SAMSUNG

White Paper:

Migrating to FirstNet®: The Definitive Guide

How to take full advantage of the dedicated communications network built for public safety

Migrating to FirstNet

Public safety has long faced communications challenges during major incidents, especially when multiple agencies are involved. After the lessons learned during the 9/11 terrorist attacks, Congress established the First Responder Network Authority with a singular, compelling mission: Develop, build and operate the nationwide broadband network that equips first responders to save lives and protect U.S. communities. That network, known as FirstNet, is available to all first responders across the country today.

This guide will help public safety agency leaders understand the operational benefits of FirstNet and plan a successful transition to the network that was designed by and for first responders. It contains information and guidance on all the following:

- The key advantages of FirstNet
- How FirstNet supports more effective response to major incidents
- Laying a foundation for your FirstNet migration
- Deploying mobile devices to your personnel
- Effective device security and management

Part 1: The Network That Public Safety Needs

For decades, the basic communication needs of public safety were met with traditional land mobile radios (LMR). Today, however, agencies are pursuing new solutions that augment LMR with mobile apps delivered by smartphones, tablets and wearables. Mobility has great potential for public safety, but public safety leaders have been reluctant to rely on mobile technologies for mission-essential communications or information access due to concerns about reliability. Cellular frequencies can become overloaded and, as the dependence on data increases, bandwidth limitations often restrict the ability to effectively share essential information.

Major incidents involving large numbers of personnel are particularly challenging, especially when they occur in densely populated areas where there is competing demand for cellular bandwidth. At times when they're most needed, conventional cellular networks can become so congested that public safety cannot depend on them for essential transmissions. For example, during the Boston Marathon attack aftermath, cellular networks became overloaded, and calls could not go through.[1]

The FirstNet Advantage

FirstNet provides first responders with priority access, including preemption, to a reliable public safety network capable of transmitting large volumes of mission-essential information, including video, high-resolution photographs, geolocation services and access to cloud-based data such as detailed maps of critical infrastructure. Increasingly, mobile technology has become a force multiplier, improving overall situational awareness and effectively using very limited resources. However, data that doesn't get to the decision makers is worthless.

FirstNet always prioritizes first responder public safety data traffic and makes it possible for law enforcement, fire and EMS personnel to use their technology assets with minimal concern that they will be hampered by a congested or overtaxed cellular network. In some situations, FirstNet allows first responders to preempt commercial users of the network to help ensure that public safety has network access.

Authorized by an act of Congress in 2012, the First Responder Network Authority operates as an independent authority within the National Telecommunications and Information Administration, which is part of the U.S. Department of Commerce (DOC). In March of 2017, the First Responder Network Authority announced a private/public partnership with AT&T to build and manage the nation's first broadband network that will provide real-time, always-on priority and preemption to first responders.

That network, along with various other communications services and capabilities, is known as “FirstNet.” Under the 25-year agreement, the First Responder Network Authority is leasing 20MHz of spectrum and success-based payments totaling $6.5 billion to build out additional coverage on the network over the first five years. AT&T is spending approximately $40 billion over the life of the contract and investing in expanding its network infrastructure and cellular bands, which will be augmented by the FirstNet spectrum, to provide more than 160MHz of nationwide spectrum to operate and maintain a robust, nationwide public safety network.[2] FirstNet is available to all first responders across the country today.

FirstNet provides first responders with priority access, including preemption, to a reliable public safety network capable of transmitting large volumes of mission-essential information.

FirstNet Facts

25 years
Agreement between First Responder Network Authority and AT&T

20MHz
Additional spectrum provided by FirstNet

$40 billion
AT&T investment over life of contract to expand network infrastructure

How FirstNet Works

FirstNet is unlike any other communications network; among other things, it has a physically separate, dedicated public safety core. Public safety communications and data are supported across all the current bands on the AT&T network, as well as the 20MHz of additional spectrum from the 700MHz band provided by FirstNet (commonly known as Band 14). To help ensure reliability, FirstNet features additional resiliency and redundancy, as well as extensive hardening of the network. At all times, first responder public safety personnel have priority and preemptive capabilities to maintain sufficient bandwidth for high-demand data usage, even when the commercial networks available to the public are totally overloaded.

