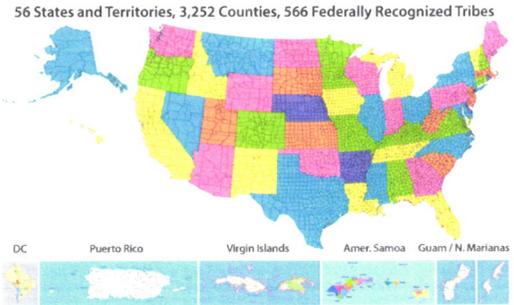


# The Promise of FirstNet

## What is FirstNet?

FirstNet will be the first high-speed wireless, broadband data network dedicated to public safety. FirstNet will be a single, nationwide network that facilitates communication for public safety users during emergencies and on the job every day. Think of FirstNet as a bigger, more reliable, secure and resilient "wireless pipe." This new network will be public safety-grade, providing access to applications and coverage where public safety needs it most.



## What will be possible with FirstNet?

Initially FirstNet will be used to send data, video, images and text and make cellular-quality voice calls. Users will get fast access to information they need to meet their mission. Unlike commercial wireless networks, FirstNet will allow for priority access among public safety users. FirstNet will also give incident commanders and local officials control over the network so, for example, they can assign users and talk groups and determine who can access applications.

## Why was FirstNet created?

After 9/11, the public safety community fought hard to fulfill the 9/11 Commission's last standing recommendation and convince Congress that it needed a dedicated, reliable network to provide advanced data communications capabilities nationwide. Commercial networks get overloaded or fail and don't provide priority access to public safety users during emergencies.

## How will FirstNet benefit public safety?

Using FirstNet will improve situational awareness and decision-making. Just as smartphones have changed our personal lives, FirstNet devices and applications will ultimately change the way public safety operates. FirstNet will save time during emergencies when seconds count. FirstNet will save money for states by leveraging nationwide purchasing power and scale economies. Using FirstNet can help save lives, solve crimes and keep our communities and emergency responders safer.

## How will states and agencies participate in the buildout of FirstNet?

To make FirstNet a nationwide network, all states must have a local radio access network (RAN) that connects to the FirstNet core. FirstNet is responsible for working through the designated state point of contact to consult with states, local communities, tribal governments and first responders to gather requirements for developing its RAN deployment plan. If the FirstNet plan is accepted by a state, FirstNet will construct the RAN. If a state prefers to build its own RAN, the state must secure FCC approval and may seek funding support from NTIA. State-built RANs must meet FirstNet security, hardening and interoperability requirements.

## What will users pay for FirstNet services?

FirstNet intends to offer services at a compelling and competitive cost to attract millions of public safety users and make FirstNet self-sustaining. The use of FirstNet services and applications will be voluntary. The costs for FirstNet services and devices have not yet been set.

**WIRELESS BROADBAND,  
DEDICATED TO PUBLIC SAFETY**



Energy & Telecommunications Meeting  
September 13, 2013 - Day 2  
Harlowton, Montana

# The Process for Working with FirstNet



## State Consultation and Outreach

To make FirstNet a nationwide network, all states must have a radio access network (RAN) that connects to the FirstNet core. By law, FirstNet is responsible for working through the designated state point of contact to consult with states, local communities, tribal governments and first responders to gather requirements for developing its RAN deployment plan. These outreach efforts began in mid-May 2013 with six regional workshops. Ten individuals from each state/territory, including some tribal representatives, participated in an interactive meeting where they provided requirements, priorities and concerns to FirstNet. Now FirstNet is gearing up for individual visits to continue the dialog about our common mission.

## State Visits

FirstNet will work through the designated state point of contact to arrange a visit, agree on the agenda and identify participants. Timing will depend on state readiness, the State and Local Implementation Grant Program (SLIGP) Phase 1 award and how quickly FirstNet can staff up its outreach team. The agenda for the initial FirstNet visit will focus on users and coverage needs, leveraging available information from the Department of Homeland Security Office of Emergency Communications. We will also discuss known state assets, expectations for data collection, as well as other state-specific issues. This meeting will pave the way for ongoing collaboration that will culminate in the development of a plan from FirstNet for constructing state RAN.

## Tribal Outreach

FirstNet plans to create an education and outreach program to engage tribal members in discussions about the network and their public safety needs. FirstNet will encourage state governors to include tribal nations in the local FirstNet consultation process. In addition, FirstNet plans to hold separate meetings with tribes.

