Technical Report

Oregon Statewide Interoperability Coordination (SWIC)

OREGON PUBLIC SAFETY BROADBAND NETWORK

Planning for FirstNet

Document Number
SWIC-OPSBN-12-01, Release 1.0

Issued December 31, 2012

Statements in this document that are forward-looking statements are subject to various risks and uncertainties concerning specific factors, including but not limited to those specific factors discussed herein. When used in this document, the words such as "could", "plan", "estimate", "expect", "intend", "may", "potential", "should" and similar expressions, are forward-looking statements. Information provided in this document is necessarily summarized and may not contain all available material information.

Revision History

Rev	Sections Affected	Description of Changes	Date
1.0	All	Original Issue	12/31/12

Table of Contents

Revision History ii
List of Figures v
List of Tables vi
1. INTRODUCTION 1
2. EXECUTIVE SUMMARY 2
3. PURPOSE 7
4. BACKGROUND 7
4.1. Public Safety Communications Technological Evolution 7
4.2. Recent History at the National and Oregon State Levels 10
5. FIRSTNET 13
6. SERVICE DESCRIPTION 16
6.1. Use and Applications 17
6.2. Systems Description 24
6.3. Operations and Maintenance 29
7. STAKEHOLDERS 32
7.1. State Interoperability Executive Council (SIEC) and Other Stakeholders 33
7.2. Stakeholder User Groups 34
7.3. Partners 35
8. GOVERNANCE 36
8.1. Managing Organization 38
8.2. OPSBN Management Steering Committee 39
9. BENEFITS AND VALUE 40
10. BUSINESS MODEL AND FINANCIAL CONSIDERATIONS 44
11. BOUNDARIES AND ASSUMPTIONS 50
11.1. Constraints 50
11.2. Exclusions 51
11.3. Assumptions 51
12. RISK MANAGEMENT 52
13. RECOMMENDATIONS AND NEXT STEPS 55

14. CONCLUSION 68

15. REFERENCES 70

16. ACRONYM LIST 74

APPENDIX A - INTEGRATING LOCAL AND NATIONAL NETWORKS AND APPLICATIONS A-1

A.1 NETWORK OPERATING CHALLENGES A-1

A.2 APPLICATION INTEGRATION A-6

A.3 PROVISIONING USER EQUIPMENT AND SERVICES A-8

APPENDIX B - USER EQUIPMENT EVOLUTION B-1

APPENDIX C - PSBN NUMBERING & OPERATIONAL IMPLICATIONS C-1

APPENDIX D - OREGON BTOP GRANT APPLICATION SUMMARY D-1

List of Figures

Figure 4-1 Progression of LMR from Conventional Analog to Interoperable P25 Technology 8
Figure 4-2 Commercial Wireless Technology Generations Yield Increasing Capabilities 9
Figure 4-3 Public Safety Communications Evolution to a Single Converged Mission Critical Platform 10
Figure 4-4 Public Safety Communications Broadband National and Oregon Event History 12
Figure 5-1 FirstNet Legislation Doubles Bandwidth for Public Safety by adding 10MHz D Block 14
Figure 6-1 Oregon Public Safety Broadband Survey: Cellular Data Adoption 18
Figure 6-2 OEC Goal 2 Data Collection: Mobile Data Use over Commercial and Private Networks 19
Figure 6-3 Oregon Public Safety Broadband Survey: Cellular Data Technologies Used for Wireless Data 19
Figure 6-4 Functional Elements of an LTE Broadband System 25
Figure 6-5 High Level Architecture of an LTE System 26
Figure 8-1 Oregon Public Safety Broadband Governance Management Structure 39
Figure 8-2 Stakeholder and User Information Flow 40
Figure 9-1 Survey Respondents Experience Positive Impacts of Wireless Data Use 43
Figure 10-1 Survey Reported Rate Structures for Commercial Wireless Service 46
Figure 10-2 Survey Reported Billing Formats for Commercial Wireless Service 47
Figure 13-1 Public Safety Broadband Communications National and Oregon Timeline 2012 – 2013 66
Figure 13-2 Public Safety Broadband Communications National and Oregon Timeline 2014 – 2015 through 2022 67

Figure C-1 Public Land Mobile Network Identifier (PLMN ID) = 313-100 ..... C-1
Figure C-2 International Mobile Subscriber Identity C-2

List of Tables

Table 5-1 Summary of FirstNet Legislation Timeline Milestones 16
Table 6-1 High Bandwidth Data Communications are Key to Potential Public Safety Applications 21
Table 7-1 Emergency Support Functions 34
Table 7-2 Potential Investor Partners for OPSBN 35
Table 8-1 FirstNet Board of Directors 37
Table 10-1 NPSBN Funding Afforded by the Middle Class Tax Relief and Job Creation Act ... 45
Table 12-1 OPSBN Planning, Deployment, and Operations Risks and Potential Mitigations..... 53
Table 13-1 OPSBN Recommendations – Near Term (6-12 mo.) 57
Table 13-2 OPSBN Recommendations – Long Term (12 mo.+) 61

Table B-1 Comparison of Public Safety LMR and Commercial Grade LTE Equipment B-3

1. INTRODUCTION

For over 75 years, the public safety community has relied on Land Mobile Radio (LMR) for dependable, two-way voice communications when responding to emergencies and performing daily tasks. In recent decades, the introduction of low and medium speed data networking has brought useful software applications to the public safety end user, including Computer-Aided Dispatch (CAD), electronic mail, and labor saving capabilities like electronic citation and crash reporting systems. With the advent of affordable, high speed data communications – the same Internet Protocol (IP) based technology that runs today's commercial Internet – entirely new ways of communicating are becoming a reality for first responders, integrating information in the form of words, pictures, and video into their life changing activities.

In the future, public safety communications users may:

- Send video feeds from monitoring cameras inside a school to police vehicles on their way to a school emergency.
- Be alerted immediately to a downed firefighter via a helmet camera transmitting real-time video back to the operations center and the dangerous surroundings via clothing mounted heat sensors.
- Have dispatch send high-definition video, photos, and maps to responders, rather than just an address.
- Transmit high volume, real-time patient information such as streaming video and vital health stats to emergency rooms and trauma centers while the ambulance is en route.

This document describes these exciting applications, the broadband network making them possible, and the roadmap to their reality for the state of Oregon.

- **Document Organization**

The document begins by summarizing history and background for Oregon's Public Safety Broadband Network (OPSBN) program, as well as recent FirstNet legislation. It follows with a service description that highlights the network's uses and its architecture, as well as important considerations for successful ongoing operations within the state.

As important as the physical network structure, a supporting organizational governance structure is next proposed after first highlighting the many and diverse OPSBN stakeholder groups.

The report then turns to a discussion regarding value, examining the benefits, operational business model, and financial considerations of this undertaking. It concludes by summarizing risks, constraints, and assumptions bounding the implementation and offers recommendations with a corresponding timeline for actions. The appendices offer additional technical background regarding the network, national requirements, and the implications of both to Oregon.

2. EXECUTIVE SUMMARY

The following OSPBN Executive Summary is designed as a pull-out standalone white paper, complementing the detailed report while summarizing the detailed document sections.

OREGON PUBLIC SAFETY BROADBAND NETWORK

Imagine public safety first responders

- Viewing live video from monitoring cameras inside the school while traveling in police vehicles to a school emergency
- Sending video of patient and vital health stats to the emergency room from the ambulance en route to the hospital
- Being alerted immediately to a downed firefighter via a helmet camera transmitting real-time video and aware of the dangerous surroundings and vital signs via clothing mounted heat and bio sensors

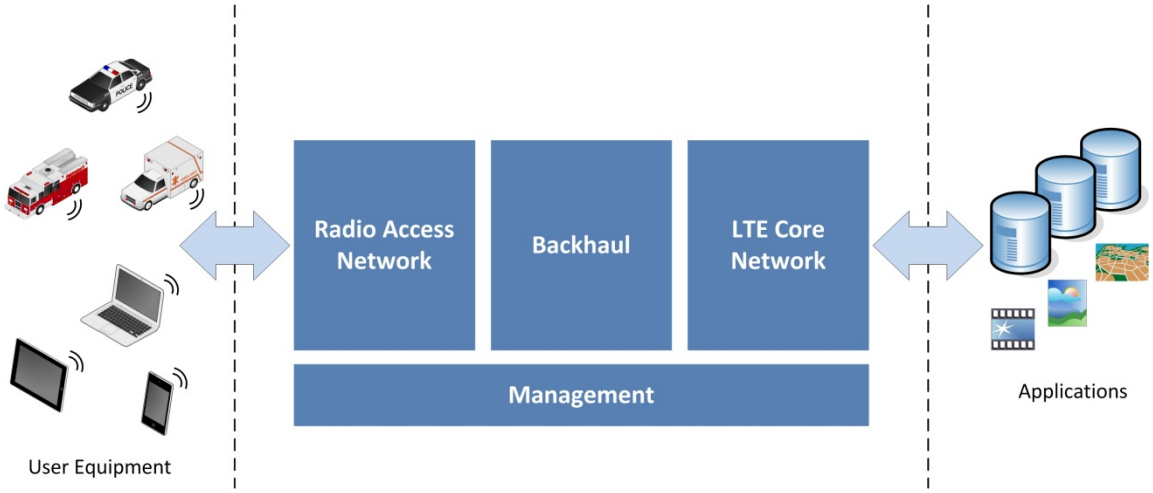
All these and more become possible with the deployment of Oregon Public Safety Broadband Network (OPSBN), a high speed broadband data communications network dedicated to public safety.[1] OPSBN will be part of the nationwide public safety broadband network (NPSBN), a single interoperable network that will allow police officers, firefighters, emergency medical personnel, and other public safety officials to transparently communicate with each other as appropriate across jurisdictions.

FirstNet. Title VI, "Public Safety Communications and Electromagnetic Spectrum Auctions," of the Middle Class Tax Relief and Job Creation Act of 2012 (PL112-96) includes provisions to fund and govern the NPSBN, reallocate the 700 MHz D Block spectrum to public safety, and authorize the FCC to conduct incentive auctions to raise $7 billion for building and managing the new network. It establishes the First Responder Network Authority, or FirstNet, within the Department of Commerce's National Telecommunications and Information Administration (NTIA) to oversee network planning, construction, and operation. FirstNet members were announced on August 20, 2012 by the U.S. Commerce Secretary and include Chief Jeffrey Johnson, the former chair of the Oregon State Interoperability Executive Council (SIEC).

LTE Network. To ensure interoperability and foster the availability of low cost user devices, the Act directs a specific wireless technology be used for the network – Long Term Evolution or LTE. LTE is the fourth generation (4G) cellular technology currently being deployed by commercial service providers. An LTE network consists of these major elements:

- User Equipment (UE), such as a vehicle mounted modem, laptop computer air card, handheld smartphone or tablet

[1] The Department of Homeland Security Command, Control and Interoperability Division Basic/Futures Research program has developed a compelling video to illustrate broadband's potential within emergency management. See http://precisioninformation.org.



Major Elements of an LTE Broadband System

- Radio Access Network (RAN) consisting of towers and cell site base station equipment which make the wireless connection to the UE mobile devices
- Evolved Packet Core (EPC), performing core LTE controller activities, such as identifying subscribers and establishing connections between them and application packet gateways
- Backhaul network, which interconnects the RAN equipment to the EPC, typically via suitable fiber optic and microwave links
- Management functionality, which includes network management, provisioning, billing, accounting, authorization, and access control

Applications. However, the high speed data network in and of itself is simply the transmission medium. The real value of OPSBN is in the life changing, lifesaving public safety applications that it will enable. LTE technology opens the door to entirely new operational processes for public safety operations. The expansive data throughput of LTE broadband, which is theoretically *more than 15 times faster* than third generation (3G) cellular data today, is truly a transition "from garden hose to fire hose," enabling a broad range of new public safety support capabilities that, until now, were simply not possible. Listed in the table on the next page is a sampling of these exciting applications, some of which are in use today.

Mission Support vs. Mission Critical. When discussing applications, it's important to make a distinction between mission *critical* and mission *support* use by public safety users. The mission critical voice communications provided by Land Mobile Radio (LMR) technology are supported today by wide coverage, highly reliable networks. Until OPSBN is similarly deployed, *LTE high bandwidth data applications such as streaming video will be for mission support use*. For example, note that the last item in the table is Push-To-Talk Voice over Internet Protocol (VoIP). LTE VoIP is still in development in standards bodies and requires a relatively dense build-out of tower and communications infrastructure as compared to LMR. Therefore, the National Governors Association (NGA) has stated, "it will be many years before VoIP will be carried over the [LTE] network, so states will need to continue to sustain LMR systems…even as they build toward public safety broadband."

Business Model. Once constructed, FirstNet intends to sustain network operations using a fee based business model, with revenue coming from three sources:

- Network User Fee – Fee from each public safety or secondary network user

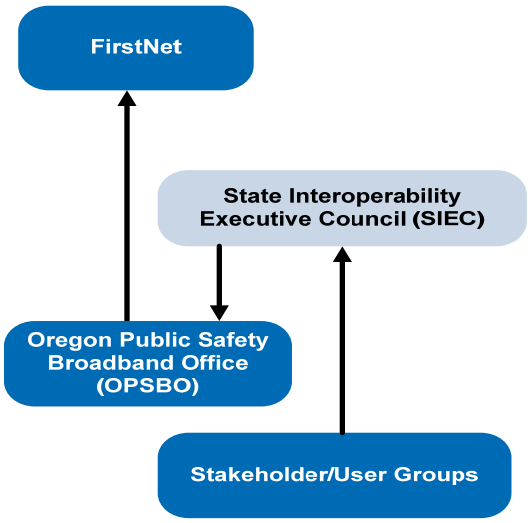
Public Safety Broadband Applications	
• Video Surveillance, Remote Monitoring (streaming)	• Dynamic Mapping, Weather, Traffic
• Remote Database Access/Queries (mug shots, finger prints, reporting, NCIC, criminal history, hot files)	• Instant Messaging, SMS, One-way Notifications, Tactical Chat Rooms
• Multimedia Command and Control (floor plans, incident stills, surveillance)	• Real-time, One- and Two-Way Video in Vehicles or Handhelds
• Computer-Aided Dispatch (CAD), Next Generation 9-1-1 (NG 9-1-1)	• Geo-Location and Asset Tracking (vehicle, personnel, assets)
• Records Management Systems Access (local queries)	• Mobile Office (bulk file transfer, email, Internet web access, virtual private networking – VPN)
• Mobile Incident Command	• Geospatial Applications
• Medical Telemetry	• Automated License Plate Recognition
• Field Based Reporting	• Digital Signage, Traffic Alerts, Automated Transactions
• Remote Control of Robotic Devices	• Standardized Push-To-Talk (PTT), Voice over IP (VoIP) - *future*

High Bandwidth Data Communication is Key to many Public Safety Applications

- Lease Fee for Network Capacity – Access fee from secondary user
- Lease Fee for Network Equipment/ Infrastructure – Fee for use of FirstNet antennas, towers, and other assets

Commercial LTE service will not be allowed on NPSBN. Secondary users, such as utilities, will be allowed to use the network on a for-fee basis, increasing the subscriber base and making the network more affordable for public safety users. There is no information yet whether the User Fee will be a flat monthly rate per subscriber or a usage based arrangement. Oregon public safety users have typically preferred a flat rate, due to its predictability and ease in budgeting.

Governance. The Act requires each state to designate a single officer or governmental body to coordinate with FirstNet. Oregon plans for an Oregon Public Safety Broadband Office (OPSBO) to serve as this single voice to FirstNet. Similar to the administration of the State Radio Project (SRP), the proposed OPSBO will handle day-to-day program management and coordination functions. The OPSBO will initially reside within Oregon Department of Transportation's Major Projects Branch (MPB), and later transition to the Department of Administrative Services (DAS). A multi-agency Management Steering Committee is proposed to advise and oversee the activities of the OPSBO. The SIEC will consolidate and communicate stakeholder and user needs to the OPSBO for conveyance to FirstNet.



Stakeholder and User Information Flow

Next Steps. Requirements for the State and Local Implementation Grant Program were released by NTIA in August 2012. The 56 states and territories are eligible for $135M in planning funds through the program, which may be used to create or expand governance structure, ensure local and tribal consultation, plan education and outreach, and determine and manage staffing. They can also be used to establish standard Memorandums of Agreement (MOUs) to facilitate use of existing assets. A Request for Proposal (RFP) for the grant funds is scheduled to be released in the first half of 2013, with distribution and use of those grant funds for planning activities in 2013 and 2014. In the first quarter of 2015, FirstNet is expected to begin informing states of their national deployment plan and funding levels. 2015 is also when the first funding from spectrum auctions is anticipated to become available for network construction. The spectrum auction process is expected to continue through 2022.

Opt-In or Opt-Out Decision. FirstNet is required to develop and present a plan to each state to build, operate, and maintain both the nationwide network and the network in each state. Once FirstNet has developed a plan, notified Oregon, and provided funding levels to achieve the plan objectives, Oregon will have 90 days to decide whether to **opt in** and participate in the deployment of the nationwide public safety broadband network or **opt out** and deploy its own portion of the national network. If a state opts out, it still must achieve the level of connectivity and interoperability that is specified by FirstNet for the nation. Based on the information that is currently available regarding FirstNet and the status of Oregon's existing network facilities, we recommend that Oregon adopt an **Opt-In** position.

Managing Expectations. During this long, multi-year network deployment, it will be important to manage stakeholder expectations of this exciting technology by emphasizing these key messages:

- LTE is not a replacement for LMR technology today.
- LMR will continue to provide mission critical voice communications for the foreseeable future.
- LTE introduces new capabilities to assist the first responder and makes current data applications even better. It is a supplementary technology that offers the first responder new data and video services, providing additional and timely information.
- OPSBN is a high speed data communications network. Its true power and value will be realized once useful, interoperable applications are in the hands of users.
- States will need to prepare their local networks and establish new processes to make full use of this promising capability.

3. PURPOSE

The purpose of this report is to communicate the vision, direction, and steps that are necessary to realize a high bandwidth data network infrastructure in support of Oregon's public safety community. The primary audience for this document is the Oregon Governor's Office, State Legislature, local governments, and public safety stakeholders. This planning document is intended as a tool for building awareness, support, and a common understanding of the Oregon Public Safety Broadband Network (OPSBN). The OPSBN is Oregon's portion of the nationwide public safety broadband network as mandated by federal regulations under FirstNet.

This report defines the OPSBN program by identifying its goals and objectives, key stakeholders and governance, potential uses and proposed architecture, and anticipated business model. Most importantly, it identifies and describes the increased mission effectiveness and operational efficiency offered to Oregon's public safety stakeholders. These gains are supported by the reliable, high speed data communications offered by a 700 MHz Long Term Evolution (LTE) broadband network.

4. BACKGROUND

This section begins by discussing the technological evolution and convergence of public radio communications. Against this backdrop the history of recent policy developments at the national and Oregon state levels are chronicled, ending with the signing of the FirstNet legislation.[2] Section 5 provides details on FirstNet.

4.1. PUBLIC SAFETY COMMUNICATIONS TECHNOLOGICAL EVOLUTION

For decades, first responder public safety communications has been synonymous with push-to-talk voice service provided by Land Mobile Radio (LMR) technology, i.e., the two-way radios used by police, fire, medical, and other emergency management personnel. Figure 4-1illustrates the progression of LMR technology, beginning with conventional analog voice service, progressing to trunked radio systems, and finally to the current interoperable Project 25 (P25) digital standard.