Use of the 700MHz spectrum is noteworthy because this band of frequencies has particularly effective propagation (signal penetration) when it comes to buildings and larger geographic areas. FirstNet prioritizes the traffic from first responder public safety devices and can invoke preemption when necessary. When preemption is invoked, the network prioritizes FirstNet traffic and can relocate and, when necessary, disconnect lower-priority transmissions. This mission critical feature gives first responders the ability to reliably communicate and coordinate during emergencies and large events. FirstNet also features available end-to-end encryption, round-the-clock security monitoring and overall superior reliability and availability.

FirstNet is designed to support the day-to-day operations of first responders and provide the functional foundation for existing and emerging technologies that demand a reliable and high-capacity network. Effective FirstNet solutions will improve team communications and situational awareness, enhance device security and mobile device management, provide highly secure connections to public safety applications and access cloud services to optimize agency endpoint computing. FirstNet capabilities like enhanced push-to-talk (EPTT), and soon to be deployed mission-critical push-to-talk (MCPTT), as well as location-based services, will synergize public safety technology devices and applications in ways that traditionally have not been possible.

> At all times, first responders have priority and preemptive capabilities to maintain sufficient bandwidth for high-demand data usage, even when the commercial networks available to the public are totally overloaded.

Part 2: Managing Major Incidents With FirstNet

Scenario 1: Active Shooter

Gunfire rings out in a busy shopping mall in a mid-sized city, causing instant panic. Calls pour into the 911 center, and a request goes out to adjacent agencies for assistance. One of the shoppers captures a short video clip of the shooter and shares it with the first officer to arrive on scene. The video, although recorded with a cell phone, shows enough detail to construct a good description of the suspect. It can also be determined that his weapon is a long gun — probably a high-capacity rifle.

The officer quickly provides this information to responding units by voicing the details and pushing the video out to their FirstNet equipped devices. Responding officers can see the video on their in-vehicle mobile data terminal, smartphones and tablets, and officers already on scene can view the video on their issued smartphones. A photo of the suspect is also shared with all police officers and other emergency responders in real time over smartphones and tablets on FirstNet. The information regarding the suspect's weapon allows officers to make critical decisions in terms of positioning, selection of cover and use of the highest level of available body armor.

Because all responding officers, including those from other agencies, are equipped with smartphones, real-time geolocation reporting is possible. This allows the commander to see individual officer locations and effectively manage resources. The commander is also able to quickly access a cloud-based file containing a detailed layout of the shopping center complex, including fire exit doors and the names of individual stores. This diagram can easily be shared with other units on scene, greatly improving the situational awareness of the officers. Ultimately, the combination of timely information combined with effective deployment results in the capture of the suspect as he tries to change locations. Despite congestion on the commercial cellular network, responding officers' calls and critical mission data get through because of the priority and preemption provided by FirstNet.

Despite congestion on the commercial cellular network, responding officers' calls and critical mission data get through because of the priority and preemption provided by FirstNet.

The firefighters' equipment has integrated sensors that stream status reports to incident command by pairing with smartphones.

Scenario 2: Large-Scale Multiple-Agency Fire Response

After a long spell of hot, dry weather, a wildland fire erupts near an area of new home construction. Dozens of partially-built homes line newly paved streets, and the huge amount of exposed and onsite lumber could easily become fuel for the voracious fire that's being driven by a moderate wind. Several fire units respond, including a large contingent of volunteer firefighters who drive directly to the scene. Since the streets and construction are new, responding personnel are unfamiliar with the area and its resources, including the location of fire hydrants. However, these fire personnel have force-multiplying technology that is paired with FirstNet Ready™ smartphones and tablets.

While on the way to the scene, the incident commander gets updates from his passenger, a firefighter who is using a tablet to access the city's cloud-based database that contains planning department diagrams with street layouts and hydrant locations. The firefighter also gets a real-time weather report to determine temperature, humidity, wind direction and other relevant variables. Arriving on scene, the firefighter opens the rear door of the vehicle, revealing a large flat panel display used to manage the incident. With a touch of the tablet, the information, which is continually being updated, is transferred to the panel display and accessible by the incident commander.

