - Identify the cache storage location.
  - Determine appropriate Point(s) of Contact for access to the cache.
  - Establish processes to transport the cache.
  - Establish a method to track the assignment of cache devices for accountability and demobilization.

- Identify costs to develop and maintain the cache.
- Train with cache devices.
- Develop Credentialing and Access Management policies and procedures to ensure users can log into devices that are distributed from the cache.

Pro Tips: 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.

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.

SECTION 9: INCORPORATING FIRSTNET INTO YOUR COMMUNICATIONS PLANS

As technology evolves and becomes more ubiquitous, it is critical that communications plans reflect those advances. Emergency Managers 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

Emergency Managers can speed up equipment deployment and reduce the stress of providing robust communication capabilities at an incident scene 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.

Pro Tips: Plan for Requesting a Deployable

Agencies may work with AT&T in advance to understand the roles and responsibilities associated with requesting a deployable asset or other need.

For additional information on requesting a deployable, visit **FirstNet.gov/Deployables** or **Section 3**.

Some questions to ask during this planning process may include:

- 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 (gas, telecom, electric, etc.)
- How are you currently communicating today?
- What devices and applications are these agencies already using?
- How do you track the locations of resources (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 process to request a deployable? A state process?

Emergency Support Function 2

The ESF-2 section of an emergency management 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 EMA staff and EOC 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 type of information can be useful when coordinating an Uplift Request (read more in **Section 6**) or when staging a deployable (read more in **Section 3**). For an example of form ICS 205A, see **Appendix E**.

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 better enable a unified approach to emergency response.

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

"We were strategic in our switchover to FirstNet. We started with routers to see how the system handled the large amount of data that is shared between the city's Emergency Communications Center and the field units. Next, we began to switch out cellular devices for those that had city-issued phones in public safety. We meet with the FirstNet team once a month, now virtually, to talk about any issues, what's going well, and what's to come."

BOBBY GELORMINE
SENIOR PLANNER, CITY OF CHESAPEAKE FIRE DEPARTMENT, VIRGINIA

FirstNet.gov/Chesapeake

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

A PACE (Primary, Alternate, Contingency, and Emergency) communications plan establishes predictable and redundant communications capabilities and 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.

For more on PACE planning, see: **Leveraging the PACE Plan into the Emergency Communications Ecosystem, Apr. 2023 (cisa.gov)**

Use Case: Field Operations Guide Example

In 2019, the Missouri Department of Public Safety included four FirstNet network-specific areas in its Field Operations Guide: deployables, recommended interoperable applications per discipline, information on the Uplift Request Tool, and FirstNet Central.

FirstNet.gov/Missouri-Guide

During Indiana's Terre Haute air show, local, state, and federal first responders deployed FirstNet to provide a robust interoperable broadband connection for all public safety entities.

SECTION 10: NETWORK EXPERIENCE ENGAGEMENT PROGRAM

The key to an efficient response for public safety officials is familiarity with their technology and tools. The FirstNet Authority Public Safety Engagement 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 through our engagement efforts. Contact the FirstNet Authority Public Safety Advisor for your state or territory by visiting **FirstNet.gov/advisor**.

Agencies can engage with the FirstNet Authority in facilitated discussions intended to work through pre-incident or event planning, exercise support, and post-incident or event reviews. Details on each engagement are outlined below.

Incident Pre-Planning

Emergency Managers are constantly planning ahead for all 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. During the planning session, the FirstNet Authority team will lead a discussion to 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

- Enhanced Push-to-Talk/FirstNet Push-to-Talk
- 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.

"Planning for large events is multi-faceted. An often-overlooked item is infrastructure planning, especially wireless communications. Most infrastructure systems are designed for a certain population. Working with the FirstNet Authority helps us understand the existing capacity around a planned event and potential solutions to fill any gaps. They also work with us to prepare a communications plan with redundancy."