[2] Public Law 112-96, "Middle Class Tax Relief and Job Creation Act of 2012." FirstNet is found in Title VI of PL112-96, entitled "Public Safety Communications and Electromagnetic Spectrum Auctions." Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf

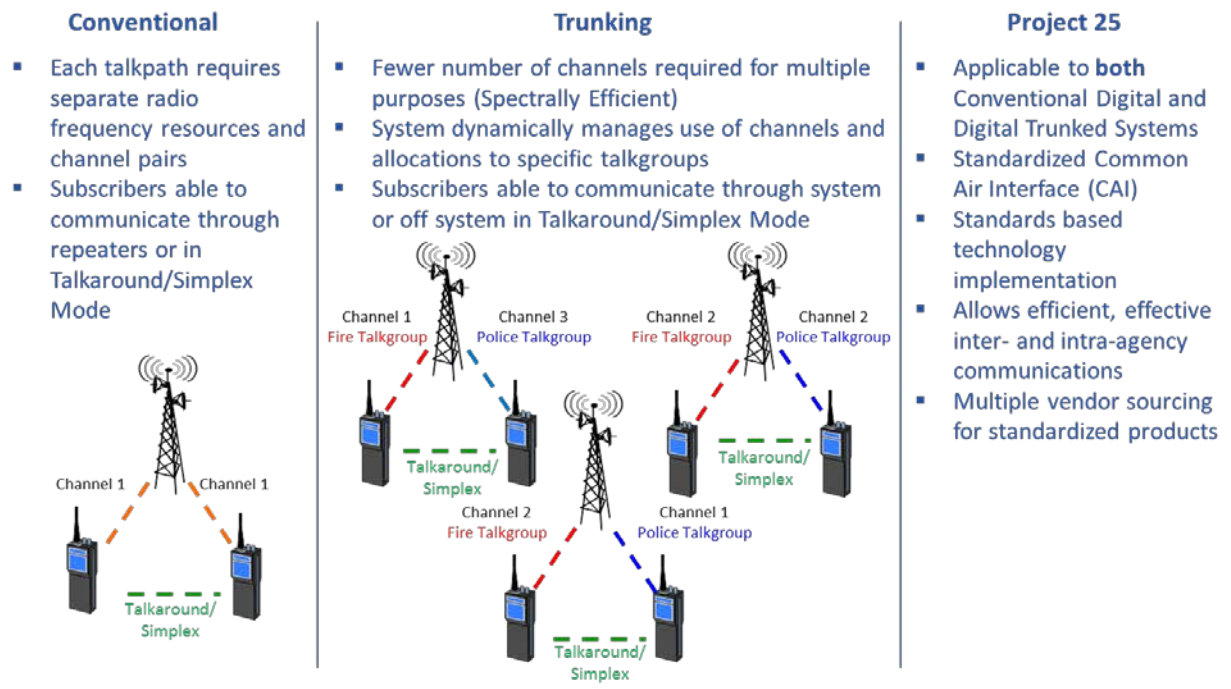


Figure 4-1 Progression of LMR from Conventional Analog to Interoperable P25 Technology[3]

Discussions regarding interoperability have been at the recent forefront of this evolution, heightened by the 9/11 Commission Report recommending the development of a nationwide interoperable public safety communications network in response to the inability of first responders to communicate during the terrorist attacks.[4]

In parallel development, commercial cellular wireless technology has been advancing at a much faster rate, driven by a globally expanding customer base with an insatiable appetite for new services. The growth has been further spurred by the decreasing cost and increasing processing capabilities of mobile devices. The Office of Emergency Communications (OEC) explains, "The wireless industry notes the progression of wireless technology in terms of 'generations':

- First-generation wireless includes **voice-only** communications devices such as the analog cellular phone.
- Second-generation wireless introduced digital wireless and includes personal communications service devices that offer **voice and text**.

[3] OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon, p. 14.
[4] GPO (2004, July 22). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, p. 397. Retrieved from http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf

- Third-generation encompasses smartphones and other advanced devices that provide **voice, text, and Internet capabilities**. These devices can run a multitude of applications, in many cases simultaneously.
- Fourth generation (4G) wireless systems such as LTE are being designed to provide higher speeds and more **advanced applications such as streaming video**."[5]

Figure 4-2 illustrates this progression in technology and capability.[6]

Figure 4-2 Commercial Wireless Technology Generations Yield Increasing Capabilities

When it adopted LTE as the standard for use on 700 MHz public safety broadband networks, the Federal Communications Commission's (FCC's) goal was to leverage this low cost platform, i.e., the same 4G technology beginning to dominate the commercial market.[7]

Significant time, effort, and planning are required to bring the public safety LMR and commercial wireless broadband paths together to meet this objective. Figure 4-3 shows the evolution and convergence of the two paths, with the goal of a robust, single platform capable of supporting mission critical voice and data applications as its desired end state.

---

[5] OEC (2011 November). *Interoperability Planning for Wireless Broadband*, p. 2. Retrieved from http://www.publicsafetytools.info/oec_guidance/docs/Interoperability_Planning_Wireless_Broadband_Web_111711.pdf

[6] OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon, p. 13.

[7] OEC (2011 November). *Interoperability Planning for Wireless Broadband*, p. 16. Retrieved from http://www.publicsafetytools.info/oec_guidance/docs/Interoperability_Planning_Wireless_Broadband_Web_111711.pdf

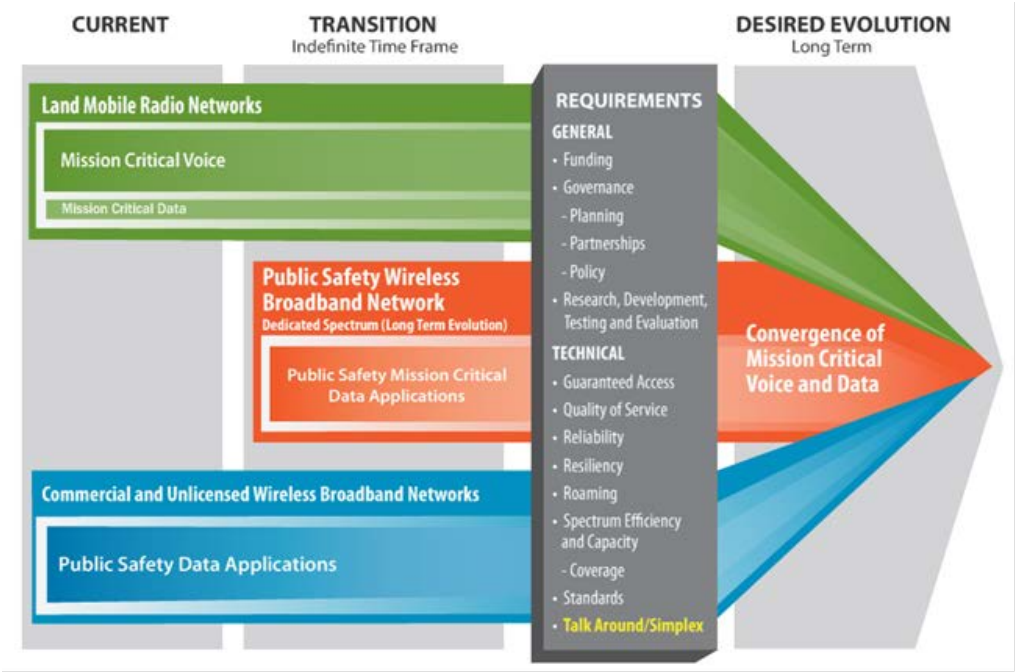


Figure 4-3 Public Safety Communications Evolution to a Single Converged Mission Critical Platform[8]

The requirements list at the figure's center indicates just some of the many aspects yet to be developed, adopted, and implemented in order to make the objective of a converged mission critical platform a reality.

4.2. Recent History at the National and Oregon State Levels

To accomplish the goal of convergence, national and state level policy regarding public safety communications has been required to evolve as well. The State of Oregon has been deeply involved in this formative process, both locally and nationally.

In 2009, the FCC met with national public safety leaders to discuss the possibility of using the Public Safety Broadband Spectrum (PSBB Block) 700 MHz frequency spectrum to develop a National Public Safety Broadband (NPSBN) system. This discussion, coupled with hearings and national workshops sponsored by the FCC, led to a decision by the FCC enabling public safety officials to apply for and use the PSBB Block 700 MHz spectrum.

A national broadband plan was written by the FCC and local government agencies were allowed to apply for waivers to use the PSBB Block spectrum. Oregon, along with 20 other waiver jurisdictions, received authorization (via a waiver) from the FCC to use this spectrum in May 2010. The spectrum was designated by the FCC for specific use with LTE technology. This was considered a landmark decision at the time, due to the high market value of the released

[8] OEC (2011 November). *Public Safety Communications Evolution*, p. 2. Retrieved from http://www.publicsafetytools.info/oec_guidance/docs/Public_Safety_Communications_Evolution_Brochure.pdf

spectrum. The market auction value of this spectrum was approximately $2.7B if auctioned without conditions for nationwide use.[9]

As one of the waiver jurisdictions, in June 2010 Oregon applied for, but did not receive, $150 million in grant funding via the Department of Commerce National Telecommunications and Information Administration's (NTIA's) Broadband Technology Opportunities Program (BTOP) to build a state network. Subsequently, in December 2011 Oregon released a Request for Information (RFI) through its Office of Innovative Partnerships Program (OIPP), seeking a public-private partnership to establish a public safety broadband pilot project in the state.

On February 22, 2012, President Obama signed into law Public Law 112-96, the Middle Class Tax Relief and Job Creation Act of 2012. Title VI of PL112-96, entitled "Public Safety Communications and Electromagnetic Spectrum Auctions," includes provisions to fund and govern the NPSBN, reallocate the 700 MHz D Block spectrum to public safety, and authorize the FCC to conduct incentive auctions to raise $7 billion for building and managing the new network. It also established within the NTIA the First Responder Network Authority (FirstNet), to oversee network planning, construction, and operation.

With the advent of this legislation, the jurisdictional waivers have been recalled by the FCC since the expanded spectrum, 10 MHz PSBB Block + 10 MHz D Block = 20 MHz, will now be administrated by FirstNet.[10] Given this development, Oregon suspended its pilot planning activities, awaiting further decisions at the national level regarding FirstNet grant funding and direction.

Figure 4-4 provides a timeline of recent events at the Oregon and national level leading up the establishment of FirstNet.

[9] Noel, S. (2011). *Oregon LTE at a Glance*. Internal planning document, p. 1.
[10] FCC (2012, July 30). Order FCC-12-85A1.

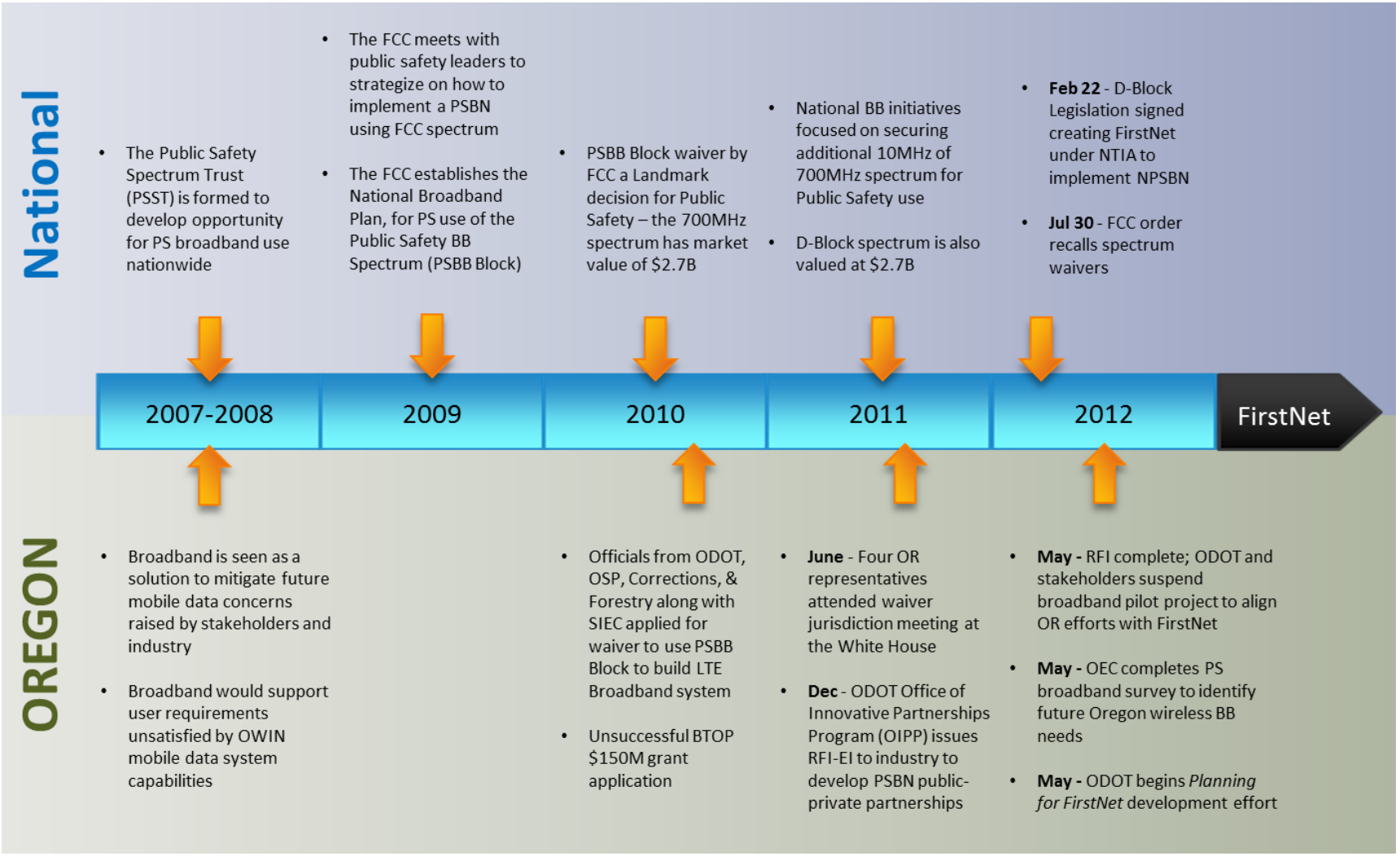


Figure 4-4 Public Safety Communications Broadband National and Oregon Event History

5. FIRSTNET

As introduced in the prior section, Title VI, "Public Safety Communications and Electromagnetic Spectrum Auctions," of the Middle Class Tax Relief and Job Creation Act of 2012 (PL112-96), includes provisions to fund and govern a Nationwide Public Safety Broadband Network (NPSBN). This legislation:

- Reallocates the 700 MHz D Block spectrum to public safety
- Authorizes the FCC to conduct incentive auctions to raise $7 billion for building and managing the NPSBN
- Ensures access to the network for federal, state, and local public safety and secondary users (e.g., utilities, critical infrastructure providers)
- Establishes a new entity within the NTIA to oversee planning, construction, and operation of the nationwide network, known as FirstNet[11]

The following paragraphs describe these key points in more detail and the section concludes by outlining Oregon's relationship and responsibilities to FirstNet.

- **Increased Spectrum for Public Safety Broadband Services**

Every wireless network operates within a portion, or band, of radio spectrum. In 2007, the FCC had allocated to public safety use the 10 MHz PSBB Block within the 700 MHz radio band. The legislation added the adjacent D Block, 10 MHz between 758–763 and 788–793 MHz, setting it aside for first responders and giving FirstNet responsibility for both blocks. See Figure 5-1.

As a result, FirstNet now has authority over a combined 20 MHz portion of public safety broadband spectrum, enabling a richer and broader range of services than would otherwise be available with only half the bandwidth.[12]

[11] DHS (2012). *Public Safety Broadband: Fulfilling a 9/11 Commission Recommendation*. Retrieved from http://www.dhs.gov/files/programs/public-safety-broadband.shtm

[12] National Governors Association (2012, June 28). Preparing for Public Safety Broadband. *White Paper*, p. 3. Retrieved from http://www.nga.org/files/live/sites/NGA/files/pdf/1206PREPAREBROADBANDPAPER.PDF

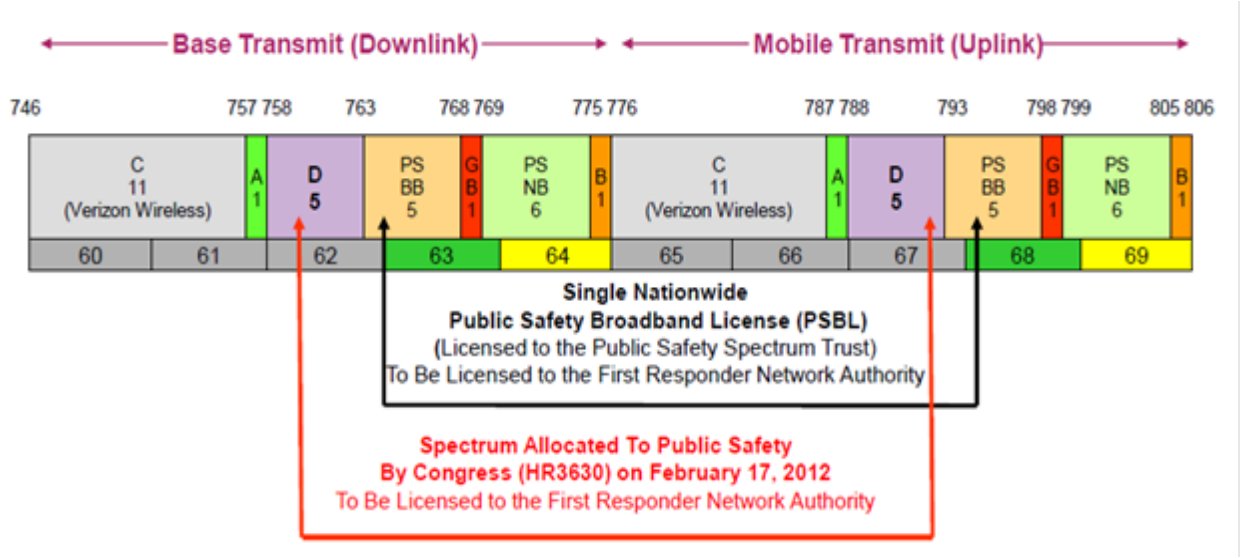


Figure 5-1 FirstNet Legislation Doubles Bandwidth for Public Safety by adding 10MHz D Block[13]

- **Who Can Use FirstNet?**

Using the allocated radio spectrum, the law calls for FirstNet to operate and deliver services via the network to approximately 60,000 federal, state, and local agencies. Authorized users of the new network include:

- Emergency response providers, including federal, state, and local governmental and non-governmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities
- Secondary users, including non-public safety entities (e.g., utilities, critical infrastructure providers)[14]

FirstNet is not authorized to offer commercial service to consumers. However, it must offer service to public safety users throughout the United States, including all 50 states, the District of Columbia, and all territories, such as Guam and the Marianas Islands.[15]

- **FirstNet Implementation Approach**

Under the Act, the FCC was responsible for establishing a Technical Advisory Board for First Responder Interoperability (Interoperability Board), tasked to develop recommended "minimum technical requirements for interoperability" for the FCC to submit to FirstNet for

[13] McEwen, H. (2012, March 15). *Nationwide Public Safety Broadband Network*, p. 3. NTIA Communications & Technology Committee presentation.
[14] OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon, p. 31.
[15] Lawson, S. (2012, June 15). US pushes forward on public-safety LTE network. *Network World*. Retrieved from http://www.networkworld.com/news/2012/061612-us-pushes-forward-on-public-safety-260253.html

implementation. The Interoperability Board would then disband. This was accomplished as of May 2012.[16]

FirstNet will then use the minimum technical requirements for interoperability to develop and issue Request for Proposals (RFPs) for the construction and operation of the NPSBN "without materially changing them," per the Act. FirstNet has been funded up to $7 billion from incentive auctions to be deposited in a Network Construction Fund. To pay for operating expenses, FirstNet is authorized to assess user fees and fees associated with leasing network capacity and infrastructure.