The assisting firefighter then launches the agency's unmanned aerial vehicle (UAV, or drone) and controls it with the same tablet used on the way to the fire. As the UAV reaches a preset altitude, it hovers and rotates, sweeping the area with a built-in high-resolution camera streaming live video back to incident command. That same video is also viewable by any authorized firefighter with a smartphone and the dispatch center. As the incident commander directs initial deployment to the active fire areas, the UAV is switched into thermal imaging mode to look for small hot spots in the construction area that might indicate if a wind-driven ember has ignited a separate fire.

The firefighters' equipment has integrated sensors that stream status reports to incident command by pairing with smartphones. Depending on the sensors chosen, data can include firefighter heart and respiration rate, body temperature, body position (such as firefighter down), SCBA air status and, because they're carrying a smartphone, their specific real time location.

Threshold criteria can be set so that the information is only displayed at incident command if there is an indication of a problem, thus avoiding information overload. If a firefighter is equipped with a body worn camera, the video can be streamed or viewed on demand from command or any other authorized station.

All data transfer is handled by FirstNet, and critical information will get through to the decision makers, even during periods when conventional cellular networks are struggling.

Scenario 3: Traffic Accident with Multiple Injuries

A high-speed crash occurs on a busy multilane roadway. Initial 911 calls indicate there are at least two involved vehicles and multiple victims with serious injuries. Two paramedic units are sent to the scene. Dispatchers have access to stationary freeway cameras and route this video to the responding units. It's clear that traffic is at a standstill for cars going the same way as the involved vehicles, so units respond from the opposite direction.

Once on the scene, the EMS personnel triage patients and begin transmitting vital data using telemetry-equipped devices paired with the paramedics' smartphones. One of the first responders takes several photos of the injuries and the relevant mechanism of injury. The patient data and supporting pictures are sent to the receiving trauma center, where attending doctors can prepare for the patient's arrival.