KEVIN FRIIS
PLANNING MANAGER, CUYAHOGA COUNTY, OHIO
OFFICE OF EMERGENCY MANAGEMENT

FirstNet.gov/OperationalAssistance

Pre-Planned Events

Similar to emergency incident pre-planning discussions, the FirstNet Authority is available to engage with your agency about public safety broadband capabilities needed at your upcoming special event. Whether it's a county fair or a large National Security Special Event (NSSE), the FirstNet Authority has the ability to scale a planning engagement session to fit your needs. 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 (e.g., police, fire, EMS, EOCs, ECCs)
- Broadband capabilities needed, including but not limited to:
  - Voice/text/email
  - Enhanced Push-to-Talk/FirstNet Push-to-Talk
  - 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

Working alongside public safety officials during all phases of the event planning process provides the FirstNet Authority with valuable feedback on their 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. Additionally, your agency will receive maps marked with the locations you identified as well as a document with the details you provided about the locations, capabilities, and technologies you will be using during the event. All of this information is also provided to the FirstNet ROG to assist them in determining the right solution for your event.

"For our communications team, it has become standard protocol to reach out to the FirstNet Authority before any pre-planned event to ensure we have the broadband solutions and coverage we need. There's nowhere else that we can get that level of expertise about broadband and FirstNet capabilities. I recommend getting the FirstNet Authority involved early to help pre-plan — they are a huge help."

CHRIS CARNEY
FORMER COMMUNICATION SYSTEM SPECIALIST, ORANGE COUNTY, NEW YORK DEPARTMENT OF EMERGENCY SERVICES

FirstNet.gov/After-Action

Post Incident/Event Review (PIER)

PIERs are valuable tools for both the FirstNet Authority and users of the FirstNet network. Through the 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 (CAP), the FirstNet Authority PIER provides information and considerations that emergency management 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.

Use Case

Rhode Island Exercise at T.F. Green International Airport

In the winter of 2020, the Rhode Island Emergency Management Agency tested the FirstNet network's capabilities during a simulation of an aircraft accident with mass casualties. Rhode Island public safety and public health representatives at the exercise needed to be able to communicate over a long distance — from the exercise scene to the emergency communications center. Rather than use LMR devices, they turned to broadband communications to facilitate the transfer of complex messages over extended distances and view data in real time.

FirstNet.gov/Airport

The majority 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 (HSEEP) Master Scenario Events List (MSEL) 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.**

FirstNet Boulder Lab and Public Safety Immersive Test Center

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 quality of service; priority and preemption; enhanced situational awareness technologies and applications; and future public safety functions, services, and applications.

The Public Safety Immersive Test Center (PSITC), managed in partnership by the FirstNet Authority and the National Institute of Standards and Technology's (NIST) Public Safety Communications Research Division, is a state-of-the-art

facility designed to spur the development and deployment of communication technologies for public safety. The center offers a controlled environment where first responders and technology developers can evaluate new equipment and applications in realistic scenarios.

The Boulder FirstNet Lab and Public Safety Immersive Test Center are located at the technical office of the FirstNet Authority in Boulder, Colorado.

Experts at the Boulder FirstNet Lab are available to provide in-person and virtual demonstrations. Lab tours are open to any public safety agency or first responder, whether they're subscribed to FirstNet, considering using FirstNet, or just want to learn about public safety broadband technology. Access to the PSITC may be scheduled at no cost to public safety agencies and supporting organizations within the private sector and academia.

If you would like to set up a tour, please visit **FirstNet.gov/Lab**.

The FirstNet Authority participated in communications planning for the 2023 Super Bowl in Glendale, Arizona, as part of our Network Experience and Engagement Program. Over 14 months, the planning committee worked with public safety agencies, military partners, utility companies, health organizations, and communication providers to determine the right solutions to support the event.