- **Oregon's Interactions with FirstNet**

FirstNet must consult with state, local, and tribal jurisdictions through a single state designated officer or governmental body regarding the distribution and expenditures of funds to carry out its responsibilities. Those include land acquisition and leasing, construction, infrastructure placement, coverage areas, resiliency requirements, assignment of priority to local users, assignment of priority to other users, and training needs of local users. Therefore, the Oregon Governor's Office must identify this single point of contact to represent the state in all interactions with FirstNet.

The Act provides $135 million nationwide to support planning and implementation efforts to prepare for NPSBN implementation. Each state will be required to apply to NTIA for grant funds. State, regional, tribal, and local jurisdictions will use the monies to identify, plan, and implement the most efficient and effective way for their jurisdiction to use and integrate the infrastructure, equipment, and other architecture associated with local roll-out of the network. Unless waived by the NTIA, these implementation planning grants will require a 20 percent match from the state. Grant application acceptance by NTIA is contingent on the office or single designated point of contact having been identified as part of the submission.

- **Opt-In/Opt-Out Decision**

FirstNet is also required to develop and present a plan to build, operate, and maintain the nationwide network and the network in each state. Once FirstNet has developed a plan and its network funding level, it will inform the state. The state will have 90 days to decide whether to opt in and participate in the deployment of the nationwide public safety broadband network or opt out and deploy its own portion of the network. States cannot opt out of the nationwide public safety broadband network until FirstNet presents its plan. Beginning from the decision to opt out, a state has 180 days to develop and complete an RFP for the construction, maintenance, and operation of its portion of the network. This timeframe includes applying to NTIA for a grant for construction and leasing spectrum from FirstNet. The FCC will evaluate the state's alternative

[16] Technical Advisory Board for First Responder Interoperability (2012, May 22). Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network, *Final Report.*

plan, comparing it to the minimum technical requirements for interoperability. It will determine whether the state's plan or the FirstNet plan will be used for the construction and operation of the radio access network (RAN).[17] States that successfully opt out must be interoperable with the NPSBN.[18]

Table 5-1 Summary of FirstNet Legislation Timeline Milestones[19]

Date	Milestone
February 2012	President signs legislation
March 2012	FCC appoints Interoperability Board members
May 2012	Interoperability Board sends technical recommendations to FCC
June 2012	FCC approves technical recommendations
August 2012	FirstNet Governance Board members appointed
To be determined	FirstNet issues RFP for NPSBN construction and operation - FirstNet will inform states of plan for build-out and funding levels
90 Days after completion of RFP	States inform FirstNet whether they will participate in NPSBN deployment or build their own Radio Access Network (RAN)
180 Days after Opting-Out	States develop and complete RFPs for constructing, maintaining, and operating the state RAN

In summary, Table 5-1 recaps the timeline milestones called out by the federal legislation. Oregon's state level governance, approval authority, and corresponding actions in response to this federal timeline are discussed in later sections. Section 13 Recommendations and Next Steps, suggests an Opt-In decision position for Oregon. Figure 13-1 and Figure 13-2 illustrate the current national and Oregon timeline for public safety broadband communications through 2022.

6. SERVICE DESCRIPTION

This section discusses current and potential uses for Oregon's public safety broadband data network. It differentiates and defines "mission critical" vs. "mission support" applications. Further, it describes the LTE network elements and architecture supporting FirstNet and highlights OPSBN operational considerations.

[17] See Section 6.2. for an explanation of the RAN and other major elements of an LTE network.
[18] Technical Advisory Board for First Responder Interoperability (2012, May 22). Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network, *Final Report*, p. 17.
[19] Adapted from OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon, p. 40.

6.1. USE AND APPLICATIONS

The introduction of software applications (or "apps") operating on mobile computing platforms such as Apple's iPhone has dramatically changed the way people communicate, work, and play. In similar fashion, the advent of public safety apps served via a robust, high speed network has the potential to completely change the landscape of daily operations within the public safety community.

Before discussing the many exciting applications and uses of the new network, an important distinction must be made between *mission critical* and *mission support* use by public safety users. Harris Corporation, in its response to Oregon's RFI, provides practical working definitions of these terms:

Mission Critical – Communications that are required to maintain safety of first responders and the people with whom they interact

Mission Support – Communications that provide improved operational efficiency, enhance safety, and augment command and control, but are not essential[20]

Currently, mission critical voice communications is provided by Land Mobile Radio (LMR) technology and has a long history of operating over redundant, highly available networks for public safety use. Initial high bandwidth data applications supported by OPSBN such as streaming video are anticipated to be for mission *support* use only. Regarding the eventual transition of the public safety LTE network to carrying mission critical voice communications, the National Governors Association (NGA) notes that "it will be many years before Voice over Internet Protocol (VoIP) will be carried over the [LTE] network, so states will need to continue to sustain LMR systems far into the foreseeable future, even as they build toward public safety broadband."[21]

- **Current Oregon Mobile Data Use**

Within the context of the above definition for *mission support*, there exists a myriad of uses for high speed data applications in support of public safety. Early in 2012, the OEC within the Department of Homeland Security (DHS) completed a survey of the current and projected use of public safety broadband data applications in the state of Oregon. Twenty-five state, county, and local agencies contributed to the survey. Participants were primarily from the Portland area with representation ranging from law enforcement, fire and rescue, and emergency management to public works and the Oregon Department of Transportation.

[20] Harris Corporation (2012, March 2). *Response to the State of Oregon's Request for Information and Expression of Interest (RFI-EI) for Public Safety Long Term Evolution Broadband Spectrum Network Proof-of-Concept Pilot (LTE PSBN Pilot)*, p. 13. Italics added.
[21] National Governors Association (2012, June 28). Preparing for Public Safety Broadband. *White Paper*, p. 6. Retrieved from http://www.nga.org/files/live/sites/NGA/files/pdf/1206PREPAREBROADBANDPAPER.PDF

The survey found that many agencies are already using mobile data applications in fulfilling their missions, supported by both private and commercial data networks. Figure 6-1 from the survey shows the general trend of increasing adoption of mobile data applications by public safety agencies.[22]

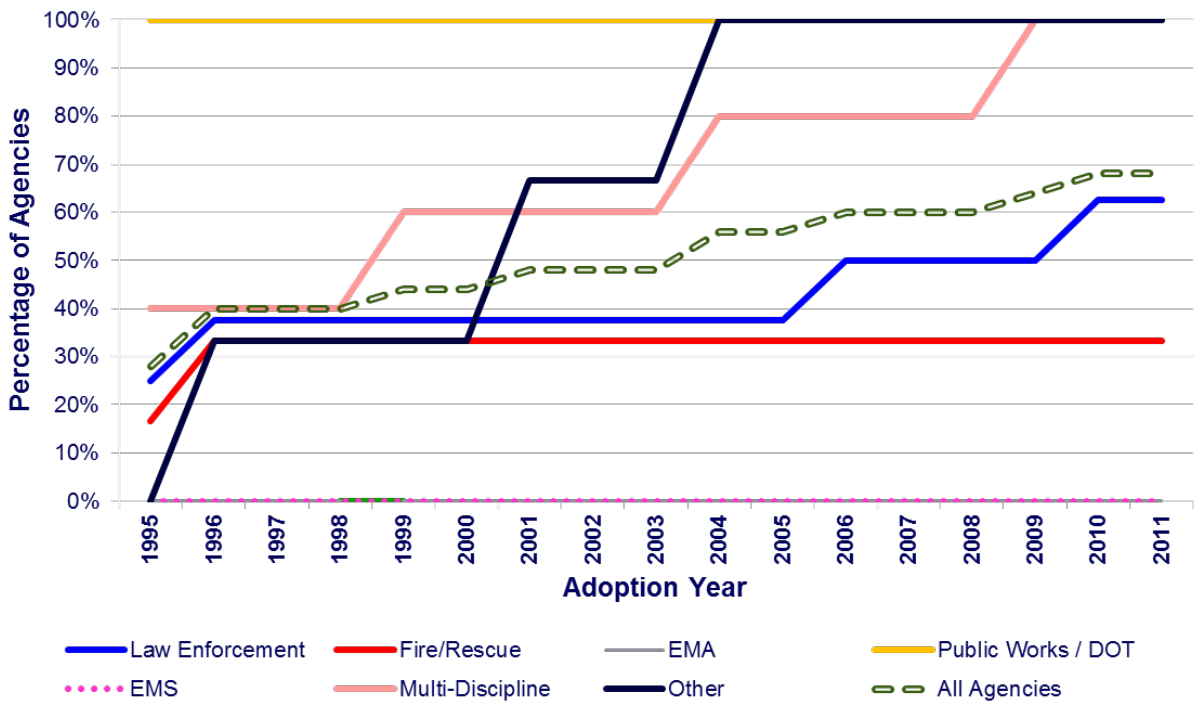


Figure 6-1 Oregon Public Safety Broadband Survey: Cellular Data Adoption

A separate survey conducted by OEC associated with the National Emergency Communications Plan (NECP) Goal 2 further illustrates the wide use of mobile data in daily operations throughout the state. [23] See Figure 6-2.

[22] OEC (2012, June). *Review of Public Safety Wireless Data Usage, State of Oregon, Portland Area*, p. 29. Used with permission.
[23] http://www.siec.wa.gov/success/files/NECP_Goal_2_Overview.pdf

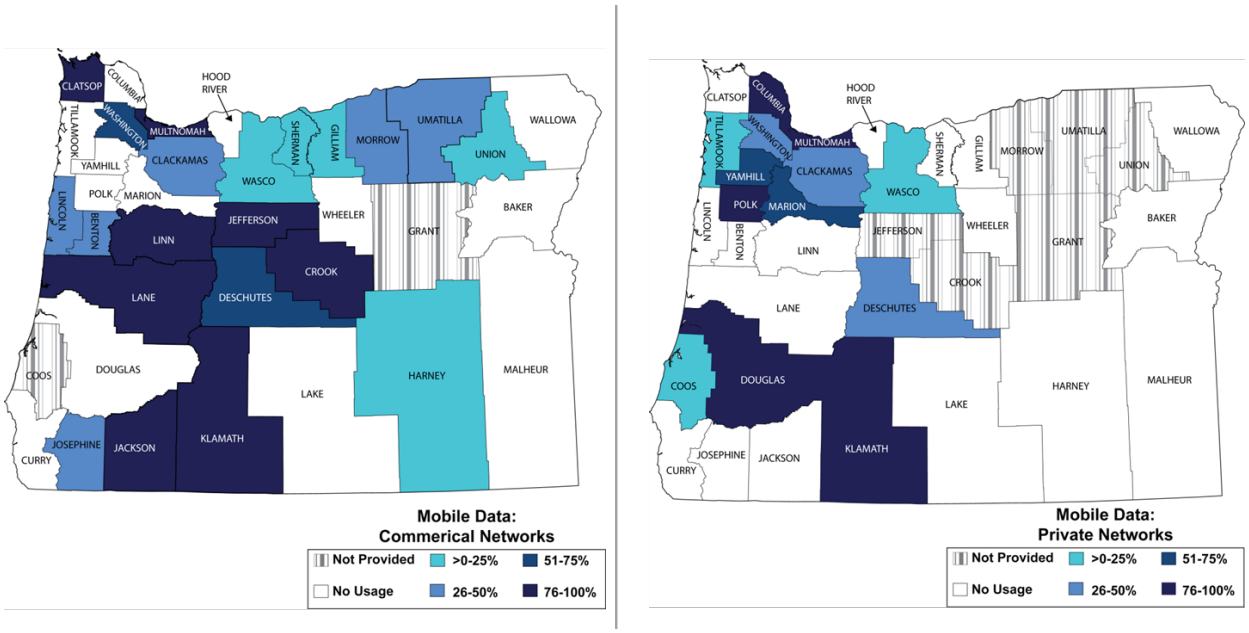


Figure 6-2 OEC Goal 2 Data Collection: Mobile Data Use over Commercial and Private Networks[24]

In fact, returning to the broadband survey, *32 percent* of the cellular data users surveyed were using advanced 4G technology today, as shown in Figure 6-3.[25]

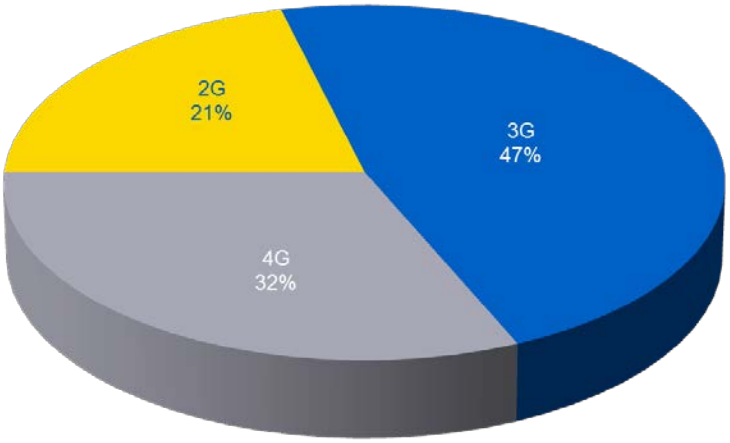


Figure 6-3 Oregon Public Safety Broadband Survey: Cellular Data Technologies Used for Wireless Data

For example, the City of Portland is using 4G LTE technology for data applications using available commercial service.[26] Further, the Oregon State Police (OSP) uses cellular technology to connect their in-vehicle mobility platform to Computer-Aided Dispatch (CAD) tools, locally hosted mapping, and the e-Citations electronic ticketing system. In fact, e-Citations and e-Crash

[24] OEC (2012, May). *NECP Goal 2 Analysis with Workshop Findings & Recommendations*, p. 20.
[25] OEC (2012, June). *Review of Public Safety Wireless Data Usage, State of Oregon, Portland Area*, p. 30. Used with permission.
[26] OEC (2012, June 21). Oregon Broadband Survey Workshop, Portland, Oregon.

electronic ticketing and crash reporting systems are estimated to have saved 55,000 hours of law enforcement time to date.[27]

In answer to what is driving these increasing public safety data adoption rates and usage, participants in the OEC broadband survey identified their top three wireless data applications as:

- CAD system interface
- Messaging
- Database inquiries

Finally and most importantly, broadband survey respondents identified the top three positive outcomes from their use of current wireless data systems as:

- Enhanced employee safety
- Rapid dissemination of key information
- Decreased response times

Taken together, these results illustrate that Oregon's public safety community is both using mobile data networking in an ever increasing manner, and finding value in its use.

- **Potential Public Safety LTE Applications**

In addition to increasing the speed and efficiency of current data applications, LTE technology opens the door to entirely new operational processes for public safety operations.[28] The expansive data throughput of LTE broadband, which is theoretically *more than 15 times faster* than 3G cellular data today,[29] is truly a transition "from garden hose to fire hose,"[30] enabling a broad range of new public safety mission support capabilities that, until now, were simply not possible. For example, from the incident scene it can enable first responders to see real-time situational awareness information via hardened smartphones. This may include viewing detailed building diagrams and dynamic geographic information system (GIS) map data, as well as video feeds from traffic cameras of the severity and extent of an accident, enabling them to act quickly and in coordination. Emergency medical personnel could transmit patient information and health telemetry to emergency rooms and trauma centers while en route to the medical center, with the vital lifesaving data arriving in advance of the injured.[31] Motorola Solutions, in its response to Oregon's RFI, highlights the wide ranging value provided by LTE technology to:

[27] ODOT (2012, December). "E-Citing things are happening with law enforcement data", *Inside ODOT*.
[28] DHS Command, Control and Interoperability Division Basic/Futures Research program has developed a compelling video to illustrate broadband's potential within emergency management. See http://precisioninformation.org for more information.
[29] Government Technology, Alcatel-Lucent (2010). *A How-To Guide for LTE in Public Safety*, p. 8.
[30] Hatch, L. (2012, June 5). [E-mail]. *Frequently Asked Questions*. (Texas)
[31] Roberts, M. R., (2012, May 1). Fire's Case for Broadband. *Urgent Communications*. Retrieved from http://urgentcomm.com/networks_and_systems/mag/fire-ems-broadband-needs-201205/index.html

- *Coordinate* incident response
- *Ensure* critical voice & data
- *Enhance* situational awareness
- *Improve* workforce efficiencies
- *Connect* across resources[32]

Table 6-1 summarizes frequently discussed applications made viable by LTE.

Table 6-1 High Bandwidth Data Communications are Key to Potential Public Safety Applications

Potential Public Safety Broadband Applications	
• Video Surveillance, Remote Monitoring (streaming)	• Dynamic Mapping, Weather, Traffic
• Remote Database Access/Queries (mug shots, finger prints, reporting, NCIC, criminal history, hot files)	• Instant Messaging, SMS, One-way Notifications, Tactical Chat Rooms
• Multimedia Command and Control (floor plans, incident stills, surveillance)	• Real-time, One- and Two-Way Video in Vehicles or Handhelds
• Computer-Aided Dispatch (CAD), Next Generation 9-1-1 (NG 9-1-1)	• Geo-Location and Asset Tracking (vehicle, personnel, assets)
• Records Management Systems Access (local queries)	• Mobile Office (bulk file transfer, email, Internet web access, VPN)
• Mobile Incident Command	• Geospatial Applications
• Medical Telemetry	• Automated License Plate Recognition
• Field Based Reporting	• Digital Signage, Traffic Alerts, Automated Transactions
• Remote Control of Robotic Devices	• *Standardized Push-To-Talk (PTT), Voice over IP (VoIP) - future*

In fact, many of the technologies supporting these applications are in commercial use today. Implementing a reliable and secure public safety LTE network will put them also in the hands of public safety users. In describing how LTE meets public safety needs, the publishers of *Government Technology* with the help of Alcatel-Lucent illustrate these tangible benefits offered to public safety users:

> **Situational Awareness** – Immediate, dependable communication is critical during an incident response. The capabilities of LTE get everyone on the same page, faster than ever before. Is a firefighter down? Is she trapped or unconscious? A helmet camera streaming real-time video back to the operations center can be the difference between life and death. With LTE, information can be exchanged from anywhere, instantly, in many ways. Video can be sent from the scene to commanders. Messages, images, surveillance videos, floor plans, mug shots – whatever is needed – can be instantly disseminated to all responders who need the information. Data from the field can be integrated with incident-management databases, for the

[32] Motorola Solutions, Inc. (2012, March 2). Executive Summary. *Response to the State of Oregon's Request for Information and Expression of Interest (RFI-EI) for Public Safety Long Term Evolution Broadband Spectrum Network Proof-of-Concept Pilot (LTE PSBN Pilot)*, p. 1. Italics added.

best possible situational awareness. The result is better decision making by leaders, and better safety for both responders and the public.