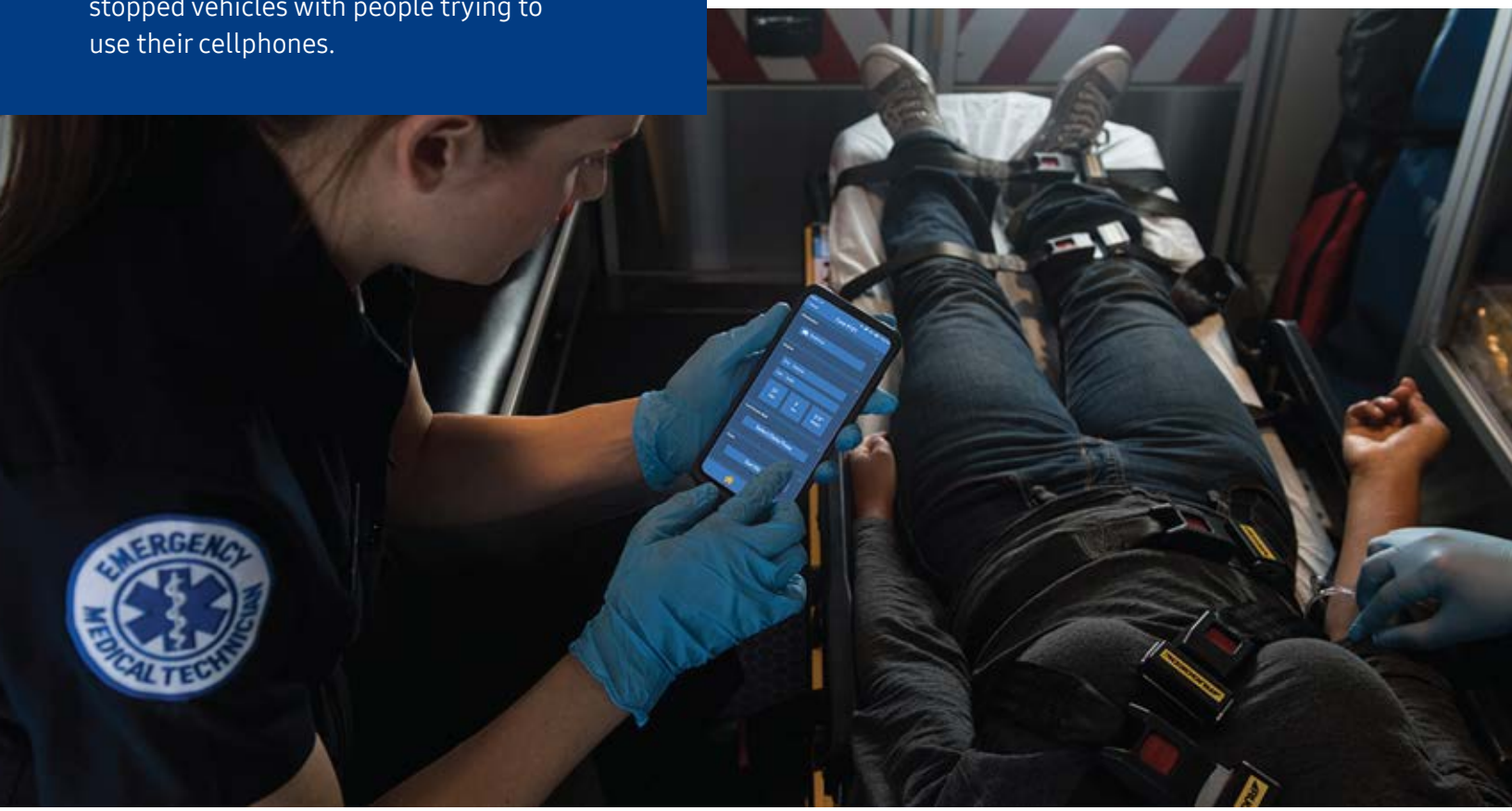
FirstNet supports the effective emergency medical response by reliably transferring data, even in the middle of hundreds of stopped vehicles with people trying to use their cellphones.

Due to the critical injuries sustained by one of the crash victims, paramedics request an air ambulance. A helicopter with flight paramedic and trauma nurse is sent. The same medical data and pictures are available to the air rescue team to evaluate while in route, thus providing a common operating picture for all those involved in the treatment of this patient.

FirstNet makes the above actions possible today by reliably transferring data, even in the middle of hundreds of stopped vehicles that contain people who are using (or trying to use) their cell phones. EMS can achieve HIPAA compliance by using devices secured with Samsung Knox, which offers defense-grade data security.

Keeping the Path Clear

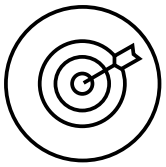
These scenarios are hypothetical and demonstrate the possibilities when innovative technologies are combined with the reliable FirstNet broadband network. Information from sensors, drones or videos is useless if it can't be accessed by those who need it, when and where they need it. FirstNet helps critical information get through.



Part 3: Laying the Foundation for Your Migration

Although most public safety agencies utilize smartphones at some level, in many instances mobile devices are only issued to administrators and many first responders use their personal mobile devices in an unofficial capacity. The advent of FirstNet presents an opportunity for public safety agencies to reassess their use of mobile devices at a strategic level.

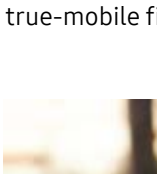
Modern smartphones offer a broad and versatile range of benefits to agencies and first responders. Beyond the core benefits of more flexible communications and on-the-go information access, smartphones can be employed in more sophisticated ways alongside other technologies, unlocking the door to a wide range of potential applications. Over the next several years, smartphone issuance for all first responders will become the standard operating procedure, allowing agencies take advantage of today's data-rich environment and the always-on prioritized broadband communication capability provided by FirstNet.



Determine the Desired Outcome

What capabilities do you want your emergency personnel to gain? This question will drive many of your future decisions, including software and hardware evaluation and implementation timelines. One advantage of leveraging smartphones is you can start with basic capabilities and build upon that foundation, deploying new applications or features that tap into device sensors or other advanced capabilities, which are continually being developed and introduced into the market.