CONCLUSION

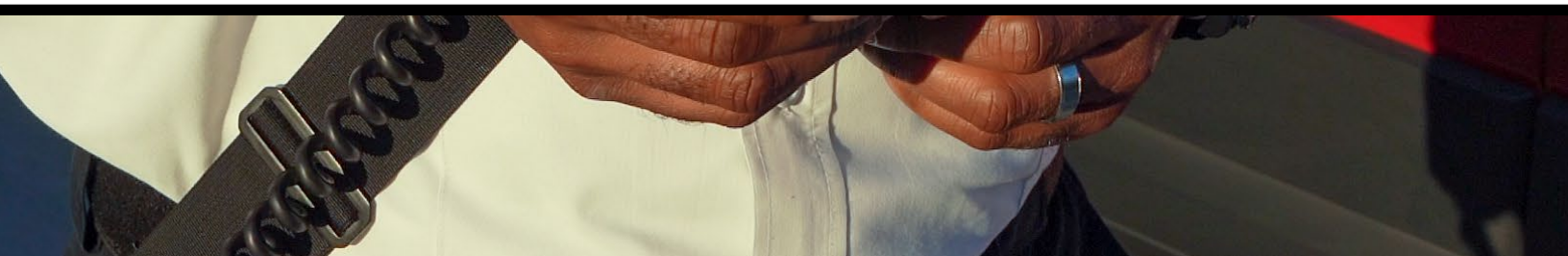
This has been a high-level overview of the tools and technologies available to FirstNet users. As more public safety agencies and individuals join FirstNet for their broadband communications needs, this guide will continue to serve as a reference for specific features and functions that Emergency Managers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

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 Emergency Managers 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/EM**.

More information can be found by following the links in **Appendix A: Contact Guide**.

For more information about Emergency Management and FirstNet, visit FirstNet.gov/EM.

Gainesville Fire Rescue in Florida tested FirstNet across the county to see the benefits in every aspect of their response. The agency manages specialized teams such as HAZMAT response, urban search and rescue, and advanced emergency medical services.



APPENDICES

APPENDIX A: CONTACT GUIDE

APPENDIX B: GLOSSARY

APPENDIX C: BEST PRACTICES FOR USING FIRSTNET DEPLOYABLES

APPENDIX D: FIRSTNET DEPLOYABLE REQUEST FORM

APPENDIX E: SAMPLE ICS 205A FORM INCORPORATING FIRSTNET DEVICES

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: 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 (911) 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.

APPENDIX C: BEST PRACTICES FOR USING FIRSTNET DEPLOYABLES

This is a list of suggested Do's and Don'ts for an efficient and effective use of the FirstNet deployables program. A list of deployable site requirements can also be found at: **www.firstnet.com.**

DO	DON'T
Know who is authorized to request a deployable. Know how to request a deployable (access Deployable Request Tool on FirstNet Central, call AT&T FirstNet Solution Consultant, or call FirstNet Customer Care at 1-800-574-7000). If calling FirstNet Customer Care, be prepared to provide the agency's FirstNet Foundation Account Number (FAN).	Don't assume support was requested. A deployment request form from an authorized FirstNet user must be submitted to formally start the process.
Specify any problems that are being experienced and describe why the deployable is being requested. Identify locations where coverage is needed, the approximate number of users, and the approximate number and types of devices in use. Explain what the devices will be used for and what capabilities will be needed (e.g., voice, text, email, apps, data, images, video, web browsing, sensors).	Don't specify a particular solution. AT&T has many resources and will work with you to identify the best solution for your coverage needs.
Provide incident conditions (environmental concerns, extreme cold/heat, high winds, potential hazards) and how large the incident site is. Discuss terrain and access (passable roads, steep inclines or sharp curves, wash-outs, height/weight clearances or restrictions, escort requirements). Discuss site location information (security, level ground, clear 100' x 100' site for placement, >500' from any command post, clear view of southern sky, access for refueling generator).	Don't assume that a specific deployable or solution will automatically be deployed to a desired location. The AT&T Response Operations Group (ROG) will evaluate requirements and deployment conditions in order to send the most appropriate solution to meet the request.
Request a deployable for a planned event at least 30 days in advance. 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. Plan ahead to request deployables and use FirstNet devices/caches before they are needed.
Use deployables responsibly. They are dependent on satellite bandwidth, which is a very limited resource. 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 (see **Section 8: Device Caches**). Plan 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. Agencies can consider procuring their own cache of devices before an emergency, including mobile data hotspots that can be used to help connect non-FirstNet devices to the deployable's signal.
Remember to request a Post Incident/Event Review from the FirstNet Authority to let us know about your experiences, successes, and challenges. We need your feedback to continue to improve the program.	Don't forget to review what worked well and any areas of improvement following a deployment. The FirstNet Authority can help identify successes and deficiencies after an event, as well as future considerations to help make the next deployment go more smoothly.