Digital Imaging – LTE enables large files to be sent extremely quickly. Detailed images of crime scenes, disaster scenes, suspects and more – all in high resolution – can be sent whenever they're needed. A photo can be received by a responder in the field in two seconds. It takes minutes with today's public safety networks, making it impractical in many situations. With LTE, photos can be sent quickly in both directions. If an officer isn't responding by radio, a dispatcher can instruct the squad car to send a photo. Dispatchers, first responders, commanders and others will be able to communicate more effectively.

Video – LTE gives new meaning to the phrase "a picture is worth a thousand words." Seeing what's happening at an incident scene is much more helpful than hearing about it. It saves precious time and gives decision-makers at operations centers more data to work with. LTE provides fast transmission of even high definition video. And there are numerous applications for public safety. For example, during a school emergency, LTE, with proper integration, can provide responders with access to the video surveillance feed from inside the school, sending it directly to squad cars. Video streaming of crime scenes and video conferencing are other examples. And video can be sent quickly and easily, in both directions. With LTE, video will likely play a much larger role than ever before.

Large Data Files – If a firefighter needs to see blueprints of a commercial building that's on fire, there aren't many options for getting that information today. Sometimes it can be displayed from a CD on a laptop, but that's time-consuming, and the information isn't always up to date. With LTE, very large files, such as detailed blueprints, can instantly be sent to numerous devices. And information can be pulled from a variety of other databases as well – hazardous materials, for example. With LTE, volumes of data can be received in just seconds.

Geographic Information Systems (GIS) – Mapping has become a very useful tool in many applications. LTE will increase the power of maps for public safety. LTE has functionality that improves on existing Global Positioning Systems (GPS), for greater accuracy. With LTE, commanders will be able to track their people and vehicles more accurately. Having better, real-time map displays will allow them to coordinate a better response and keep their people safe. GIS data can be combined with other data to make these maps even more useful. With a better overall picture, commanders can also leverage LTE to keep everyone on the response team well informed.

Automatic Vehicle Location (AVL) – LTE makes AVL more accurate and reliable. LTE supports both GPS and assisted GPS. In assisted GPS, LTE base stations are used as additional reference points to more accurately fix the position of fire engines, police cars and other vehicles. The system will no longer rely on satellites alone. This is especially helpful in urban environments, where tall buildings can hinder GPS. And with LTE, photos or other data can be linked to location information. A police officer, for example, can automatically be shown crime or suspect information related to the neighborhood he's entering in his squad car. Better AVL also gives improved situational awareness, and lets dispatchers quickly send additional information to a vehicle based on its location.

Computer-Aided Dispatching – Today, most information that's sent from dispatch to a responder is textual. It's often an address, and not much more. With LTE, dispatch can also send high-definition video, high-resolution photos, detailed maps and other data pertinent to the response. Video from one responder can be sent to dispatch, and then from there it can go out to other responders.

Access to Report Management Systems – LTE gives faster, greater access to central report management systems. Personnel out in the field will be able to access data within reporting systems from mobile devices like never before.

Telemetry/Remote Diagnostics – LTE enables more data to be sent automatically from mobile devices so the data can be analyzed elsewhere. Patient data can be sent from an ambulance to the hospital, for example, so doctors have vital information before the patient arrives. Diagnostic information for a device or a vehicle can be sent automatically as well.

Bulk File Transfer – Information sharing is at an all-time high. Bulk file transfers require high throughput, which public safety networks typically don't have. With LTE, bulk file transfers will be very fast. Whether for multiple high-resolution images or huge amounts of raw data, large files will get there fast with LTE.

Enhanced Day-to-Day Operations – Efficiency can be greatly increased when people have instant remote access to databases for vehicle records or suspect files, or can submit reports electronically. Public safety personnel are more effective when there's less paperwork to do, or when they're not waiting for information. The speed of LTE helps keep public safety personnel focused on their real work. It helps them do their jobs better.

Decreased Load on Narrowband Channels – Without a data system, a police officer needing a license plate check has to call in on his radio and ask a dispatcher to look it up. It can take many tens of seconds to fulfill this simple request, wasting valuable time on the narrowband radio system. With high-speed wireless broadband, the officer can do the lookup himself – and get the answer much more quickly. Transmission of large files can also put unreasonable pressure on narrowband channels. For example, it can take ten minutes to download a mug shot on narrowband, but just a few seconds with LTE. By shifting requests like this and others to a broadband system, the narrowband system can handle other tasks more efficiently.[33]

As mentioned previously, many Oregon public safety users are already using private and commercial data communications to better fulfill their missions. The additional speed and capacity of the OPSBN LTE network will make the applications such as those discussed above an integral part of their operational day, improving the efficiency and effectiveness of limited human resources. Appendix A provides a detailed analysis of the considerations regarding integrating local networks and applications with the NPSBN.

- **Public Safety Cloud**

With the deployment of regional and national public safety broadband networking, the many benefits and synergies of cloud computing that are touted in the commercial Information Technology (IT) space become real possibilities for public safety as well. Historically, LMR networks and associated messaging applications were unique to the locality served by the proprietary LMR network, limiting access and increasing cost. In contrast, the National Institute of Standards and Technology (NIST) defines cloud computing as embodying the following computing resource characteristics:

- **Broad Network Access** – Accessible over the network, using standard networking technologies
- **On-Demand Self-Service** – Can be provisioned by users automatically, as needed

[33] Note: Excerpted from "*A How-To Guide for LTE in Public Safety*," pp.14-17. Copyright 2010 by Alcatel-Lucent. Used with permission.

- **Resource Pooling** – Pooled in a multi-tenant model, and assigned to users on demand as needed
- **Rapid Elasticity** – Rapidly provisioned or decommissioned in any quantity at any time
- **Measured Service** – Metered and monitored to allow a pay-as-you-go model[34]

A cloud environment for public safety offers the opportunity on a regional or national basis to serve up common, best-in-class applications that will be truly accessible by all public safety users across all jurisdictions. Whether an Oregon firefighter, a California firefighter, or an Oregon firefighter fighting a fire in California, all would have access to the same applications via the public safety cloud. It would enable creating a central "App Store" for common tools that could be downloaded by users, regardless of their geographical location. Further, other applications could be hosted in the cloud itself, providing pay-per-use services, an economical alternative for cash strapped agencies and also one that satisfies infrequent needs. For daily use, OSP has noted that simply using the integrated public safety cloud for administrative purposes, such as single sign-on with authentication via a centralized active directory, would be a time and cost saver. Today, OSP users work within as many as eight security domains, each partition requiring its own time consuming ID and password login processes.

In sum, instituting a cloud based services architecture, made possible by an underpinning public safety broadband network infrastructure, takes interoperability to a new level – offering users the prospect of shared tools and streamlined processes, with the implied promise of saving in operations dollars and increasing efficiency.

6.2. SYSTEMS DESCRIPTION

Figure 6-4 is a high level diagram illustrating the major functional areas of an LTE broadband network system. An operational LTE network consists of the following key elements:

- User Equipment (UE), which communicate with the RAN wirelessly over the air.
- Radio Access Network (RAN), consisting of radio towers, antennas, and base station equipment.
- Backhaul network, which interconnects the RAN to the EPC, typically via suitable fiber optic or microwave links.
- Evolved Packet Core (EPC), which forms the LTE core controller network.

[34] Boubez, Dr. Toufic, InterAct Public Safety (2012, October 7). *Cloud Computing and Public Safety Services*, p. 4. Retrieved from http://www.interact911.com/wp-content/uploads/overview/cloud-computing-public-safety.pdf

- Management functionality, which includes network management, provisioning, billing, accounting, authorization, and access control.

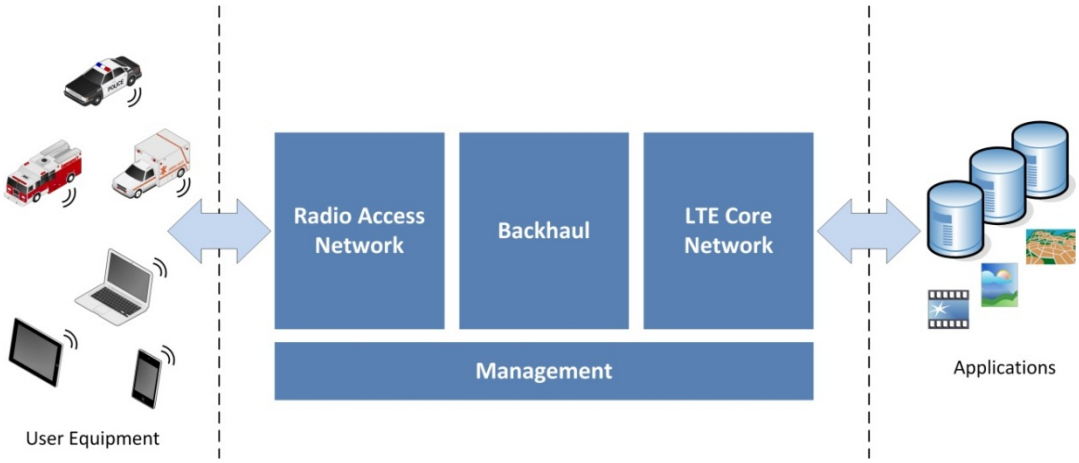


Figure 6-4 Functional Elements of an LTE Broadband System[35]

Security has been designed into the network end-to-end as part of the LTE standard. Functions such as encryption, authentication, and authorization are implemented using network elements throughout the architecture.

The major network elements supporting these functional areas are described below.

- **Operating Frequency Spectrum**

An LTE network is a mobile wireless data system. Commercial networks in the United States operate in the 700 MHz band. Band 13 and Band 17 are each 10+10 MHz full duplex channels, spaced 30 MHz apart. The rights to use Band 13 have been purchased by Verizon Wireless while AT&T uses Band 17. The public safety band of 10+10 MHz (753-763 MHz and 783-793 MHz) in Band 14 is not used by either commercial carrier. This is illustrated in Figure 5-1. See Section 5, FirstNet.

- **LTE Network Notional Architecture**

Figure 6-5 is a conceptual network architecture diagram depicting these elements and the interconnections supporting user application, signaling, and operations and management data communications across a public safety LTE network. These also play a role in the security architecture of the network.

[35] Note: Adapted from "*Ultimate Wireless Broadband Solution for Public Safety*." *Strategic White Paper*, p. 11. Copyright 2010 by Alcatel-Lucent. Used with permission.

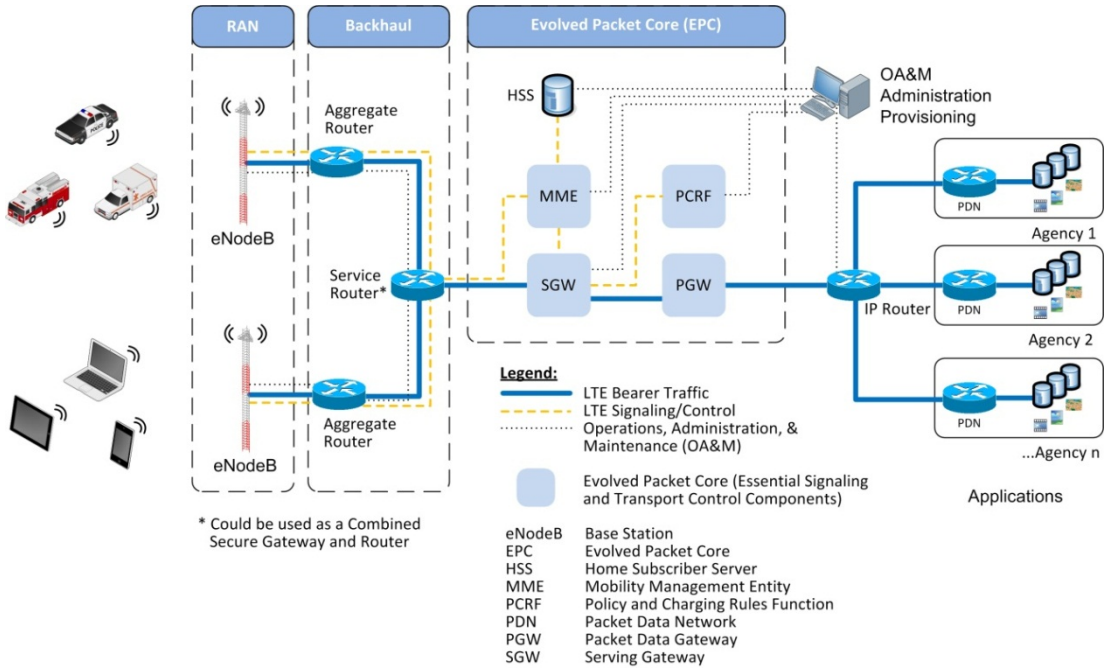


Figure 6-5 High Level Architecture of an LTE System[36]

- **User Equipment (UE)**

UE in a commercial environment is typically a smartphone or LTE wireless data card. These are mass produced and the resulting economies of scale permit these sophisticated devices to be sold to the customer for a few hundred dollars. Such devices could be adapted for public safety in a multi-modal configuration, supporting not only LTE, but also 2G and 3G circuit switched connections. Commercial phones and terminals use 2G or 3G mode for voice calls today, since those technologies are optimized for voice. Voice over LTE (VoLTE) has not yet been standardized and deployed. Appendix B further describes the evolution of UE.

Present user devices operate with a transmitter power of 200mW. This low transmitter power is a compromise to achieve reasonable battery life, acceptable radio frequency (RF) radiation into the user, and reasonable data rates. However, it is small in comparison with the 5W transmitter power of an LMR radio, for example. This lower power results in LTE cells that are smaller. So, more LTE cells are required to cover the same area than would be for LMR.

These devices are identified on a network and personalized to a user by inserting a Subscriber Identity Module (SIM) card (Universal Integrated Circuit Card (UICC)) in the devices. Device provisioning is discussed in greater detail in Appendix C.

[36] Note: Adapted from "*A How-To Guide for LTE in Public Safety*," p. 11. Copyright 2010 by Alcatel-Lucent. Used with permission.

- **Radio Access Network (RAN)**

RAN is the generic name for the wireless access network. In earlier generations, this was often thought of as a collection of multiple base stations (BS or cell sites) which were connected to Base Station Controllers (BSC). One BSC often controlled multiple BS and negotiated cellular hand-off between them rapidly using an intra-BSC handover. A BSC would send control signaling outside the cell to another BSC only when a terminal began to move outside the range of all the BS controlled by that BSC.

In an LTE network, the base station equivalents are now called eNodeBs. They communicate with one or more Mobility Management Entities (MMEs), which are part of the EPC for control purposes.

One key feature of the LTE network is that the eNodeBs support multi-homing, enabling them to be connected to more than one MME. This capability could be used to reduce congestion and improve response time, improve reliability, or to connect them to more than one service provider simultaneously.

- **Backhaul Network**

The transmission of the data and control traffic between the eNodeBs and EPC is performed by the backhaul network. This is a high bandwidth IP-based network designed to avoid delays which could affect response times. The backhaul may be provided using some combination of fiber optic, T1, or microwave links.

Since LTE requires an IP network, existing backhaul, such as legacy microwave, may not be suitable if it cannot support IP traffic. This is a very important cost factor for public safety since the backhaul would need to be upgraded with mixed mode equipment to support both the legacy application and the IP standard. Alternatively, a separate IP microwave link may be required for LTE.

The backhauled traffic requires several priority levels to support public safety. Hence it is often implemented as a Multi-Protocol Label Switched (MPLS) network. This allows bandwidth reservation for different classes of traffic to ensure that priority and Quality of Service (QoS) are maintained, depending on the application, network load, and other factors. For example, streaming video to a fire chief at an incident scene could have higher class of service than a text message sent between two secondary responders.

The bandwidth required from the backhaul network depends on the number of eNodeBs in the RAN it is serving. As more eNodeBs are backhauled to the EPC, the cost to move that data, either in terms of fees charged by the capacity provider, or equipment costs for the backhaul links, will rise.

- **Evolved Packet Core (EPC)**

The EPC is a high speed, high bandwidth, high capacity, IP-based real-time switching controller that acts as the central controller of the LTE network. It is typically implemented as a powerful

high performance multi-processor server and transaction processing computer connected to a web of high speed data trunks. The functional elements of the EPC are shown in Figure 6-5. In principle, a single EPC could control the LTE network for the entire United States, though networks are often partitioned for reliability and redundancy and linked together to form a common network.

Recently, smaller EPCs that could serve smaller networks have come on the market. These smaller EPCs could be linked together to form a system of systems if needed. A completely portable example of this was shown by a vendor at the August 2012 APCO exhibition. The entire unit and one associated eNodeB were built into the back of a sports utility vehicle for use at an incident scene, making it a self-contained LTE system.

The major functional elements of the EPC are:

EPC – Mobility Management Entity (MME)

The MME controls the signaling between the UE and the core network. It handles the establishment, maintenance, and release of the data traffic and initial authentication of a user. It also controls the establishment of the connection between the network and UE, its maintenance during mobility, and supports tracking, roaming, and handovers for the UE. The MME is also responsible for finding the UE by paging for an incoming call or session.

EPC – Home Subscriber Server (HSS)

The HSS maintains subscriber information, including the user's QoS profile and any access restrictions to roaming outside the FirstNet network, or, possibly, outside the state. It also holds information about the Packet Data Networks (PDNs) to which the subscriber can connect using Access Point Names (APNs) or a PDN address. This is discussed in Appendix A. The HSS holds real-time information regarding to which MME the subscriber is connected. It also includes the Authentication Center (AUC) to generate the information necessary to authenticate a subscriber. There is one HSS in an EPC, though it may be implemented as a distributed database. Since Oregon will be part of FirstNet, its HSS information will be centralized within the FirstNet core.

EPC – Serving Gateway (SGW)

All user data (packets) are transferred through the SGW. It serves as the anchor when the user's radio transfers its connection to a different eNodeB within the RAN when the user moves. The SGW in commercial application may collect information for billing, such as the number of user packets transmitted during a session. It also acts as the connection point to legacy networks.

EPC – Packet Data Network Gateway (PGW)

The PGW handles IP address allocation as well as the enforcement of such items as guaranteed bit rate providing QoS in the data and traffic rules from the Policy and Charging Rules Function (PCRF). It also acts as the connection point to transfer data to other systems that are not

standardized by the Third Generation Partnership Program (3GPP) organization[37], such as CDMA2000 and WiMAX.

In some implementations, the SGW and PGW may be combined into a single S/PGW router element.

EPC – Policy and Charging Rules Function (PCRF)

The PCRF provides the rules for maintaining QoS for user traffic with dynamic QoS control. It is responsible for authorizing, maintaining, and enforcing the provisioned QoS profile of the subscriber. It provides the QoS authentication, class identifier, and bit rates for the subscriber to be enforced in the PGW.

6.3. Operations and Maintenance

Once a network system has been installed, it must be managed and maintained. The following paragraphs describe the operational considerations for the associated user equipment and the network based on Oregon's current knowledge of FirstNet. Also included is an initial list of considerations for integrating the existing state and local public safety networks with the new NPSBN.

- **User Equipment Maintenance, Trouble Reporting, and Resolution**

Today, each agency owning an LMR radio system negotiates its equipment maintenance and trouble resolution through staff technicians and contracts with vendors. Some states even run their own radio maintenance facilities. In contrast, FirstNet will negotiate a nationwide contract to serve those states that opt in to the system and will also likely require any Opt-Out states to show that they have dedicated staff or contract with an approved contractor. For the latter, it is likely that the Opt-Out maintenance contracts will be at the state level and not a local responsibility. Furthermore, given the relatively low cost of the LTE devices, the contractor will likely follow a replacement system similar to that of commercial cell phone providers. For a per device insurance fee, commercial service providers will simply send a refurbished device to replace a faulty one and repair or discard the non-operational device.