With the availability of FirstNet, agencies can progressively reduce self-maintained infrastructure and start utilizing the cloud, enabling a true-mobile first workforce.



Assess Your Current Systems

It's also important to take time to evaluate your existing systems like computer aided dispatch (CAD) and records management. Many of the leading public safety software providers have introduced mobile and cloud-based applications, however features and functionality may vary. Start by talking to vendors of the software you want to use on your smartphones to plan your deployment, training and expectations accordingly. With the availability of FirstNet, agencies can progressively reduce self-maintained infrastructure and start utilizing the cloud, enabling a true-mobile first workforce.

Agency Issued Devices vs. Individually Owned Devices

Many agencies have programs that allow first responders to receive a stipend for using their personal smartphone — a bring your own device (BYOD) policy — for department business. This may be acceptable for first responders who have limited reliance on their smartphone when on duty. However, as mobile devices become more central to first responder communications and other key workflows, agencies should consider whether it is time to purchase and manage smartphones as they do with other mission-critical equipment. Issuing smartphones offers advantages when it comes to device management, configuration and application deployment.

Decisions on whether to continue with a BYOD policy or shift to agency-issued smartphones will differ across agencies and user groups. For example, fire departments may continue to operate a BYOD policy for volunteer members while career firefighters all receive department-issued phones.

Agencies with a BYOD approach can also leverage FirstNet for individually owned phones by setting up an account and then providing a list of authorized users. In the case of volunteer public safety professionals, individuals can simply subscribe directly to FirstNet service with proof of identity and agency affiliation. Once that's done, FirstNet will work with the individuals to change over the device (if necessary) and issue the required FirstNet SIM card.

Eligibility for FirstNet

There are two categories of public safety entities eligible for FirstNet access: Primary Users and Extended Primary Users.

- **Primary Users** are effectively those public safety organizations and personnel that serve as first responders, including, but not limited to, law enforcement, fire protection services, emergency call (911) dispatching and emergency medical services.

- **Extended Primary Users** are agencies or organizations that support Primary Users, such as emergency room personnel, public works, department of transportation and agencies that support scene mitigation, remediation or restoration during or after an incident.

Part 4: Staging Your Transition

Once you have established your mobile strategy and objectives, migrating to FirstNet is easy. Most users already use mobile devices in their personal lives and can easily learn to use public safety apps on smartphones and tablets. Nonetheless, there are some elements of mobile device deployment that will require planning and support. These include the selection of devices and rate plans, and the selection and use of device management tools. This section will prepare you to make informed decisions.

Agency administrators should begin with a planning phase that includes a thorough review of operations and how FirstNet will benefit their organization. Any area of electronic communication or data transfer should be reviewed. Smartphones, tablets and in-vehicle computers are obvious considerations. Essentially, any public safety operation or device that currently relies on a cellular network should be considered.

Once you have completed your review, determine what will be needed to obtain FirstNet capability and whether the remaining service life of devices is a factor. In general, if device replacement is necessary, it will be faster and more cost effective to coordinate the transition when equipment is scheduled for changeout. However, you should also look for opportunities to improve your operational effectiveness and save money by leveraging the power of today's newer smartphones. For instance, in-vehicle computers that use either a built-in modem or rely on an existing vehicle-mounted modem will require a FirstNet Ready vehicle modem. In this case, it may be prudent to consider using a FirstNet Ready smartphone with a Samsung DeX docking station to provide the functional equivalent of an in-vehicle computer. This type of approach can yield significant cost savings and improve operational effectiveness, since a single device can support in-field, in-vehicle and in-station operation. (See sidebar: DeX in-Vehicle Is a Transformative Solution)

Smartphones have proven to be powerful tools for public safety personnel, and FirstNet provides first responders with priority access to cellular services and, if necessary, will relocate or drop lower priority users to make capacity available. If you have an existing smartphone program, check the listing of FirstNet Ready devices to see if your device is listed.[3] If so, you may be able to simply add a FirstNet SIM to access FirstNet. If your smartphone isn't on the FirstNet Ready list (or if you're not using AT&T as your carrier), then you may want to consider the service life of the smartphones and available promotions to determine the timing for a move to the FirstNet network. Switching to FirstNet early will allow you to proactively roll out new mobile capabilities and take advantage of reduced equipment or device costs associated with any available FirstNet incentives.