APPENDIX D: FIRSTNET DEPLOYABLE REQUEST FORM

A fillable FirstNet Deployable Request Form can be found online at: **www.firstnet.com/content/dam/firstnet/white-papers/firstnet-deployable-request-form.pdf**

This form is intended as a reference for agencies that are considering requesting a FirstNet deployable, in order to collect all of the necessary information that will be requested by AT&T when filing the request. Having this information at hand when making the request will speed up the process and ensure that AT&T can appropriately evaluate and manage the deployment request.

Note that the fillable form does not constitute filing the actual request. Agencies should review the form and collect as much detail about the situation as they prepare to request assistance.

Deployables can be requested in one of three ways:

1. By logging onto FirstNet Central (**https://localcontrol.firstnet.att.com**) to use the Deployable Request Tool
2. By calling the Agency's AT&T FirstNet representative
3. By calling the FirstNet Customer Care number (1-800-574-7000) and saying the word "deployable" during the automated menu prompts.

APPENDIX E: SAMPLE ICS 205A FORM INCORPORATING FIRSTNET DEVICES

A sample Incident Command System (ICS) 205A form incorporating FirstNet Primary and Extended Primary users, along with other carriers, is included in the following pages.

A fillable version of the ICS 205A form can be found at **training.fema.gov/icsresource/icsforms.aspx**.

COMMUNICATIONS LIST (ICS 205A)

1. Incident Name: Sample: Severe Traffic Incident	2. Operational Period: Date From: Date To: Time From: Time To:

3. Basic Local Communications Information:

Incident Assigned Position	Name (Alphabetized)	Method(s) of Contact (phone, pager, cell, etc.)
Law Enforcement Commander		202-555-1212 (FirstNet phone, Primary)
Fire Commander		202-555-1213 (FirstNet phone, Primary)
EMS Commander		202-555-1214 (FirstNet phone, Primary)
Operations Section Chief		202-555-1215 (Verizon phone)
Transportation Unit Leader		202-555-1216 (FirstNet phone, Extended Primary)
Towing Strike Team Leader		202-555-1217 (FirstNet phone, Extended Primary)
Utilities Strike Team Leader		202-555-1218 (T-Mobile phone)

4. Prepared by: Name:_____ Position/Title:_____ Signature: _____

ICS 205A
Communications List

Purpose. The Communications List (ICS 205A) records methods of contact for incident personnel. While the Incident Radio Communications Plan (ICS 205) is used to provide information on all radio frequencies down to the Division/Grouplevel, the ICS 205A indicates all methods of contact for personnel assigned to the incident (radio frequencies, phone numbers, pager numbers, etc.), and functions as an incident directory.