## Data Collection

Data gathering, supported by funding from SLIGP Phase 2, will help ensure that the FirstNet state RAN build-out plans meet user needs. FirstNet will preview the components of the data request to help states understand the level of effort so they can adjust their SLIGP budgets accordingly. Data collection will cover the following general areas:

- Architecture of an evolved packet core and radio access network
- Required coverage areas of the network
- Hardening, security, reliability and resiliency requirements
- Assignment of priority users and selection of secondary users
- Availability of assets that may be utilized

States will be asked to submit available data as soon as it is compiled instead of waiting to complete the entire data request. FirstNet will continually update planning and modeling efforts based on new input. Our goal is to avoid surprises by working closely with state representatives as we develop the final FirstNet build-out plan.

## RAN Proposal Response

To make FirstNet a nationwide network, all states must have a RAN that connects to the FirstNet core. A state can decide whether to have FirstNet construct the RAN or, it can "opt out" and seek the required approvals to build its own RAN that meets stringent FirstNet requirements.

## RAN Response Timing

A state has 90 days from the date that the governor receives the FirstNet build-out plan to notify FirstNet, NTIA and the FCC in writing whether it prefers to engage FirstNet to build its RAN or construct its own RAN. If a state chooses to build its own RAN, it has 180 days to complete a request for proposal for its RAN. The state must also submit an alternate plan to the FCC for consideration.





### State Decision Process

FirstNet will collaborate with states to develop and deliver a RAN plan that meets their needs.



### Funding the Build-out

If the state's plan is approved by the FCC, the state may apply for grant funding from NTIA. To obtain federal funding to construct a RAN, a state must:

- Demonstrate the technical capability to operate and fund the RAN
- Maintain ongoing interoperability with the FirstNet network
- Complete the project within specified comparable timelines
- Execute its plan cost effectively
- Deliver security, coverage and quality of service comparable to the FirstNet network

There are additional funding implications if a state receives approval to build its own RAN:

- States pay any fees associated with using FirstNet core elements
- Grant program specifics are not developed yet
- NTIA will determine: eligible costs of the grant program; whether a match will be required; and funding levels

### Licensing FirstNet Spectrum

If the state plan is not approved, the construction, operation and maintenance of the state RAN will proceed in accordance with the FirstNet plan. If a state receives approval to build its own RAN, the state then needs to negotiate a lease for the use of FirstNet spectrum.

**WIRELESS BROADBAND,  
DEDICATED TO PUBLIC SAFETY**



## VIEW FROM THE TOP

Forward-looking perspectives from top leaders, regarding where our industry is today and, more importantly, where it is heading.

### **FirstNet invites participation in human-factors study that will be crucial to success**

**Aug. 12, 2013** by [Urgent Communications contributor](#) in [View from the Top](#)

*FirstNet needs to understand how the new network will affect the way law-enforcement, fire and emergency-medical-services personnel carry out their duties every day. By considering human factors, FirstNet can design systems that fit the human body and its cognitive abilities, as well as optimize system performance and productivity.*

#### **By Harlin McEwen, chairman, Public Safety Advisory Committee (PSAC)**

Much of the discussion about FirstNet—the nationwide, public-safety broadband network now in development—has focused on technology. However, an extremely important, but often overlooked, aspect of this network is the impact it will have on people. We need to understand how the new network will affect the way law-enforcement, fire and emergency-medical-services personnel carry out their duties every day.

FirstNet must consider human factors and design systems that fit the human body and its cognitive abilities, as well as optimize system performance and productivity. This is crucial in the public-safety environment, where split-second decisions and actions are often essential to save lives and property.

The FirstNet Board has asked the PSAC to analyze the long-range changes that the new network will have on people who use, operate and maintain the network every day. The PSAC believes that the needs of first responders and the individuals who support them, along with the latest technology, must drive network-design decisions.

When FirstNet is operational, public-safety agencies will have the ability to send data, video, images and text and make commercial-grade voice calls. Priority access and greater security and reliability will be key features of the network. These capabilities will provide dramatic improvements over the way we communicate today.

In our current land-mobile-radio environment, we have thousands of disparate wireless systems deployed by local, state and regional entities. The resulting interoperability problems extend across people, as well as technology.

For example, during Katrina and Sandy, public-safety personnel rushing from jurisdictions outside the affected areas to provide mutual aid often needed orientation to local communications terminology and practices. That can cost time, money and lives. With a nationwide network, we can remedy this situation. First, we must develop standardized approaches; then, individuals must be trained to use them. That's a tall order, but the benefits are well worth the effort.

The PSAC has enthusiastically tackled this assignment from the FirstNet board, and the PSAC executive committee has developed a template to gather data. The template has been distributed to PSAC members, and the plan is to deliver our recommendations to FirstNet this fall, so they can be included in the extensive market research that FirstNet is conducting prior to selecting network technologies.