As such, for Oregon, a negotiated service level agreement (SLA) becomes crucial for the NPSBN and with FirstNet. For example, there may be a shipping delay before replacements for defective or damaged equipment arrive. As resolution, Oregon may propose to FirstNet that vendors establish local facilities within Oregon to expedite replacements, possibly delivering the equipment the same day by courier. Alternatively, given the relatively low cost of LTE equipment, Oregon may propose to maintain spares stock itself, as takes place today. The spare radios must be updated and maintained at the current software version level so they may be quickly placed in service by simply switching the SIM cards. However, this approach may prove

[37] 3rd Generation Partnership Project (3GPP) is the standards body responsible for the LTE standard. For more information, see www.3gpp.org.

cost prohibitive for specialized mobile devices. It may also require the addition of more secure storage space and staff trained to troubleshoot LTE equipment to determine usability.

- **Network Management, Monitoring, and Surveillance**

Operations activities such as network management, monitoring, and surveillance are important to supplying reliable wireless service to LTE user equipment. Network management activities include configuration and provisioning of network elements. Other key operation tasks include monitoring for congestion, overload, and mal-operation as well as surveillance (observing) or guarding against hostile attacks, data leaks, and theft. It is reasonable to assume that FirstNet will take responsibility for the monitoring and surveillance of the network, especially since it has been chartered with deploying the network core (EPC), where most processing takes place for these functions. Whether these activities are performed by FirstNet itself or by a contracted commercial carrier, key operations parameters such as network quality, performance, and repair response time will all be SLA items that Oregon will want to review and compare to its needs. For example, this could include considerations of slower response times in rural areas. It could also be structured around clauses specifying the proximity of service centers within some maximum distance or maximum response time from a suitable central city or cities.

For LTE, monitoring network security becomes a centralized function that is associated with the management of the EPC.[38] However, NPSBN security can also be dependent on the security of local PDN connected to it. The responsibility for managing and securing the local PDNs is expected to remain with the local administrators. This clearly requires close cooperation and common security standards, since at the national level the combined PSBN+PDN will be only as secure as its weakest link. For example, even simple Internet access is often a source for malware. The NPSBN may be required to implement its own defensive security gateways through which all traffic to the outside flows, to ensure that the larger network is not compromised.

- **Operational Considerations in Preparing for FirstNet**

Ensuring a robust, useful broadband data service for Oregon's public safety users via NPSBN will require close negotiations with FirstNet regarding SLA terms that meet Oregon's needs. As a prerequisite, Oregon will need to establish an overall *management structure for interacting with FirstNet*, including a single authorized point of contact, as required by the Act. This person, or head of a governing body of officials, must be authorized by the Governor to negotiate with FirstNet. For example, the person or group will need to approve and sign documents with FirstNet on behalf of Oregon. Such efforts require delegated authority to be established in accordance with the procedures followed by the state. Section 8 recommends formally recognizing an Oregon Public Safety Broadband Office (OPSBO) for this purpose.

[38] See Security Policy, NPSTC (2012). *High Level Statement of Requirements for FirstNet Consideration*. A NPSTC Public Safety Communications Report.

In addition to executing an agreement with FirstNet, Oregon must consider how it will *prepare to manage the NPSBN within the state*, i.e., OPSBN. Waiting for FirstNet to define everything first before beginning planning will not leave Oregon sufficient time to assess FirstNet's offer when presented or to provide comments while FirstNet's plans are being developed. Upfront planning will prepare Oregon to quickly respond when asked by FirstNet whether to opt in or out.

For example, some state level operational issues that are better addressed early in the process include:

- Determining a state administrative structure for equipment purchases by statewide agencies, possibly from a FirstNet approved list, as well as user administration and UE provisioning (e.g., device set up and service activation), including where and how they will be performed. These activities could be performed by a single office for all agencies within the state or by an office within each agency.
- Decide whether statewide PDNs should be consolidated or continue to operate separately for each agency.[39]
- To facilitate both security and management, determine which applications should be standardized across statewide agencies. Identify expertise and develop a process for approving special applications to operate inside the state.
- Decide what UE should be standardized across all agencies within the state, as well as determining which specialized but standardized devices meet the needs of individual agencies.
- Identify one or more provisioning agents who will be authorized to access the FirstNet provisioning software to add or delete users, UE, and services. These may be certified state employees or contractors.
- Determine the process controls to keep track of these sophisticated user terminals, to assure none "walk away" or are otherwise misplaced or unused. Assess whether these controls can be satisfied by existing Asset Management policies and procedures.
- Decide whether the state should control the approval and purchases of all terminals within the state (i.e., for both state and local agencies) or whether this should be handled in a decentralized manner.
- Determine how spare equipment should be managed to ensure that there is an adequate inventory but not purchasing so many that they become obsolete before they are put in service. Similarly, determine lease vs. purchase decisions in a way that keeps equipment

[39] Packet data networks (PDN) are referred to as Public Safety Entity Networks (PSEN) in NPSTC's Statement of Requirements (SoR).

current. This is relevant regardless of whether FirstNet dictates equipment choices, since the quantities purchased will depend on state decisions unless FirstNet negotiates nationwide leases.

Corresponding questions at the local level include:

- How can local and county agencies consolidate their PDNs for more efficient operations?
- How can local and county agencies consolidate or standardize their applications to create new statewide standards?
- What local applications may FirstNet standardize?
- How will Oregon-specific standardized applications interact with applications from other states?
- Who are the provisioning agents who are authorized to access FirstNet's provisioning software to add or delete users, UE, and services?
- Could the same UE used by the state also be used by local agencies, including the specialized terminals discussed above? If other terminal types are also needed, can they be standardized across all the relevant local agencies within the state which need them?
- Should they implement the same processes, and administrative and network controls to ensure that these terminals are not lost or misplaced and are appropriately disposed of at the end of useful operational life? Asset Management controls may need to be added to some agencies' contracts if not already in place.
- How should spares be managed to ensure that there is an adequate number while not locking the agencies into using obsolete terminals simply because they had purchased too many? Alternatively, which should be purchased vs. leased and why? While issues such as equipment sparing may be addressed at the state level, it is important to involve local agencies and other stakeholders in decisions that may impact their own operations.

Oregon can begin addressing many of these topics now. Establishing the interim OPSBO, making necessary upfront decisions, and beginning preparations will ensure that Oregon will be ready to respond to FirstNet's requirements.

7. STAKEHOLDERS

The Oregon State Interoperability Executive Council (SIEC) represents the public safety stakeholder community and will remain the key representative entity for stakeholders for OPSBN. However, other interest groups, such as investor partners, become important stakeholders for activities such as network planning and deployment. Further, during network operations, stakeholder user groups will also be coordinated through the existing SIEC. This section highlights the key stakeholder entities requiring representation. The following

Governance section describes the structure and functional linkages for stakeholders to the state and to FirstNet.

7.1. STATE INTEROPERABILITY EXECUTIVE COUNCIL (SIEC) AND OTHER STAKEHOLDERS

The SIEC is chartered with developing policy and guideline recommendations, identifying technology standards, and coordinating intergovernmental resources to facilitate statewide wireless communications interoperability with emphasis on public safety. Current members as appointed by the Governor include representation from the following organizations.[40]

- Oregon State Police (OSP)
- Office of Emergency Management
- Department of Forestry
- Department of Corrections
- Department of Transportation
- Department of Administrative Services
- Department of Human Services (for emergency medical services)
- Oregon Military Department
- Oregon Fire Chiefs Association
- Oregon Association of Chiefs of Police
- Oregon State Sheriff's Association
- Oregon Association of Public Safety Communications Officials/National Emergency Number Association (APCO/NENA)
- Tribal Representative from Confederated Tribes of the Warm Springs
- League of Oregon Cities
- Region 35 Radio Planning Committee
- Association of Oregon Counties
- Special Districts of Oregon
- Two members of the Legislative Assembly with interest in the subject of public safety and wireless communication systems
- Oregon National Guard

[40] State Interoperability Executive Council website, http://www.oregon.gov/SIEC/

- Oregon Department of Public Safety Standards and Training

Added to this list can be local entities that have been actively involved in Oregon's public safety broadband efforts to date, such as the BTOP grant and RFI. These include City of Portland, Lane Council of Governments (LCOG), City of Salem, Washington County Consolidated Communications Agency (WCCCA), and Clackamas County Communications (C-800).

For the purposes of OSPBN, the list of stakeholders is expected to expand and evolve to include other potential users such as utilities, federal civil and military organizations, as well as public-private partners and private sector entities. The latter may include telecommunications service providers, fiber consortiums, and equipment manufacturers. The former may include federal agencies such as:

- DHS Federal Emergency Management Agency (FEMA)
- DHS Office of Emergency Communications (OEC)
- Customs and Border Protection (CBP)
- Federal Bureau of Investigation (FBI)
- Department of the Interior (DOI) Bureau of Land Management (BLM)
- Department of Defense (DOD)

For example, DOD users may make use of the network during combat training at training centers and test ranges as well as to support public safety activities at military bases.

7.2. Stakeholder User Groups

Stakeholder user groups would be coordinated through the existing SIEC, consist of the public safety entity users of the OPSBN, and may be organized by region. Users would include public safety, law enforcement, fire, emergency response, emergency medical services, and related personnel, agencies, and authorities. Additionally, the user base should include any emergency response agency or authority with Emergency Support Function (ESF) responsibilities as noted in Table 7-1 below.

Table 7-1 Emergency Support Functions

Emergency Support Functions	
ESF1	Transportation
ESF2	Communications
ESF3	Public Works and Engineering
ESF4	Firefighting
ESF5	Emergency Management
ESF6	Mass Care, Housing, and Human Services
ESF7	Resources Support
ESF8	Public Health and Medical Services
ESF9	Urban Search and Rescue
ESF10	Oil and Hazardous Materials Response
ESF11	Agriculture and Natural Resources

Emergency Support Functions
ESF12 Energy ESF13 Public Safety and Security ESF14 Long-term Community Recovery and Mitigation ESF15 External Affairs

ESF is the grouping of governmental and certain private sector capabilities into an organizational structure to provide support, resources, program implementation, and services that are most likely needed to save lives, protect property and the environment, restore essential services and critical infrastructure, and help victims and communities return to normal following domestic incidents.[41]

7.3. PARTNERS

Investor partners would be entities with a financial interest in the successful implementation of OPSBN. These entities would realize tangible benefits from establishment of the network. Potential partners include entities from the local, state, and federal levels, as well as the telecommunications, utilities, and maritime sectors. Local, state, and federal agencies and departments would benefit from the availability of the broadband network to enhance function and operations. Telecommunications service providers would benefit from the use of infrastructure, service, and applications on the network. Likewise, utilities, as secondary users on the network, would benefit from shared access on the network for their own data. Use of lessons learned in public-private partnerships such as those forged by Oregon's Office of Innovative Partnerships and Alternative Funding via their Oregon Innovative Partnerships Program (OIPP) will be leveraged to identify participants. Potential partner entities are summarized in Table 7-2.

Table 7-2 Potential Investor Partners for OPSBN

Partner Entities	
Local • Municipalities • Public Safety Answering Points (PSAP) • Police • Fire • EMS	**Telecommunications** • National network service providers • Local and private network service providers • Backbone service providers • Internet Service Providers • Tower owners
State • Department of Transportation • Oregon State Police (OSP) • Department of Corrections • Department of Forestry • Oregon Military Department • Department of Public Safety Standards & Training	**Utilities** • Electrical • Gas • Water • Sewer

[41] Retrieved from http://www.phe.gov/preparedness/support/esf8/pages/default.aspx

Partner Entities	
• Oregon National Guard • Oregon Department of Fish & Wildlife	
Federal • Homeland Security • Department of the Interior (DOI); U.S. Forestry Service; Bureau of Land Management, National Park Service • Department of Defense (DOD) • Bureau of Reclamation, Hydroelectric / Dam infrastructure; U.S. Army Corps of Engineers	**Maritime** • Merchant Exchange • U.S. Coast Guard • River Guard • Oregon Port District

8. GOVERNANCE

This section discusses the national level organizational structures and responsibilities of the First Responder Network Authority (FirstNet), how the national level will coordinate with Oregon, and how Oregon will organize for the planning and implementation of the NPSBN.

The federal Middle Class Tax Relief and Job Creation Act of 2012 (the Act) was adopted on February 22, 2012. The legislation calls for the establishment of two national governance entities, a time-limited Technical Advisory Board for First Responder Interoperability and a standing FirstNet Board of Directors.

- **Technical Advisory Board for First Responder Interoperability**

The FCC Technical Advisory Board for First Responder Interoperability (Interoperability Board) is a short-term entity tasked with developing the minimum technical requirements to ensure nationwide interoperability of the NPSBN. The Interoperability Board is composed of 15 members; four representing public safety, three members of State and local governments, four on behalf of wireless providers, and three representing equipment manufacturers. Upon FCC approval of the technical requirements, the Interoperability Board's role is finished and the board is terminated. The Interoperability Board completed its Final Report on May 22, 2012.[42]

- **FirstNet Board of Directors**

The FirstNet Board of Directors, established by the NTIA, is the governing authority of the NPSBN and the managing entity for the public safety spectrum, the license for which was granted to FirstNet by the FCC on November 15, 2012 for an initial term of ten years.[43] FirstNet comprises 15 members including the DHS Secretary, the Attorney General, the Office of

[42] Technical Advisory Board for First Responder Interoperability (2012, May 22). Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network, *Final Report*.
[43] Press release: http://www.ntia.doc.gov/press-release/2012/firstnet-praises-fcc-granting-spectrum-license

Management and Budget (OMB) Director, and 12 additional members appointed by the Secretary of Commerce. Of the final 12 members, at least three are local, state, or tribal, at least three are public safety, at least one has technical expertise, at least one has network expertise, and at least one has financial expertise. These members were announced on August 20, 2012 by the U.S. Commerce Secretary and include Jeff Johnson, the former chair of the Oregon SIEC.[44] See Table 8-1.The board held its first meeting on September 25, 2012, where it adopted bylaws and delivered conceptual network and applications presentations.[45]

Table 8-1 FirstNet Board of Directors[46]

FirstNet Board of Directors
• Sam Ginn, Chairman, former Chairman of Vodafone AirTouch and Pacific Telesis • Craig Farrill, Co-founder of Kodiak Networks, formerly of Vodafone and AirTouch • William Keever, retired regional president for Vodafone, AirTouch, Pacific Telesis • Paul Fitzgerald, Sheriff, Story County, Iowa, former president, National Sheriff's Association • Deputy Chief Chuck Dowd, NYPD, Major Cities Chiefs Police Association representative • Jeff Johnson, Fire Chief (retired), former President, International Association of Fire Chiefs • Kevin McGinnis, Program Manager, National Association of State EMS Officers (NASEMSO) • Tim Bryan, CEO, National Rural Telecommunications Cooperative • Ed Reynolds, retired, former president of BellSouth Mobility and AT&T executive • Susan Swenson, retired, former president & CEO of Cellular One • Teri Takai, DOD CIO and former CIO of Michigan and California • Wellington Webb, former Mayor of Denver, Colorado • Secretary of Homeland Security Janet Napolitano • Attorney General Eric Holder • Director of the Office of Management and Budget (Acting) Jeffrey Zients

FirstNet is responsible for overseeing planning, deployment, and operation of the NPSBN. This includes development of RFPs, roaming agreements, and determination of network infrastructure and grant funding.

While FirstNet is the national governing authority, it is required by statute to consult with state, local, regional, and tribal jurisdictions in areas of management, standards, certified equipment list, RFPs, commercial infrastructure, contracts, cyber-security, public safety answering points, rural deployment, and prohibition of the provision of consumer services.[47]

A critical milestone for FirstNet is to provide sufficient information to states to enable objective decision making to opt in or out of the NPSBN. This will require effective communication between FirstNet, states' representatives, and stakeholders.

[44] Press release: http://www.commerce.gov/news/press-releases/2012/08/20/firstnet-board-members-appointed-acting-us-commerce-secretary-rebecca

[45] http://www.ntia.doc.gov/other-publication/2012/firstnet-board-actions-09252012

[46] Barnett Jr., J.A. (2012, September 24). *What Should FirstNet Do First? State Integration into the National Public Safety Broadband Network*, p. 7. Retrieved from http://potomacinstitute.org/attachments/article/1294/FirstNet%20NPSBN%20Report.pdf

[47] OEC (2012, April 17). *Statewide Communication Plan Interoperability Plan (SCIP) Implementation Workshop, Oregon*.

8.1. MANAGING ORGANIZATION

Overseeing FirstNet implementation in Oregon will be a complex undertaking that combines policy, technology, advocacy, and resource allocation. A broad mix of skill sets will be required and includes: management (administration, technical, and fiduciary responsibility); leadership (at the highest levels of state and local governments); stakeholder participation (agencies, governments, and end-users), as well as oversight and governance.

- **Oregon State Interoperability Executive Council (SIEC)**

The Oregon State Interoperability Executive Council (SIEC), created by Governor's Executive Order 02-17 in 2002, is charged with improving and developing interoperable public safety communication systems in Oregon. Through the Governor, its advisory recommendations form public safety communication policy in Oregon.[48] The SIEC is the ideal governance structure to engage key stakeholders in the public safety community across Oregon, receiving inputs and communicating information locally regarding the rapidly changing FirstNet initiative.

- **Oregon Public Safety Broadband Office**

The Act calls for states to designate a single officer or governmental body to serve as point of contact (POC) to coordinate with FirstNet. To facilitate day-to-day program management and coordination activities with FirstNet for Oregon, the State has established an interim Oregon Public Safety Broadband Office (OPSBO) to be advised by the SIEC and to serve as the single POC to FirstNet. The OPSBO will initially reside within the Major Projects Branch (MPB) of the Oregon Department of Transportation (ODOT). The OPSBO performs as administrative and financial manager for Oregon's PSBN, with ODOT as the state agency that is assigned contracting authority to execute the implementation planning grant.[49] Then, during the 2013-2015 biennium, the OPSBO is planned to migrate to the Oregon Department of Administrative Services (DAS), aligning its oversight with that of the SIEC.[50]

In the current arrangement, the OPSBO would report progress through MPB and the Management Steering Committee described in the following subsection, to ODOT, through the Oregon Transportation Commission, to the Governor's Office. The established SIEC would continue to serve as the single voice for stakeholders, reporting to the Governor's Office and functioning in an advisory role to the OPSBO.

See Figure 8-1 for this governance management structure showing the chain of responsibility.

[48] ODOT (2012, December). *Voice Radio Communications*. Oregon Department of Transportation State Radio Project Draft Discussion Paper, p. 1.
[49] On August 21, 2012, the Department of Commerce through the National Telecommunications and Information Administration (NTIA) published guidance on Development of Programmatic Requirements for the State and Local Implementation Grant Program to Assist in Planning for the Nationwide Public Safety Broadband Network (NPSBN). See http://www.ntia.doc.gov/files/ntia/publications/fr_sligp_08212012.pdf
[50] ODOT (2012, December). *Oregon's FirstNet (Broadband) Implementation*. Oregon Department of Transportation State Radio Project Draft Discussion Paper, p. 3.