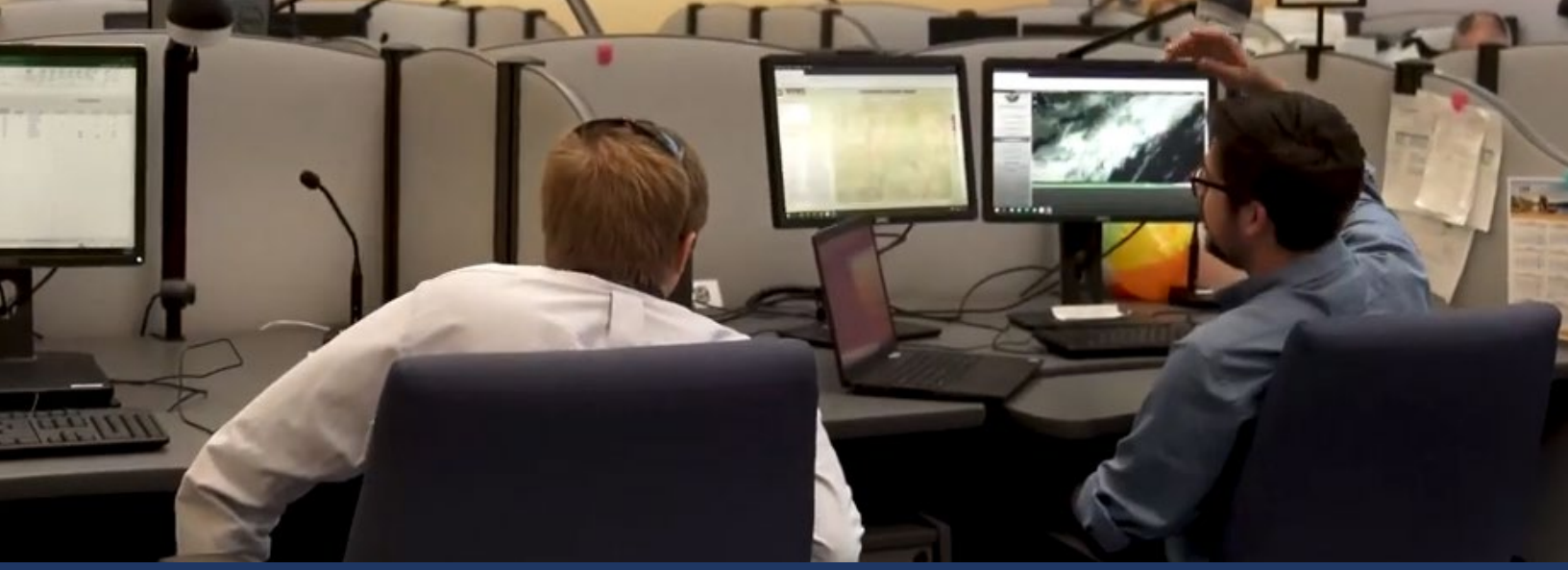
Preparation. The ICS 205A can be filled out during check-in and is maintained and distributed by Communications Unitpersonnel. This form should be updated each operational period.

Distribution. The ICS 205A is distributed within the ICS organization by the Communications Unit, and posted as necessary. All completed original forms must be given to the Documentation Unit. If this form contains sensitive information such as cell phone numbers, it should be clearly marked in the header that it contains sensitive information and is not for public release.

Notes:

- The ICS 205A is an optional part of the Incident Action Plan (IAP).
- This optional form is used in conjunction with the ICS 205.
- If additional pages are needed, use a blank ICS 205A and repaginate as needed.

Block Number	Block Title	Instructions
1	**Incident Name**	Enter the name assigned to the incident.
2	**Operational Period** • Date and Time From • Date and Time To	Enter the start date (month/day/year) and time (using the 24-hour clock) and end date and time for the operational period to which theform applies.
3	**Basic Local Communications Information**	Enter the communications methods assigned and used for personnelby their assigned ICS position.
	• Incident Assigned Position	Enter the ICS organizational assignment.
	• Name	Enter the name of the assigned person.
	• Method(s) of Contact (phone, pager, cell, etc.)	For each assignment, enter the radio frequency and contact number(s)to include area code, etc. If applicable, include the vehicle license or ID number assigned to the vehicle for the incident (e.g., HAZMAT 1, etc.).
4	**Prepared by** • Name • Position/Title • Signature • Date/Time	Enter the name, ICS position, and signature of the person preparingthe form. Enter date (month/day/year) and time prepared (24-hour clock).



FirstNet Authority Resources for Emergency Managers

Emergency Management Take

Sign up for our newsletter to understand the impact of public safety broadband on your operations. You hear directly from our emergency management subject matter expert in a quarterly dive deep into public safety broadband topics important to your discipline.

FirstNet.gov/Newsletters

Emergency Management Page

Check out this one-stop shop and learn about FirstNet for Emergency Managers.

FirstNet.gov/EM

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

FirstNet Authority Public Safety Advisors

If you need assistance in your local area, reach out to a FirstNet Authority public safety advisor.

FirstNet.gov/Advisor

FirstNet Devices

Learn how public safety agencies are using FirstNet devices. These devices include smartphones, tablets, routers, modems, and wearables that use FirstNet network capabilities to meet first responders' unique needs.

FirstNet.gov/Devices

FirstNet Apps

Learn how public safety agencies are using apps over FirstNet and get a link to the FirstNet App Catalog.

FirstNet.gov/Apps

FirstNet Deployables

Get all the details on the deployables program, a unique element of FirstNet. 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 Authority

First Responder Network Authority

info@FirstNet.gov | FirstNet.gov

@firstnetgov