The PSAC already has divided its initial research into four design categories: devices, applications, policies and procedures and network access/security. We will be investigating the ergonomic needs of users, operators and "maintainers"—those responsible for infrastructure maintenance—in each of these areas. Here are examples of these needs:

## **Devices**

Police officers need devices that can be operated with one hand, and firefighters must use devices while wearing heavy gloves. Emergency medical technicians (EMTs) and paramedics require devices supporting concurrent video, voice and telemetry for transmitting patient data to emergency-room personnel. Network operators—FirstNet and any potential partners—must deliver priority-access capabilities for devices and applications and the ability to provision devices remotely. Those who maintain infrastructure day-to-day need the ability to authorize access to information resources on the fly and remotely activate/deactivate devices, components and applications without user intervention.

## **Applications**

GPS and voice-enabled navigation applications providing turn-by-turn directions to incident scenes can be provided to users. Infrastructure elements must support end-to-end security for delivery and use of sensitive data, such as information from the National Crime Information Center (NCIC), Nlets—the international justice and public-safety network—and state criminal justice information systems. Maintainers want applications and data sources to incorporate criteria for authorizing use by local, regional, state, multistate and/or nationwide entities.

## **Policies and Procedures**

Documentation, training and exercise doctrines must be developed for users working with new devices, applications and data sources. FirstNet will need to define and offer high availability, prioritization, quality-of-service (QoS), redundancy and resiliency.

In addition, memoranda of understanding and service-level agreements must be developed for operating partners, whether they are commercial or governmental entities. Maintainers will need operating procedures for the life cycle of devices, applications and data sources.

## **Access (Security)**

One of the key ways that FirstNet will be differentiated from commercial networks is in the area of security. Ubiquitous, end-to-end authenticity and confidentiality of information traversing the network will be crucial for users, operators and maintainers.

There are many examples of excellence in specific public-safety agencies around the country. We will leverage this knowledge of human factors as we develop a nationwide vision and strategy. When FirstNet launches, we want to ensure that it works better than anything we have today for our emergency responders.

I invite *Urgent Communications* readers to provide their ideas and recommendations to their PSAC representative or directly to the PSAC at [PSAC@hq.dhs.gov](mailto:PSAC@hq.dhs.gov).

*The law creating FirstNet required that its Board establish a standing Public Safety Advisory Committee to assist it in carrying out its duties and responsibilities. Harlin McEwen serves as chairman of this committee. He is also chairman of the communications and technology committee of the International Association of Chiefs of Police. Now retired, McEwen previously served as police chief for the city of Ithaca, N.Y., and as FBI deputy assistant director in Washington, D.C.*



**Public Safety Advisory Committee  
Over the Horizon/Human Elements/Factors  
Scoping and Data Gathering Template**

**Task Scope:** The Public Safety Advisory Committee (PSAC) was asked by FirstNet to analyze the long-range impacts of the nationwide public safety broadband network (NPSBN) on the way law enforcement, fire, and EMS operate and consider the impact it will have on their duties once the network is built and operating. It is important that the business and needs of first responders drive decision, not technology. This task looks to answer the questions:

- What are the human elements that FirstNet needs to consider when designing the network?
- What are the potential user issues that will arise when using the NPSBN?
- How will the NPSBN be used by first responders and how will it impact operations?

To determine the human factors<sup>1</sup> impact of the network, the PSAC Executive Committee (EC) defined the "human element" of the system as users, operators<sup>2</sup>, and maintainers<sup>3</sup>. Next, the PSAC EC identified categories to compartmentalize the various impacts, which are shown in the table below. Based on these categories, PSAC members are being asked to brainstorm and list potential human impacts. Examples are provided in *italics* for each category. Once PSAC members submit the initial list of impacts, the PSAC EC will compile and review the input and provide to FirstNet for review. The PSAC EC will then work with FirstNet to determine the highest priority categories and human factors/elements. Once the highest priority factors/elements are determined, the PSAC will develop recommendations or proposed processes outlining how these human elements should be addressed.

---

<sup>1</sup> Human factors is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data, and other methods to design in order to optimize human well-being and overall system performance.

<sup>2</sup> Operator is responsible for the day-to-day operations of the network (e.g., FirstNet, commercial carrier)

<sup>3</sup> Maintainer would be the entities/divisions within the operator entity that are responsible for maintenance services for the operator. Personnel that keep the day-to-day infrastructure elements running.