Switching to FirstNet early will allow you to proactively roll out new mobile capabilities and take advantage of reduced equipment or device costs associated with any available FirstNet incentives.

FirstNet Devices

In addition to the existing spectrum bands used by cellular devices today, FirstNet utilizes additional spectrum not previously used for cellular services. As a result, all devices will ultimately need to be capable of receiving and transmitting on Band 14. However, if your device is not currently Band 14-compatible, it can still benefit from FirstNet services that are provided on the other spectrum bands used by AT&T. All you need to take advantage of FirstNet services today is a FirstNet Capable device and a FirstNet SIM card. There are a lot of device choices already available, with more being released regularly — and the newer devices are already unlocked and can operate on Band 14. Samsung offers more than 14 FirstNet Ready phones, ruggedized phones and tablets, such as the Galaxy S10+, S10, S10e, Note9, S9, S9+, A6, J3, J7, the Galaxy Tab A 8” and Tab S4. More FirstNet Ready devices will be coming in 2019.

Device Choices

When choosing devices, make sure they will fit the mission of the personnel who will be using them. When it comes to public safety operations, one size does not fit all. For some roles, such as a police investigator, a smartphone with a capable camera, slightly larger screen and stylus capability such as the Samsung Galaxy Note9 may be the most effective. Other personnel might derive benefit from a larger device such as a rugged tablet that provides a bigger screen. For many first responders, the device of choice will be a smartphone or ruggedized smartphone that is FirstNet Ready and DeX-capable.

Today, FirstNet Ready mobile devices are generally used as a complementary technology to LMR, but the long-term expectation is that mission-critical voice operations will eventually transition to smartphones. Indeed, cellular voice capabilities over FirstNet are prioritized for first responders over commercial traffic, and EPTT capabilities are widely leveraged. It is anticipated that full MCPTT capabilities consistent with 3GPP standards will be available in 2019.

Mobile first public safety leveraging FirstNet is a model that can deliver immediate benefits to agencies through improved responder safety, increased situational awareness and lowered IT costs. It makes sense to begin piloting mobile solutions as soon as possible while weighing FirstNet migration and, eventually, replacement of LMR.

DeX in Vehicle Is a Transformative Solution

Samsung DeX is a unique mobile technology that enables a Samsung Galaxy smartphone or tablet to provide a fully functional desktop experience. Built into several FirstNet Ready devices, DeX offers agencies a direct path to consolidated communications carried on a mobile device.

In the vehicle, DeX replaces the laptop with a keyboard and monitor setup that uses the Samsung smartphone as the computing device. To use the setup, a first responder simply places the phone in a docking station and it immediately launches into the desktop user experience. When they exit the vehicle, they undock the phone and take it with them.

DeX enables agencies to go mobile-first by consolidating voice and data communications onto the smartphone. Officers have continuous access to data and communications through the smartphone, and they can use the DeX functionality inside the station, where keyboard/monitor/mouse setups with DeX docks can replace desktop computers.

With the phone replacing both the laptop in the vehicle and the desktop computer in the station, DeX can help an agency reduce its IT expenditures. Single-purpose devices such as audio recorders, cameras, video recorders and scanners can also be replaced with a versatile smartphone.