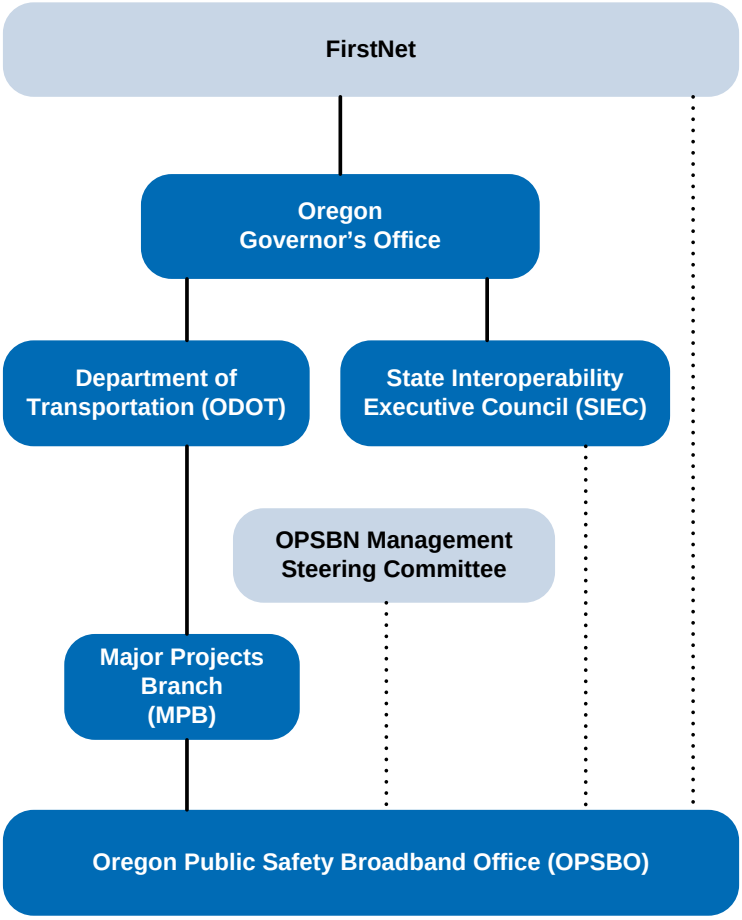


Figure 8-1 Oregon Public Safety Broadband Governance Management Structure

8.2. OPSBN Management Steering Committee

A collaborative approach will be required to implement the OPSBN. ODOT has established a Management Steering Committee that can oversee the OPSBO and ensure that reports and proposals submitted to the Oregon Transportation Commission, the SIEC, and the Governor are fully vetted and supported. The OPSBN Management Steering Committee members include:

- Governor's Advisor
- SIEC Chair
- State CIO
- ODOT Deputy Director
- OIPP Representative
- ODOT MPB Manager
- OPSBO Program Manager

It is anticipated that ODOT will request the SIEC Chair, or delegated representative, to continue to serve on the Management Steering Committee. As the project evolves, investor partners may be added as well as representative end-users suggested by the SIEC. Establishing a technical subcommittee may also be considered.

- **Communicating Stakeholder Needs to FirstNet**

In concert with the functions performed by the Management Steering Committee, it is expected that the SIEC will coordinate stakeholder user group representation. See Section 7 for a description of these organizations. The SIEC would offer a single voice for the stakeholder user groups, soliciting feedback, and consolidating input for recommendation as a member of the Management Steering Committee and to the OPSBO.

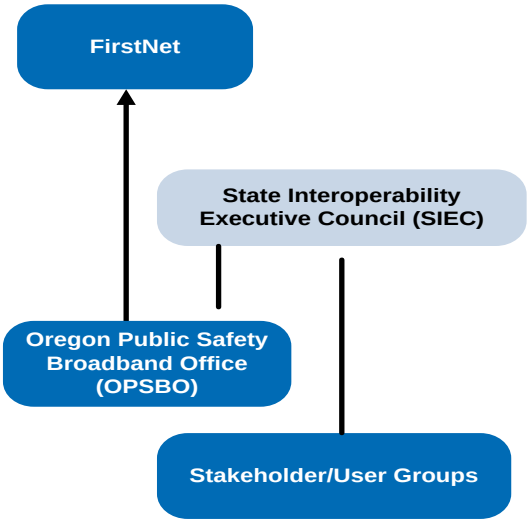


Figure 8-2 Stakeholder and User Information Flow

Stakeholder groups would be formed under and report through the SIEC, offering inputs regarding the network from a user perspective. Stakeholder feedback would be reported via the SIEC to the OPSBO, which will provide the input to FirstNet for consideration and action. Investor partners will be coordinated through Oregon's Office of Innovative Partnerships and Alternative Funding. Figure 8-2 illustrates the complete information flow, from local user to FirstNet at the federal level.

9. BENEFITS AND VALUE

As described in Section 6.1, Use and Applications, public safety broadband offers users a vast array of potential applications. In use, these applications greatly improve the speed, efficiency, and resulting effectiveness of public safety operations. This increased mission effectiveness represents the real benefit and value of the public safety broadband network. It is reflected by increased situational awareness, decreased response times, enhanced safety, and improved

efficiency. This section further describes these benefits using information supplied by RFI respondents as well as Oregon public safety users in the 2012 broadband survey.

- **Increased Situational Awareness**

During an incident, situational awareness – knowing what is happening to whom, where, and when – is key for public safety officials to effectively plan and manage emergency response and coordination. Public safety broadband will enhance situational awareness through distribution of messages, images (such as floor plans, mug shots, and incident stills) and videos, including surveillance feeds and on-scene video.[51] In the future it will support NG 9-1-1 service, offering life-saving information in the form of images, text, and video, as well as medical telemetry with streaming data. Broadband greatly increases the amount and variety of information flow resulting in rapid dissemination of vital data, enabling a more comprehensive common operating picture; one that improves decision making and response effectiveness.

- **Decreased Response Times**

Public safety broadband provides interoperable sharing of information in real-time resulting in improved communication among public safety personnel. With increased situational awareness, officials will have the ability to turn data into actionable information. As noted in Harris Corporation's response to Oregon's RFI, the ability to monitor high resolution dash cam video, or sending hazardous material abatement information directly to first responders at the scene, increases the knowledge base when responding to an incident.[52] Response times are in turn reduced as a result of information being available to responders as they reach the scene, as well as coordinated actions that could immediately be initiated upon arrival at an incident.

- **Enhanced Safety**

With greater interoperability, situational awareness, and communication, safety can be improved for both first responders and the public. Geo-location services, incident video feeds, traffic alerts, images such as floor plans, hazardous material data, and medical telemetry are just some examples of capabilities that will provide valuable benefit to overall safety through informed response decisions and actions. The wealth of information offered via broadband capably equips responders entering a developing incident or situation.

- **Improved Efficiency**

Public safety broadband provides an additional benefit of improved staff efficiency in day-to-day operations. For example, web access to databases and remote form entry decreases paperwork, increasing the amount of time personnel spend on patrol.[53] As another example, today OSP

[51] Alcatel-Lucent (2010). *Ultimate Wireless Broadband Solution for Public Safety*, p. 3-4.
[52] Harris Corporation (2012, March 2). *Response to the State of Oregon's Request for Information and Expression of Interest (RFI-EI) for Public Safety Long Term Evolution Broadband Spectrum Network Proof-of-Concept Pilot (LTE PSBN Pilot)*, p. 29.
[53] Alcatel-Lucent (2010). *Ultimate Wireless Broadband Solution for Public Safety*, p. 3-4.

mobile data terminals (MDTs) must be brought into the field office for upgrades and routine software updates, taking vehicles out of service for up to hours. Using the public safety broadband network to transmit this information would enable routine updates to be carried out in the field rather than in the office. With hundreds of MDTs in service, considerable time and cost savings would be realized with the improved efficiency afforded by public safety broadband. In the future, labor saving applications incorporating license plate recognition, scanning of driver licenses, facial recognition, and other advanced technologies can free time in a busy officer's day.

As described in Section 6.1, NPSBN can enable the creation of a public safety cloud that promises significant cost savings and efficiency gains for application users. It can potentially offer public safety applications such as common access to national, state, and local databases, CAD, and other incident response systems on a regional state, multi-state, or even national basis. Offering common, standardized, centralized applications eliminate costly replication of local systems that "can't talk to each other," instead offering a common view and access to data by all authorized users regardless of their physical location.

- **Benefits over Commercial Networks**

A dedicated PSBN provides benefits not available using only commercial networks, namely coverage of important geographical areas and the ability to prioritize bandwidth. In their response to Oregon's RFI, Harris Corporation explains these benefits as:

- **The ability to build a network that provides coverage where public safety operates.** Commercial networks are built to cover significant population areas, and geographic areas readily accessed by the public. However, public safety must be prepared to react in both accessible and inaccessible areas. Public safety may also benefit from coverage in court houses, jails, parks, and rural highways where cellular coverage is not deemed commercially viable.
- **The ability to control priorities for bandwidth allocation**. When a catastrophic event occurs, public safety users cannot be competing with civilians who congest the bandwidth to send cell phone videos to friends or news outlets. If such a congestion of the broadband network were to occur, the public safety response may be critically hampered or delayed. A public safety broadband network allows public safety administrators to have access to priority control, managing priorities in real time so that the information deemed most important is the information that gets the highest priority. [54]

[54] Harris Corporation (2012, March 2). *Response to the State of Oregon's Request for Information and Expression of Interest (RFI-EI) for Public Safety Long Term Evolution Broadband Spectrum Network Proof-of-Concept Pilot (LTE PSBN Pilot)*, p. 29.

Alcatel-Lucent described similar benefits in their RFI response,[55] noting that commercial providers only provide a best effort service and typically insufficient bandwidth and QoS compared to what is expected for public safety use. During emergencies, commercial traffic becomes very congested, adversely affecting any public safety communications being carried on the same network. A dedicated public safety broadband network with its own spectrum is needed to provide full control over the priorities associated with the users of the network.

Additionally, once built, the public safety broadband network can be viewed as a "socioeconomic equalizer"[56] that brings broadband connectivity to rural areas currently without access – areas where commercial providers would not have invested to due to the low profit margin. Broadband will create opportunities for public-private partnerships to expand access to public safety responders in rural areas.

These benefits are consistent with those identified by users in the State of Oregon Current State Mobile Data Survey Results conducted in April 2012,[57] which listed the top three positive outcomes from responder use of current wireless data systems as enhanced employee safety, rapid dissemination of critical information, and decreased response times. The positive impact of wireless data as reported by survey respondents is shown in Figure 9-1.[58]

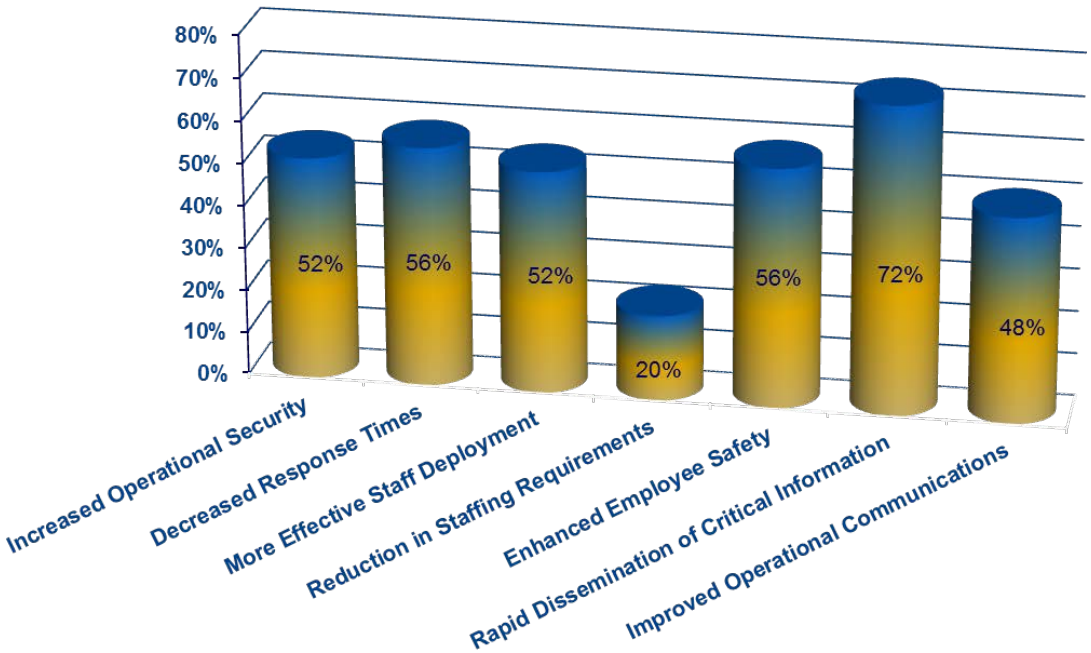


Figure 9-1 Survey Respondents Experience Positive Impacts of Wireless Data Use

[55] Alcatel-Lucent (2012, March 2). *Response to RFI-EI 00060 Oregon Public Safety Long Term Evolution Broadband Spectrum Network Proof-of-Concept Pilot (LTE PSBN Pilot)*, p. 35-36.
[56] Roberts, M. R., (2012, May 1). Fire's Case for Broadband. *Urgent Communications*. Retrieved from http://urgentcomm.com/networks_and_systems/mag/fire-ems-broadband-needs-201205/index.html
[57] OEC (2012, June 21). Oregon Broadband Survey Workshop, Portland, Oregon.
[58] OEC (2012, May 30). Review of Public Safety Wireless Data Usage, State of Oregon, Portland Area.

Oregon's public safety agencies already recognize the benefits of mobile data. A public safety broadband network would leverage LTE technology to create an interoperable network for public safety that would increase situational awareness, decrease response times, enhance safety, and improve efficiency of operations. Their successful use of wireless data today is the best demonstration of how LTE broadband network will enhance public safety mission support capabilities tomorrow.

10. BUSINESS MODEL AND FINANCIAL CONSIDERATIONS

This section discusses the funding and financial considerations associated with FirstNet and the OPSBN. It provides an overview of the anticipated business model for sustaining OPSBN operations and analyzes the overall implications for Oregon, offering suggestions to ensure a solid financial footing.

- **Funding Associated with FirstNet**

As described in Section 5, in February 2012 the president signed the Middle Class Tax Relief and Job Creation Act, establishing and funding FirstNet. The Act authorizes NTIA to provide $135 million shared across 56 states and territories to support state and local efforts to plan and integrate with the NPSBN. This grant requires a 20 percent match by the state unless waived by NTIA. The Act further authorizes the FCC to conduct incentive auctions to raise $7 billion for constructing the NPSBN and establishes the Public Safety Trust Fund to support NPSBN efforts. The funding will not be available to build the network until FirstNet completes the supplier RFP process and contracts are awarded. A timeline for these events can be found in Section 13. The law also provides up to $2 billion in borrowing authority for building that states can draw upon until proceeds from the auctions are available.[59] As auction revenues are deposited in the Fund, they are allocated in priority order. Table 10-1 shows the funds available for NPSBN legislated by the Act. In the long term, current plans foresee the network being sustained by fees paid by public sector users.

- **FirstNet Funding Implications**

When divided across 56 states and territories, Oregon's share of the initial $135 million implementation grant for planning FirstNet activities is estimated to be $1.5-3 million. The monies will be distributed in two phases. Phase One focuses on initial planning and consultation activities, including strategy and timeline development, meetings, governance planning, and outreach and education efforts. Phase Two activities will include additional consultation and planning for undertaking statewide data collection.[60]

[59] National Governors Association (2012, June 28). Preparing for Public Safety Broadband. *White Paper*. Retrieved from http://www.nga.org/files/live/sites/NGA/files/pdf/1206PREPAREBROADBANDPAPER.PDF
[60] NTIA (2012, August 22). *APCO Session: Preparation for the State and Local Grant Program*, p. 9.

Of the $7 billion planned for FirstNet, $2 billion is available now, having been advanced by the U.S. Treasury in the form of a loan against the proceeds from the upcoming spectrum auctions.[61] The rest becomes available as spectrum is auctioned, with the last auction set to complete in 2022. As much as $3 billion is anticipated to be set aside for "hardening" broadband service providers' existing core networks.

Clearly, additional funding will be needed beyond the $7 billion for a nationwide deployment. To put this into perspective for Oregon, the cost estimate for Oregon State Radio Project's (SRP's) 335 LMR sites for the whole state was originally $600 million. LTE technology requires a higher tower site density than LMR. Assuming similar site build scenarios and a 1:5 LMR to LTE density ratio, the over 1,500 LTE sites required to offer the same coverage would likely exceed $1 billion in cost for Oregon alone.[62] Separately, at the August 2012 Association of Public Safety Communications Officials (APCO) annual meeting, Verizon stated it has spent $9 billion so far to upgrade some of its sites to LTE, and well over $100 billion to build its combined 2G, 3G, and 4G networks to date.

Table 10-1 NPSBN Funding Afforded by the Middle Class Tax Relief and Job Creation Act[63]

No.	Fund	Distribution	Description
1.	State and Local Implementation Fund (NTIA)	$135M	Supports state and local efforts to plan and integrate with the NPSBN. Includes an 80% Federal share. (NTIA may borrow the entire amount upfront)
2.	Network Construction Fund (FirstNet)	$7B	Supports the design, construction, operation, maintenance, and upgrade of the NPSBN (NTIA may borrow up to $2B upfront)

- **Business Model**

FirstNet service is being planned to be financially self-sustaining. The legislation offers no funding for ongoing operations and maintenance. Under FirstNet, the business model is fee based and comes with three revenue sources:

- Network User Fee – Fee from each entity including public safety or secondary user that uses the network
- Lease Fee for Network Capacity – Fee for agreement between the FirstNet and secondary user(s) to permit secondary access

[61] Barnett Jr., J.A. (2012, September 24). *What Should FirstNet Do First? State Integration into the National Public Safety Broadband Network*, p. 37. Retrieved from http://potomacinstitute.org/attachments/article/1294/FirstNet%20NPSBN%20Report.pdf
[62] Discussion points from the OPSBN Business Plan Kickoff Working Session, June 8, 2012.
[63] OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon, p. 36.

- Lease Fee for Network Equipment and Infrastructure – Fee for entity that seeks access or use of antennas, towers, and other assets constructed or owned by FirstNet[64]

The first is anticipated to be the largest source, i.e., revenue from recurring public safety user subscriber fees. Information is not yet available as to whether this fee will be a flat rate, e.g., monthly flat rate per subscriber, or usage based arrangement. FirstNet could choose to negotiate a flat fee with carriers that includes all roaming. A tiered pricing model is also possible, with flat prices for in-network and roaming users depending on usage up to a certain number of megabytes, or for unlimited data usage.

For an Oregon perspective, the DHS OEC on behalf of Oregon conducted a survey on public safety wireless data usage. The purpose of the survey was to establish a baseline of data regarding the current state of wireless services in the Portland, Ore. region, which included questions on current user preferences in rate structures and billing formats. The most widely used rate structure for wireless device billing was a flat rate per device, with 80 percent of commercial service offered at a flat rate and 100 percent for privately owned networks. This was felt as preferred because it is predictable and therefore easier to budget. Figure 10-1 shows the rate structures for the commercial users surveyed. The OEC survey results also noted that paper billing was the predominant invoice format, as depicted in Figure 6-2.