Category	Human Element Group		
	Users	Operators	Maintainers
<b>Device design/ergonomics (detail public safety grade)</b>	<ul style="list-style-type: none"> <li>• <i>Police officers need the ability to use device with one hand</i></li> <li>• <i>Fire fighters need the ability to use devices while wearing heavy gloves</i></li> <li>• <i>EMT/Paramedics need devices that support concurrent video, voice and telemetry transmissions for patient to ER Doc teleconferences</i></li> <li>• <i>Need ruggedized devices – able to withstand harsh environments (e.g. resistant to heat/cold, drop, dust, water, etc.)</i></li> <li>• <i>Device hardware supports the collection of various biometric data from the user or others</i></li> <li>• <i>Device supports integrated security platform when coupled with proper application(s) can securely receive/transmit TS classified materials</i></li> <li>• <i>Devices incorporate power sources that provide a minimum of 10 hours duty cycles</i></li> <li>• <i>Devices in all form factors shall support a secured common alerting protocol for one-to-one and one-to-many communications</i></li> <li>• <i>Applicable devices should support the creation of ad hoc secured/non-secured WiFi personal area networks</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Devices may be provisioned remotely by local and nationwide operational entities</i></li> <li>• <i>Device authorizations to information resources may be adjusted by competent authority “on the fly”</i></li> <li>• <i>Device hardware supports Band 14 and commercial bands for interoperability</i></li> <li>• <i>Infrastructure supports ample bandwidth availability for concurrent collection of various biometric data from the users or others</i></li> <li>• <i>Infrastructure will support differentiation of priority access of devices and applications accessed upon devices</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Devices may be provisioned remotely by local and nationwide operational entities</i></li> <li>• <i>Device authorizations to information resources may be adjusted by competent authority “on the fly”</i></li> <li>• <i>The fault management system(s) and console controls shall allow remote manipulation of devices to activate/deactivate the device or components, and/or applications without user intervention</i></li> </ul>



Category	Human Element Group		
	Users	Operators	Maintainers
Applications	<ul style="list-style-type: none"> <li>• Applications support the collection, use, transmission, and receipt of multiple concurrent streams of biometric data</li> <li>• Applications support integrated security hardware platform that can securely receive/transmit TS classified materials</li> <li>• Applications incorporate Video Analytic capabilities</li> <li>• Applications integrate with and expand capabilities of connections to National Crime Information Center (NCIC), National Law Enforcement Telecommunications System (NLETS), State, Regional and local Criminal Justice Information Systems</li> <li>• Applications allow devices to access and control switched video sources at or enroute to incident scenes</li> <li>• Applications will provide GPS and voice-enabled navigation systems providing turn-by-turn directions to locations</li> </ul>	<ul style="list-style-type: none"> <li>• Infrastructure supports ample bandwidth availability for use, transmission, and receipt of multiple concurrent streams of biometric data</li> <li>• Infrastructure supports ample bandwidth availability for the use of Video Analytics</li> <li>• Infrastructure elements support the end-to-end provision of security elements supporting TS materials</li> </ul>	<ul style="list-style-type: none"> <li>• Applications incorporate criterion that articulate suitability and authorization/certification for use upon the network specifying local, county, multi-county, regional, state, multi-state, nationwide access or use.</li> <li>• Data sources should incorporate criterion that articulate suitability and authorization for use upon the network specifying local, county, multi-county, regional, state, multi-state, nationwide access.</li> </ul>



Category	Human Element Group		
	Users	Operators	Maintainers
Policies and Procedures	<ul style="list-style-type: none"> <li>• Training and exercise doctrine is developed supporting various device form factors</li> <li>• Training and exercise doctrine is developed supporting various applicable applications and data sources</li> <li>• Differential operational documentation developed regarding the behavior of devices and applications on FirstNet vice Commercial Networks if applicable</li> </ul>	<ul style="list-style-type: none"> <li>• Operating procedures and guidelines are developed for device, applications and access to various data sources</li> <li>• FirstNet and operators must define the required availability of the network in terms of availability = (total time – down time) / total time based upon the defined public safety need</li> <li>• The network will incorporate and utilize standardized elements that dictate prioritization and Quality of Service (QoS) attributes</li> <li>• Redundancy/Resiliency and high availability elements of the network must incorporate accepted practices of elimination of single points of failure, graceful and reliable failover between primary and secondary/backup elements or components and the prompt notification of failures</li> <li>• MOAs, MOUs, SLAs and/or contracts are developed between FirstNet and Commercial Carriers regarding the use of commercial networks or elements thereof by public safety users</li> <li>• MOAs, MOUs, SLAs and/or contracts are developed between FirstNet and Local, State, Regional, Federal and Tribal governments for the use of their networks, elements thereof or data by FirstNet public safety users</li> </ul>	<ul style="list-style-type: none"> <li>• Operating procedures and guidelines are maintained through a life-cycle process for applicable devices, applications and access to available data sources</li> <li>• The network must incorporate a comprehensive fault management system specifically focused for a high availability environment</li> <li>• Development of comprehensive doctrine for high availability environments</li> <li>• The network must take into off-network, peer-to-peer, and self-healing capabilities which are critically important</li> </ul>



Category	Human Element Group		
	Users	Operators	Maintainers
Access (security)	<ul style="list-style-type: none"> <li>Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is provided</li> </ul>	<ul style="list-style-type: none"> <li>Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is provided</li> </ul>	<ul style="list-style-type: none"> <li>Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is consistently maintained</li> </ul>