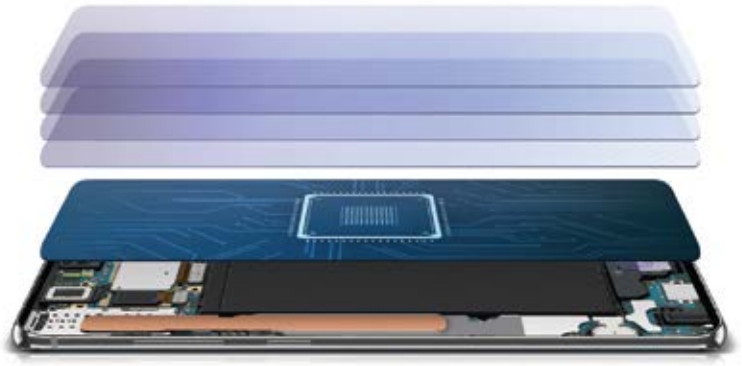
Rate Plans

FirstNet rate plans for agencies and individuals are already in place and available through several existing government contracts. There are options like traditional commercial plans, such as unlimited full service (talk, text, data, mobile hotspot and tethering) as well as pooled data rates. Determining the appropriate rate plan is an important part of the migration to FirstNet, and there is sufficient flexibility that an agency can tailor to their mission and budget.

Moving to FirstNet and changing over to FirstNet Ready devices doesn't have to be overwhelming. Deployment can be scaled to meet agency needs and, when possible, take advantage of equipment replacement cycles. However, this is the type of venture that benefits from proper planning and focused project management. It is helpful to have strong management-level oversight of the effort and work with key stakeholders in the agency who may be affected. Organizations vary greatly but consideration should generally be given to the uniformed personnel and the tech capabilities that you plan to use. You'll need assistance and ongoing support from the IT staff that currently supports your agency, and you'll want to have your communications/dispatch personnel fully involved. Consider whether services such as geolocation or sensor utilization will be subject to labor discussions and vet those areas proactively.

Policy and Training

Policy plays a key role in ensuring the success of new or expanding technology programs. It is important that a clear policy be established regarding the use of mobile devices that are connecting to the internet and/or accessing controlled databases. If the agency intends to issue individual smartphones and allow some degree of personal use, it is recommended that the policy precisely state what is permitted and what is not. Security protocols and expectations should be a component of the policy. This is particularly important in agencies where compliance with either Criminal Justice Information System (CJIS) rules or Health Insurance Portability and Accountability Act (HIPAA) regulations are applicable.



How Samsung Knox Protects Your Devices and Data

Agencies have a committed and knowledgeable mobility partner in Samsung. More than a dozen Samsung devices are FirstNet Ready, with more to come throughout 2019. The Samsung Knox platform is built in to these devices at the hardware layer, providing a security mechanism that protects against intrusion and malware.

Samsung also offers a suite of security and device management solutions that assist in addressing the security concerns inherent in a public safety environment.

Advanced security available as part of the Knox security and management stack include:

- Chip-level security built around a Trusted execution environment (TEE)
- Full-disk encryption
- Work/personal protected application containers
- Advanced biometric sensors, including ultrasonic fingerprint ID and iris scanning
- Tight integration with MDM and EMM agents

With Knox-secured devices, agencies are building their mobile programs on a secure foundation.

It's likely there will be both new equipment and new capabilities because of moving to FirstNet, and, unless you are using devices for only the most basic of communication tasks, this makes training an important consideration to ensure personnel are ready to take full advantage of the newly issued devices. It is recommended that two phases of training be utilized as appropriate for the agency:

1. The initial rollout. Work with a small group of experienced personnel who are interested in the project. It's good practice to get input from those who will be using the devices, and then start on a small scale so you can make course corrections before you fully deploy. As the momentum builds, share success stories. Once your initial group has sufficient experience to serve as in-field trainers and go-to resources, begin the full rollout of devices to the organization.

2. Operational exercises. FirstNet will enable agencies to communicate more effectively and coordinate major incidents in ways that were not previously possible. Public safety agencies understand the need to be prepared for major incidents, and training plays a key role in preparation. Some agencies may want to plan large-scale training exercises that test the capabilities of FirstNet. If your jurisdiction has moved multiple public safety groups (law enforcement, fire and EMS) to FirstNet, joint exercises will provide an excellent test of interagency communications. Remember that training is intended to work through issues, so personnel will be prepared when they are called to a real situation. Conduct an objective debrief after your scenario training. If capability gaps or areas of concern have been identified, this is the best time to address them.