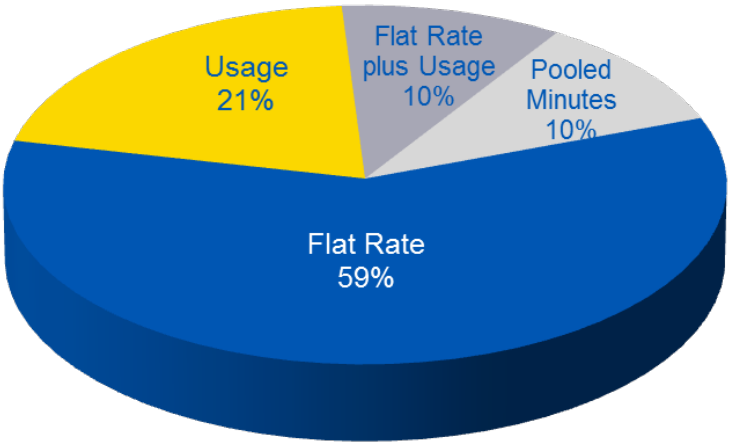


Figure 10-1 Survey Reported Rate Structures for Commercial Wireless Service[65]

Regarding billing, it has not been determined whether invoices will come from FirstNet or the contracted service provider and whether roaming charges will be billed separate or together with FirstNet charges. Also unknown is whether invoices will go directly to user agencies, which would be preferred, or received via the state POC.

[64] OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon, p. 42.

[65] OEC (2012, June). *Review of Public Safety Wireless Data Usage, State of Oregon, Portland Area*, p. 19. Used with permission.

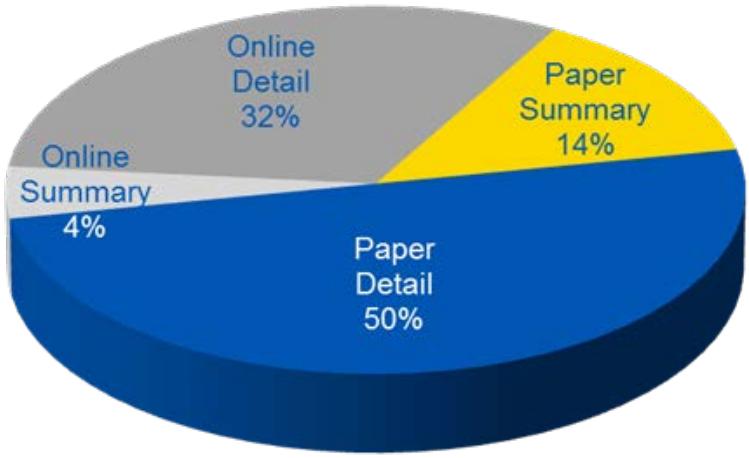


Figure 10-2 Survey Reported Billing Formats for Commercial Wireless Service[66]

- **Impacts to Oregon**

As a rural state, Oregon's geography and demographics impact the relative importance of the major cost elements associated with a network deployment such as NPSBN. These major cost elements include:

1. Radio Access Network (RAN)
2. Backhaul (both from eNodeBs and out to EPC)
3. LTE Core Network (Evolved Packet Core, or EPC)
4. Roaming on to commercial networks[67]

The decision on whether to opt in or opt out typically revolves around the first three items. For example, FirstNet may allow an Opt-Out state to build its RAN and backhaul network but still use FirstNet's core. Or, the Opt-Out candidate may choose to build everything: RAN, Backhaul, and EPC. This assumes it can connect seamlessly to the FirstNet EPC and access all FirstNet features, such as enabling security and sub-network mobility to flow through the state network. Assuming that the Opt-Out builder conforms to the same network performance requirements and covers the same geography as the FirstNet builder, all costs at a macro level remain approximately the same for these three areas regardless of Opt-In or Opt-Out decision. What changes is who is responsible for implementing them. Note that an exception could be the cost of implementing a local EPC. This would increase local hardware costs while decreasing backhaul cost since the amount of user and control data traveling cross-country to the FirstNet EPC would be reduced.

[66] OEC (2012, June). *Review of Public Safety Wireless Data Usage, State of Oregon, Portland Area*, p. 19. Used with permission.
[67] See Figure 6-4 and Figure 6-5 in Section 6.2 for more information regarding network architecture elements.

However, it's the fourth item – roaming to the commercial network when out of range of the dedicated OPSBN – that varies greatly between regions. For example, a police officer in densely populated New York may almost always be in the area served by the dedicated private network and rarely require roaming to the commercial network. A higher roaming rate would be incidental and of little consequence to this user. Not so in rural Oregon. For large areas of the state, public safety users may be on the commercial network *more* than the dedicated private network. Therefore, negotiating favorable roaming agreements and rates may become paramount to Oregon. Alternately, FirstNet could negotiate a flat roaming rate across the country, enabling the densely populated big cities to offset the cost to the rural states. This approach is similar to commercial service providers' roaming arrangements with other carriers within the United States. This arrangement was adopted over time by the service providers since no commercial carrier covers the entire country uniformly.

Another important implication to consider is the long, multi-year deployment horizon for FirstNet when contrasted with the rapid evolution of cellular technology. Stakeholders have expressed concern that if their state is scheduled for deployment in outer years, the 4G LTE technology may be obsolete before its deployed; being already replaced by its successor in the commercial networks. This not only increases public safety network costs by supporting end-of-life equipment, it can also negatively affect adoption rates. That is, the goal is to have as large a subscriber base as possible, to make PSBN service affordable and lower the cost per user. However, many areas, such as Portland and Salem, have 4G LTE service now, with growing numbers of public safety agencies using the commercial service, as is illustrated in Figure 6-1, Figure 6-2, and Figure 6-3 in Section 6. If Oregon gets scheduled in the later years for deployment, many more public safety users will already be on commercial service and will also have the dense coverage of a mature commercial network. Therefore, the cost, coverage, and quality of FirstNet service must be very competitive or else cash-strapped agencies may forego FirstNet altogether.[68] This has the potential to create a downward spiral of a dwindling user base and an ever increasing service cost. NTIA and FirstNet are aware of these concerns and may have states commit to a certain amount of usage before building. However, that merely transfers the risk to the state. A build in the early years, extending the subscriber base to secondary users such as utilities, federal, and DOD users, and negotiating tiered rates for rural use will help to mitigate this risk.

Conversely, FirstNet could be forced to upgrade its infrastructure regularly in order to remain compatible with commercial technology development and rollout and to continue to enable roaming. This transfers more of the risk to FirstNet, especially with respect to the EPC. This may be mitigated by future terminal chipsets having the more advanced capabilities of the then

[68] See "The Other Opt-Out" in: Barnett Jr., J.A. (2012, September 24). *What Should FirstNet Do First? State Integration into the National Public Safety Broadband Network*, p. 26. Retrieved from http://potomacinstitute.org/attachments/article/1294/FirstNet%20NPSBN%20Report.pdf

current commercial networks, while still supporting an older FirstNet air interface, should the NPSBN fall behind.

In light of the above observations, the following are recommended actions to prepare for a financially sustainable and timely OPSBN implementation:

- Prior to receiving the network deployment offer from FirstNet, develop a pro forma cost-benefit comparative analysis to understand the key drivers for Oregon. That way, when an official offer is presented, accompanied by a tight response deadline, decision makers will already know what aspects of the offer are important for Oregon and for which estimates to obtain the most precision. This will enable a rapid, complete, and confident response to FirstNet. Note that this knowledge of critical financial drivers, such as Oregon's rural-metropolitan mix mentioned earlier, is important even for Oregon's Opt-In position. This information will become critical when negotiating FirstNet rate structures and SLA terms favorable to the state's public safety agencies.
- Make the most use of existing information in advance of data collection to establish a rough financial baseline against which to compare incoming new information for reasonableness. As a start, a high level summary of ODOT's BTOP grant proposal is attached as Appendix D. This information can also be used to initially populate a financial model that can later be filled with more refined data as it becomes available.
- Leverage the Department of Administrative Services (DAS) Oregon Broadband Mapping Project data to reduce data collection efforts. The project, with input from approximately 103 service providers, illustrates existing broadband coverage across Oregon and makes this data available at www.oregon.gov/broadband.
- Work with OIPP to determine the level of effort and needs in formulating public-private partnerships to leverage existing state fiber infrastructure.
- Once sufficient information becomes available during data collection, perform financial analyses to answer key questions to assist Oregon decision makers, including:
    - In what regions and to what extent local public-private partnerships are required to make FirstNet service financially viable and attractive to public safety users?
    - Given current adoption rates for commercial service by public safety users, at what price point(s) will a particular region forego private OPSBN service and rely on existing 3G or 4G commercial service for data communications?
    - Conversely, are private network specific capabilities, such as preemption, added network reliability, and private network specific applications sufficient to make private service a "must have" for effective public safety mission support use? If so, what is the added premium that users would be willing to pay?

- Identify and engage participation of secondary users such as secondary responders and public services, including utilities to increase the user population base and so reduce overall cost per user to a sustainable level. A separate pricing plan for secondary users should also be considered, such as for Machine-to-Machine (M2M) use for automated meter reading by utilities, if FirstNet does not mandate a standard rate across the country.
- Work closely with FirstNet to develop financially viable commercial roaming agreements with carriers offering SLAs suitable for public safety mission support activities.
- Propose FirstNet offer service tiers that accommodate rural needs at a lower, more affordable cost. Identify what compromises will need to be made in return.
- Under FirstNet, offer arrangements that incorporate 3G data service in rural areas that are unsupported by 4G LTE service providers.
- Enhance the Opt-In decision by advocating a "bolt-on" deployment strategy that is synergistic with commercial service providers' implementation strategies to minimize time-to-market for FirstNet service and to get FirstNet applications in the hands of users as soon as possible to avoid obsolescence.

11. BOUNDARIES AND ASSUMPTIONS

An important aspect for success for any program is to have a clearly defined scope that is fully communicated by the program owner or sponsor to the delivery team, program management, and stakeholders. When defining this for a major statewide effort such as OPSBN, it is important not only to describe what it is, but also what it's not. This section complements Section 6, Service Description, by identifying the constraints, exclusions, and assumptions that underlie implementation and operation of OPSBN.

11.1. CONSTRAINTS

With the advent of the Act, the FirstNet legislation defines many of the constraints that will apply to the planning, installation, and ongoing network operation. The following list represents these and others items constraining and so further defining OPSBN.

C1. OPSBN must satisfy the PSBN Minimum Technical Requirements to the extent adopted by FirstNet.

C2. Oregon is not allowed to offer commercial service to consumers.[69]

C3. In applying for and accepting federal funds for planning consultation grants, Oregon must conform to the federal grant conditions, such as providing 20 percent matching funds or receiving a waiver from FirstNet.

[69] OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon, p. 31.

C4. Any matching contributions or other program expenditures must be part of the legislative budget.

C5. For the state to authorize and allocate funds to the program, the state must have visibility into FirstNet network cost assumptions and calculations, as required by law for justification.

C6. The network throughput and capability is currently limited to the FCC-mandated LTE standard.

C7. Current public safety LTE devices are capable of data communications only. Voice communications may become available in the future but standardized PTT voice capability has yet to be defined.

C8. The rate of technology adoption will be limited by human change capacity, i.e., successful technology adoption will require implementing a change management strategy that includes a communications plan and training.

11.2. EXCLUSIONS

The following items help bound the scope of the OPSBN program by illustrating areas that are not within the program's scope. These areas include:

E1. Initially, FirstNet will be building an LTE network. It is not a *converged* network that integrates the LMR voice network into the LTE OPSBN.

11.3. ASSUMPTIONS

As with any new initiative, defining assumptions are critical in successfully executing the program as well as understanding and communicating it to stakeholders. For OPSBN, key assumptions include:

A1. Oregon's initial position will be to opt in to the FirstNet national public safety network.

A2. Oregon will not perform as builder agent or manage Oregon's portion of the NPSBN. Therefore, many of Oregon's initial decisions will be business, financial, or process in nature; in contrast to technical decisions regarding network performance, for example.

A3. Oregon will continue to be an active participant of the Operator Advisory Committee (OAC) after it becomes an independent entity, separate from the Public Safety Spectrum Trust (PSST).

A4. The governance of the OPSBO will take place within the department to which the Governor assigns administrative, technical, and fiduciary responsibility for the execution of funding for OPSBN.

A5. The State will be expected to act as the central clearinghouse authority for information coming from local jurisdictions in Oregon to FirstNet. Further, the State will represent Oregon public safety interests to FirstNet.

A6. The SIEC will represent stakeholders and advise the OPSBO through the OPSBN Management Steering Committee on issues from a user perspective.

A7. OPSBN will be used to offer mission *support* and not supply mission *critical* services, such as public safety voice communications, within the initial planning horizon.[70]

A8. Secondary users will be allowed use of the network. These users include transportation, public works, and utilities.[71]

A9. Gaps in coverage are expected in the initial deployment of the dedicated public safety network. Therefore, means to bridge the gaps will be required. This may include use of a commercial LTE network.

A10. Use of and roaming onto commercial carrier LTE networks is a necessary capability for OPSBN users.

There are many areas yet to be defined regarding FirstNet and its interactions with the states, and therefore, also with the implementation of OPSBN. As such, the set of boundary conditions above are part of the "living document" aspect of this plan and will be refined and added to in the coming months prior to implementation.

12. RISK MANAGEMENT

Every program worthy of execution has risk. Risks pertain to the threat of potential events or circumstances that could jeopardize success of the endeavor.[72] The State of Oregon categorizes risk for its Information Technology (IT) projects into two main areas, Business or Organizational Risks and Technical Risks.[73] Table 12-1 lists the risks and potential mitigations associated with successful planning, deployment, and sustainable operation of OPSBN as part of the FirstNet NPSBN. Risks are numbered for ease of reference and are in no particular order. Identifying a risk does not constitute a criticism.

[70] See Section 6.1 Applications and Use for definition of "mission support" vs. "mission critical."
[71] OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon, p. 31.
[72] State of Oregon, *Business Case Template Appendix v1.6*, Risk and Mitigations, p.11.
[73] *Ibid*.

Table 12-1 OPSBN Planning, Deployment, and Operations Risks and Potential Mitigations

No.	Risk	Potential Mitigation
	Business or Organizational Risks	
1.	As a rural state with low population density, Oregon may not receive the attention that other states may when vying for the limited implementation grants for initial consultation and coverage needs in the subsequent deployment.	Remain active at the federal level during FirstNet launch and participate in planning activities by key agencies such as the FCC, DHS, and NTIA. Work on a regional basis to create a larger, more visible constituent base, such as with Washington state, Idaho, and Utah to represent the Northwest. Or, via the Western Governors Association (WGA) or other affinity group, such as FEMA or DHS RPS Region 10, which includes Oregon, Washington, Idaho, and Alaska. Actively identify and support nominations for the FirstNet board that are knowledgeable of the Northwest and Oregon. Volunteer Oregon as the best candidate for a FirstNet "rural state" pilot or other visible, near term activity.
2.	FirstNet deployment may be uneven, favoring metro localities and not sparsely populated areas, exacerbating a stakeholder division of "haves vs. have-nots" between the more rural coastal, southern, central and eastern areas of Oregon and the Willamette River Valley.	In negotiating with FirstNet, especially during the consultation phase, equally emphasize rural and metropolitan needs and alternatives. For example, an alternative for providing coverage in Bend might be leveraging current service offered by the local LTE service provider, rather than an expensive new build by a national carrier. This has been referred to as an "Opt-In plus" scenario. Propose that FirstNet offer service tiers that accommodate rural needs at a lower, more affordable cost. Propose that FirstNet offer arrangements that incorporate existing 3G data service in rural areas unsupported by LTE service providers.
3.	The long, multi-year schedule for FirstNet deployment creates the risk that its technology could be obsolete by the time it is implemented in Oregon. Further, the extended duration increases the likelihood that local public safety users will have already established long term contracts with commercial service carriers, making it unattractive for them to move to a higher (or additional) cost FirstNet service offering relatively few differentiators to their current service.[74]	Enhance the "Opt-In" decision by advocating a "bolt-on" deployment strategy that is synergistic with commercial service providers' implementation strategies to minimize time-to-market for FirstNet service and to get FirstNet applications in the hands of users as soon as possible.

[74] See "The Other Opt-Out" in: Barnett Jr., J.A. (2012, September 24). *What Should FirstNet Do First? State Integration into the National Public Safety Broadband Network*, p. 26. Retrieved from http://potomacinstitute.org/attachments/article/1294/FirstNet%20NPSBN%20Report.pdf

No.	Risk	Potential Mitigation
4.	The later that Oregon is scheduled in the multi-year FirstNet deployment schedule, the less likely that sufficient funding will be available for Oregon's deployment. Further, FirstNet projected timelines may not align with the proposed funding stream from the spectrum auctions.[75]	Although the "first mover" advantage of requesting an early deployment may assure finances and momentum, a later adopter position enables Oregon to benefit from the learning curve of other regions. Therefore, work to position Oregon as a "fast follower" and "rural pilot" to maximize the benefit of learning *and* FirstNet's sufficient funding during execution.
5.	The deployment proposal offered by FirstNet may be perceived by stakeholders as an unfavorable or unsustainable business model for ongoing operations.	Actively identify and engage the participation of secondary users such as "second responders" and "public services" including public utilities to increase the user population base and so reduce overall cost per user to a sustainable level.
6.	The federal government may implement a FirstNet billing solution that makes the State of Oregon responsible for collecting service fees, increasing operations costs and damaging the state's relations with local jurisdictions.	During the consultation phase, recommend to FirstNet that service be billed directly to the end user organization.
7.	When the time for commitment arrives, Oregon may be unable to act promptly enough to commit resources and speak with a single voice to the NTIA FirstNet via a single POC as required by FirstNet legislation.	Establish a Public Safety Broadband office quickly to position Oregon for prompt response. Leverage the existing Oregon Broadband Advisory Council (OBAC) and SIEC structures for engaging and obtaining consensus of state and local stakeholders.
8.	Elections at the federal or state levels may introduce government officials unfavorable to FirstNet implementation, halting progress.	Maintain the collaboration and grassroots support at the local public safety stakeholder level as was established by the waiver participants, using it to educate and influence new lawmakers regarding the continued importance of NPSBN.
	Technical Risks	
9.	Minimal deployment funding may be allocated by FirstNet for Oregon, resulting in insufficient coverage after initial deployment.	Work closely with FirstNet to develop financially viable commercial roaming agreements with carriers offering SLAs suitable for public safety mission support activities. Collaborate with other state legislated and local efforts that have been funded from other sources to create a larger combined coverage.
10.	The nationwide design template offered by FirstNet may not reflect the needs of Oregon.	Join in requirements development and design efforts at the national level, bringing Oregon's needs to the table early in the game. Perform an integral role during design review. *Actively participate* in the overall process.
11.	The federal top-down, one-size-fits-all approach of FirstNet may limit rural states' choice of service mix and features as well as cost tiers. Local users may have little control or influence in the process. The rates established may not be equitable across states, creating a situation similar to being	Maintain active participation with NPSTC and other federal entities engaged in FirstNet design to voice this concern and guide requirements development. Aggressively assert the needs of Oregon during the consultation phase.

[75] *Ibid.*, pp. 36 - 39.