MDM and EMM Solutions

Data security is critical to agencies that need to transmit vital, sensitive information freely while keeping it out of the hands of criminals and hackers. The best way to secure the data is to use secure devices that provide end-to-end encryption in conjunction with secure networks. Samsung Knox provides multilayered security and control at every turn.

If not already in use, it is recommended that agencies develop or modify end-to-end procedures for security using enterprise mobility management (EMM) or mobile device management (MDM) solutions. EMM and MDM solutions like Samsung's Knox Manage enable agencies to set and enforce policies as well as manage devices, operating systems and apps. They can also program devices to shut down and wipe their data remotely, so that a lost or stolen phone does not become a liability.

An EMM or MDM also simplifies enrollment and management by enabling IT to set user profiles and access individual devices remotely. EMM can preconfigure two-factor authentication using a combination of passwords, biometrics and third-party authentication. Other possible security measures include preventing unauthorized changes such as rooting or jailbreaking, configuring application access and applying application whitelists and blocklists. An administrator can create rules for internet connections, limit which applications can access data and restrict Wi-Fi access to select networks. These controls are particularly important in law enforcement and EMS, where agencies need to maintain compliance with CJIS and HIPAA, respectively. With Samsung Knox Configure, agencies can customize devices to their specifications before deployment.

Agencies Can Customize the User Experience With Knox Configure

Samsung Knox Configure simplifies the mobile first rollout by enabling agencies to develop a customized default profile and pre-install it on every device.

Devices arrive in the box with a custom boot-up screen and setup that incorporates device settings, apps and usage restrictions. This allows agencies to buy off-the-shelf phones and tablets and deploy them as purpose-built devices that are for agency business only. Every time the device is rebooted, it defaults to the preconfigured profile. When a first responder needs a replacement device, they can immediately log in without any additional setup.

Control and customization are extensive to a granular level and includes connectivity to Wi-Fi, Bluetooth utilization, use of USB connectivity or storage cards. The fact that hundreds of devices can be configured before distribution means huge time savings while providing a greater level of assurance that security is in place across the agency's mobile deployment. Updates can be done via a push notification from a web console, avoiding the need to touch each device. This is of value in a 24/7 operation where personnel are assigned to field operations or specialized assignments.

Moving Forward With FirstNet

Many agencies are already operational with FirstNet and benefitting from the network's promise to improve operational effectiveness. As the FirstNet ecosystem continues to mature, more and more features and capabilities will be added to provide public safety with new tools not previously available, all while operating on a network that provides the best possible experience. FirstNet seeks to continually improve network speed and capacity, and coverage will be extensive. Underscoring these improvements is the assurance that first responder public safety emergency operations always take priority over lower priority network traffic. The offerings of FirstNet Ready mobile devices and applications will continue to expand, allowing agencies to address their unique challenges. FirstNet has already changed the way first responders share and access information, and there is every reason to believe that we've only seen the beginning.

About Samsung

Samsung is your trusted partner for connecting your mission and teams to public safety networks through best-in-class smartphones, tablets and wearables. The company is deeply engaged in public safety worldwide, helping agencies enhance situational awareness and improve first responder safety with innovative solutions developed in partnership with leading public safety software providers. Samsung's fast, versatile smartphones, rugged tablets and smartly designed wearables comprise a modern communications ecosystem that delivers essential data in the most useful ways.

Footnotes

1. https://www.bostonglobe.com/business/2013/04/16/cellphone-networks-overwhelmed-blast-aftermath/wq7AX6AvnEemM35XTH152K/story.html
2. https://about.att.com/story/firstnet_selects_att_to_build_network_supporting_first_responders.html
3. https://www.firstnet.com/marketing/index.html#/marketing/index/devices

Disclaimer

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

Learn more: samsung.com/publicsafety | insights.samsung.com | 1-866-SAM4BIZ

Follow us: youtube.com/samsungbizusa | @samsungbizusa

SAMSUNG

WP-PUBLIC-SAFETY-FIRSTNET-MAY-19-SW