No.	Risk	Potential Mitigation
	a gas tax "donor" state wherein operation fees collected exceed the value of services returned.	Establish a strong and communicative relationship with local FirstNet board members and regional representatives. Engage a lobbyist to act on behalf of the state's interests.
12.	The public safety community may add such highly specialized equipment requirements and unique conditions to NPSBN that it could become too costly to deploy and prohibitive to upgrade. Restated, there may be the danger of the public safety community creating an "LMR 2.0" exhibiting all the drawbacks of existing proprietary LMR systems and none of the advantages of scale offered by using the same technology as commercial networks.	Maintain active participation with NPSTC to voice this concern and guide requirements development. Appropriately comment on the draft Statement of Requirements (SoR) under development. Inject a "younger" voice and experience into conversations regarding these topics. The current generation has grown up using mobile devices, is comfortable with the technology, and can offer new use cases for public safety based on personal experience.

Since NPSBN is in the very beginning planning stages, many other risks will be identified as plans become more detailed and additional information is released regarding FirstNet. These risks will be added to the table in future releases, reflecting the spirit of the plan as a "living" document.

As more becomes known regarding the risks themselves, risk management processes will be used to estimate the probability and quantitative or qualitative impact of individual risks, pre- and post-mitigation, creating a "risk register." Using this information, risks will be prioritized and ranked, and decisions will be made regarding which mitigations will be executed and when it is more cost effective to leave risks below a specified threshold un-mitigated.

Impacts and mitigation activities documented within the register will be used as input to program planning and scheduling. During execution, the information can also be used to designate trigger points for actions or program reviews. These are points at which the cost or scope changes to the extent where commitment to the program needs to be revisited. Formal documentation of the change and approval may be required before continuing.

Throughout program deployment, the risk register will be periodically revisited and updated, closing risks that are no longer relevant, updating impacts, and entering new risks and mitigations as they are identified.

13. RECOMMENDATIONS AND NEXT STEPS

This section describes near and long term recommendations to ensure success with Oregon's PSBN program based on state level planning performed in prior years, recent federal developments with FirstNet, and past experiences with statewide technology deployments such as the SRP. For the purposes of this section, near term is assumed to be within the next 6-12

months and includes recommendations that are expected to be more tactical and schedule-driven. Long term is considered to be 12 months and beyond, with the corresponding recommendations more strategic in nature.

- **Recommendations**

Table 13-1 and Table 13-2 display near and long term recommendations, respectively, and are designed as starting worksheets for future prioritization, assignment, action, and tracking. The rationale for each recommendation is included for context and to aid in prioritization.

These recommendations were developed from the information in prior sections of this planning document, including network architecture and performance, program risks and mitigations, and the anticipated timeline of FirstNet events and responsibilities. Most importantly, they support the potential uses for this network in improving public safety capability and response. Significant themes include:

Near Term

- Actively engage at the federal level to ensure Oregon's interests and concerns are considered and addressed, especially during the critical early stages of developing the FirstNet organization and the technical requirements for the NPSBN.
- Prepare for responding to NTIA's State and Local Implementation Grant Program. The RFP is expected to be released in first quarter of 2013.
- Prepare Oregon to respond with one voice to FirstNet consultation requests, building support and consensus among stakeholders.

Long Term

- Formally establish the OPSBO to focus and execute state efforts.
- Propose solutions to FirstNet that address Oregon's service requirements and rural coverage needs.

Table 13-1 OPSBN Recommendations – Near Term (6-12 mo.)

No.	Near Term Recommendation	Rationale	Responsible Organization	Status Date	Status
1.	Propose a position of opt-in for Oregon, provided close collaboration and interactions are maintained between the FirstNet organization and Oregon stakeholders.	Taking a proactive stance based on an engagement model given available information.		7/24/12	The recommendation of an Opt-In position has been presented to the Governor's office.
2.	Remain active at the federal level during FirstNet launch and participate in planning activities by key agencies such as the FCC, DHS, and NTIA.	As a rural state with relatively low population density, Oregon may not receive the attention that other states may when vying for the limited funds for initial consultation and subsequent deployment.		8/6/12	Aug 2012: Sent representative to NPSTC BBWG SoR meeting in Boulder, CO. Jun 2012: Sent representatives to the National Governors Association Public Safety Broadband Conference. Ongoing since 2010: Participate in the NCSWIC Broadband Working Group. Ongoing since 2010: Active in sending state representatives to the Public Safety Communications Research Center.
3.	Recommend to FirstNet that deployment funding be allocated using consideration of coverage area and terrain requirements to service a state rather than solely based on census population data. Volunteer Oregon as the best candidate for a FirstNet "rural state" pilot or other visible, near term activity.	As a rural state with relatively low population density, Oregon may not receive the attention that other states may when vying for the limited funds for initial consultation and subsequent deployment.		6/8/12	Provided feedback in RFI response to NTIA that Oregon does not support population as a main criterion for granting funds.

No.	Near Term Recommendation	Rationale	Responsible Organization	Status Date	Status
4.	Oregon should request a waiver of the 20% match requirement for FirstNet implementation planning grant funding.	Oregon's challenged economy and prior in-kind participation in waiver activity. Expecting grant to be released in 1Q2013, therefore a near term decision.		6/8/12	Provided feedback supporting waiver of 20% match in RFI response to NTIA.
5.	Actively identify and support nominations for the FirstNet board that are favorable and knowledgeable to the Northwest and Oregon. Establish a strong and communicative relationship with local FirstNet board members and regional representatives.	As a rural state with relatively low population density, Oregon may not receive the attention that other states may when vying for the limited funds for initial consultation and subsequent deployment.		8/20/12	Jeff Johnson named to the FirstNet board.
6.	Although the "first mover" advantage of an early deployment may assure finances and momentum for Oregon, a later adopter position enables the state to benefit from the learning curve of others. To maximize the benefit of learning *and* sufficient funding during execution position Oregon as a "fast follower" and "rural pilot."	The later that Oregon is scheduled in the multi-year FirstNet deployment schedule, the less likely it is to receive sufficient funding for its deployment.			
7.	Leverage the existing Oregon Broadband Advisory Council (OBAC) and SIEC structures for engaging and obtaining consensus of state and local stakeholders when performing planning activities and responding to FirstNet requests.	When the time for commitment arrives, Oregon may be unable to act promptly enough to commit resources and speak with a single voice to the NTIA FirstNet via a single POC as required by FirstNet legislation.			
8.	Identify sources, such as consultants and partners, for LTE broadband Subject Matter Experts (SMEs) to assist in the consultative phase.	NTIA's implementation grant requirements for states include leveraging and incorporating broadband technology experts in consultations with FirstNet.			

No.	Near Term Recommendation	Rationale	Responsible Organization	Status Date	Status
9.	Begin identifying approaches for collecting input and feedback from local and tribal stakeholders.	NTIA implementation grant requirements will include a plan for collecting data and representing the needs of local and tribal jurisdictions.			
10.	Outline strategies for education and outreach to stakeholders, including local and tribal constituents.	NTIA implementation grant requirements include a process for education and outreach to local, tribal, public safety, and other users.			
11.	Begin to identify major sources of existing infrastructure in preparation for developing and negotiating standard MOUs with owners.	NTIA implementation grant requirements include that standard MOUs be executed to facilitate use of existing assets.			
12.	Actively participate in system requirements development and design efforts at the national level, bringing Oregon's needs to the table early.	The nationwide design template offered by FirstNet may not reflect the needs of Oregon.		8/6/12	Sent representative to NPSTC BBWG SoR meeting in Boulder, CO.
13.	Maintain active participation with NPSTC and other federal entities engaged in NPSBN design to voice the concern that the federal top-down, one-size-fits-all approach of FirstNet may limit rural states' choice of service mix, features, cost tiers, or other aspects.	Local users may have little control or influence in the process. The rates established may not be equitable across states, creating a situation similar to being a gas tax "donor" state.			
14.	Appropriately comment on the draft Statement of Requirements (SoR) under development.	The public safety community may add such highly specialized equipment requirements and unique conditions to PSBN that it could become too costly to deploy and prohibitive to upgrade.			

No.	Near Term Recommendation	Rationale	Responsible Organization	Status Date	Status
15.	Inject "younger" voices, viewpoints, and experience into technical discussions. The current generation has grown up using mobile devices, is comfortable with the technology, and can offer new use cases for public safety from a perspective not overly influenced by LMR.	The public safety community is dominated by a generation so accustomed to LMR and its unique equipment that adaptation of existing commercial technology and more cost effective solutions may be overlooked or discarded, yielding a system that could become too costly to deploy and prohibitive to upgrade.			
16.	Work on a regional basis to create a larger, more visible constituent base, such as with Washington state to represent the Northwest or via the Western Governors Association (WGA).	As a rural state with relatively low population density, Oregon may not receive the attention that other states may when vying for the limited funds for initial consultation and subsequent deployment.		7/24/12	The Washington SIEC group has invited Oregon to jointly participate in strategic planning.
17.	Maintain the collaboration and grassroots support at the local public safety stakeholder level as was established by the waiver participants, using it to educate and influence new lawmakers regarding the continued importance of NPSBN.	Elections at the federal or state levels may introduce government officials unfavorable to FirstNet implementation, halting progress.		7/24/12	The DHS OEC is developing a new charter that is relevant to the new FirstNet environment.

Table 13-2 OPSBN Recommendations – Long Term (12 mo.+)

No.	Long Term Recommendation	Rationale	Responsible Organization	Status Date	Status
1.	In negotiating with FirstNet during the consultation phase, equally emphasize rural needs and alternatives when considering options for coverage. For example, for the City of Bend, consider leveraging current service offered by the local commercial LTE service provider, rather than an expensive new build by a national carrier. This has been referred to as an "Opt-In plus" scenario.	FirstNet deployment may be uneven, favoring metro vs. sparsely populated localities, creating a "haves vs. have nots" split between the more rural eastern Oregon and the Portland Metro area of the state.			
2.	Actively identify and engage the participation of secondary users such as "second responders" and "public services" including utilities, increasing the user population base to reduce subscription cost per user to a sustainable level.	The deployment proposal offered by FirstNet may be perceived by stakeholders as an unfavorable or unsustainable business model for ongoing operations when compared to commercial non-"public safety grade" mission support options currently in use.			
3.	During the consultation phase, take the position that OPSBO does not wish to act as the billing aggregator and that FirstNet service should be billed directly to the end user organization, including by state agency.	The federal government may propose a FirstNet billing scenario that makes the State of Oregon responsible for subscription tracking and collecting service fees without compensation. This would force the state to "tax" its users to support the staff needed to perform these tasks; increasing operations costs and damaging the state's relations with local jurisdictions.			

No.	Long Term Recommendation	Rationale	Responsible Organization	Status Date	Status
4.	Establish a Public Safety Broadband office within ODOT to act as POC for Oregon, for example within Major Projects Branch. The office will act as a focal point for statewide multi-agency collaboration.	When the time for commitment arrives, Oregon may be unable to act promptly enough to commit resources and speak with a single voice to the NTIA FirstNet via a single POC as required by FirstNet legislation.		7/24/12	Feb 2012: Established interim office within ODOT Major Projects Branch with COPS grant funding for planning. June 2010: ODOT Major Projects Branch acting informally as Public Safety Broadband Office in BTOP grant response.
5.	Work closely with FirstNet to develop financially viable commercial roaming agreements with carriers offering Service Level Agreements (SLAs) suitable for public safety mission support activities.	Minimal deployment funding may be received for Oregon from FirstNet, resulting in insufficient coverage after initial deployment.			
6.	Propose FirstNet offer service tiers that accommodate rural needs at a lower, more affordable cost. Encourage FirstNet to utilize lessons learned from rural electrification program, rural telephone service, or similar programs.	The federal top-down, one-size-fits-all approach of FirstNet may limit rural states' choice of service mix and features as well as cost competitive service tiers. Local users may have little control or influence in the process.			
7.	Under FirstNet offer arrangements that incorporate existing 3G data service in rural areas unsupported by 4G LTE service providers.	FirstNet deployment may be uneven, with deployment timing favoring metro vs. sparsely populated localities. Incorporating available 3G data services into the FirstNet service package would bring rural users into the system sooner, increasing the user population.			

No.	Long Term Recommendation	Rationale	Responsible Organization	Status Date	Status
8.	Advocate a deployment strategy that is synergistic with commercial service providers' implementation strategies (e.g., "bolt-on") to minimize time-to-market for FirstNet service and to get FirstNet applications in the hands of more users sooner.	The long, multi-year schedule for FirstNet deployment may create the risk that its technology could be obsolete by the time it is implemented in Oregon. Further, the extended duration increases the likelihood that local public safety users will have already established long term contracts with carriers for commercial service. This may make moving to a higher cost FirstNet service, which offers relatively few differentiators to their current service, unattractive or unfeasible.			
9.	Engage a lobbyist to act on behalf of the state's interests or add FirstNet to the responsibilities of current ODOT lobbyist.	The federal top-down, one-size-fits-all approach of FirstNet may limit rural states' choice of service mix and features as well as cost tiers. Local users may have little control or influence in the process. The rates established may not be equitable across states, creating a situation similar to being a gas tax "donor" state.			

- **Timeline and Next Steps**

The timing for state level actions depends on actions at the national level. Figure 13-1 and Figure 13-2 present a graphical timeline of past and planned events and activities at the Oregon and national level.

As a next step, in the first quarter of 2013 FirstNet will release an implementation planning grant RFP for monies to assist states in planning and preparing for the NPSBN. This will be under a newly formed State and Local Implementation Grant Program (SLIGP). The grant application will likely ask Oregon to:

- Certify in its application that the state has designated a single office or governmental body to serve as the coordinator of grant funds.
- Demonstrate how Oregon plans to collect input from local and tribal jurisdictions to ensure their needs are represented in the consultation process.
- Discuss how existing governance structures will be leveraged and expanded to include experts in broadband technology for consultation with FirstNet.

NTIA expects Oregon's use of these grant funds during the consultative phase to result in:

- A new or expanded governance structure in place to consult with FirstNet.
- Procedures implemented to ensure local and tribal consultation.
- A process for education and outreach to local, tribal, public safety, and other users.
- Public safety users identified.
- Executed standard Memorandums of Understanding (MOUs) to facilitate the use of existing infrastructure, or the legal barriers to such identified.
- Staffing plans to prepare for FirstNet data collection efforts. The plans are to include local and tribal representatives.

NTIA says it may also request Oregon to develop a comprehensive broadband plan similar to the Statewide Communications Interoperability Plan (SCIP). However, NTIA has advised stakeholders to wait for additional guidance before starting this plan.[76]

Looking ahead in the timeline, in the first quarter of 2015 FirstNet is expected to begin informing states of the deployment plan and funding level. 2015 is also expected to see the initial funding from spectrum auctions become available for network construction. The auction process is expected to continue through 2022.

[76] NTIA (2012, August 24). *NTIA Releases Requirements for State and Local Implementation Grant*, p 1.

- **Engage Stakeholders**

To prepare for these events, it is critical to engage Oregon's many public safety stakeholders.[77] The NGA notes that state-level stakeholders include chief information officers (CIOs), chief technology officers (CTOs), chief information security officers (CISOs), homeland security advisors (HSAs), emergency managers (EMs), state police, statewide interoperability coordinator (SWIC), state fire and EMS officials, public utilities commissioner, state budget officers, and state health officials.[78]

The local public safety community, local governments and regions, tribal nations, as well as the private sector and utilities should also be engaged to ensure unique requirements are met and special needs addressed. A coordinated effort by fully engaged stakeholders will position Oregon for successful implementation of OPSBN.

[77] See Sections 7 and 8 for more information regarding OPSBN stakeholders and input processes.
[78] National Governors Association (2012, June 28). Preparing for Public Safety Broadband. *White Paper*, p. 6-8. Retrieved from http://www.nga.org/files/live/sites/NGA/files/pdf/1206PREPAREBROADBANDPAPER.PDF

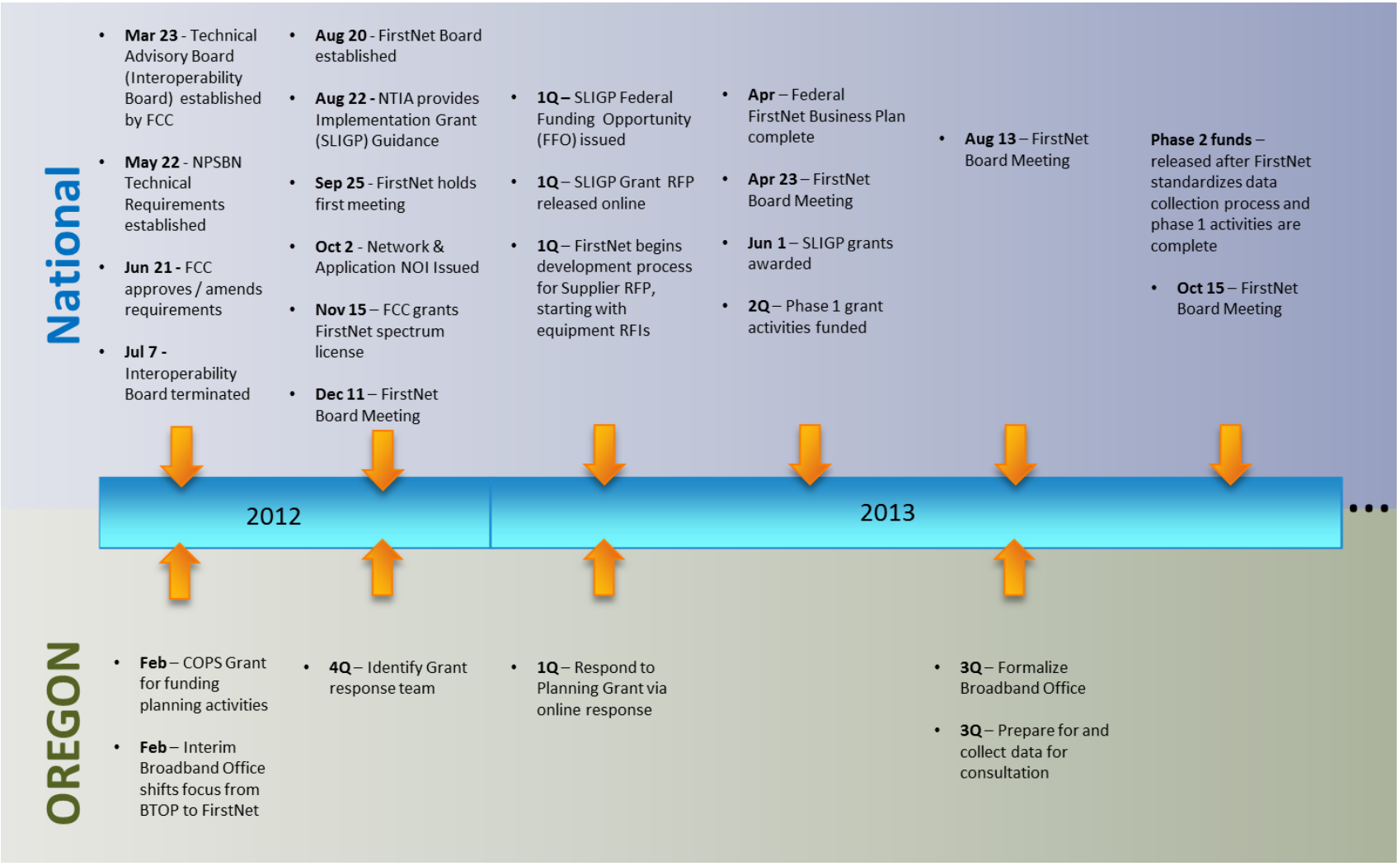


Figure 13-1 Public Safety Broadband Communications National and Oregon Timeline 2012 – 2013

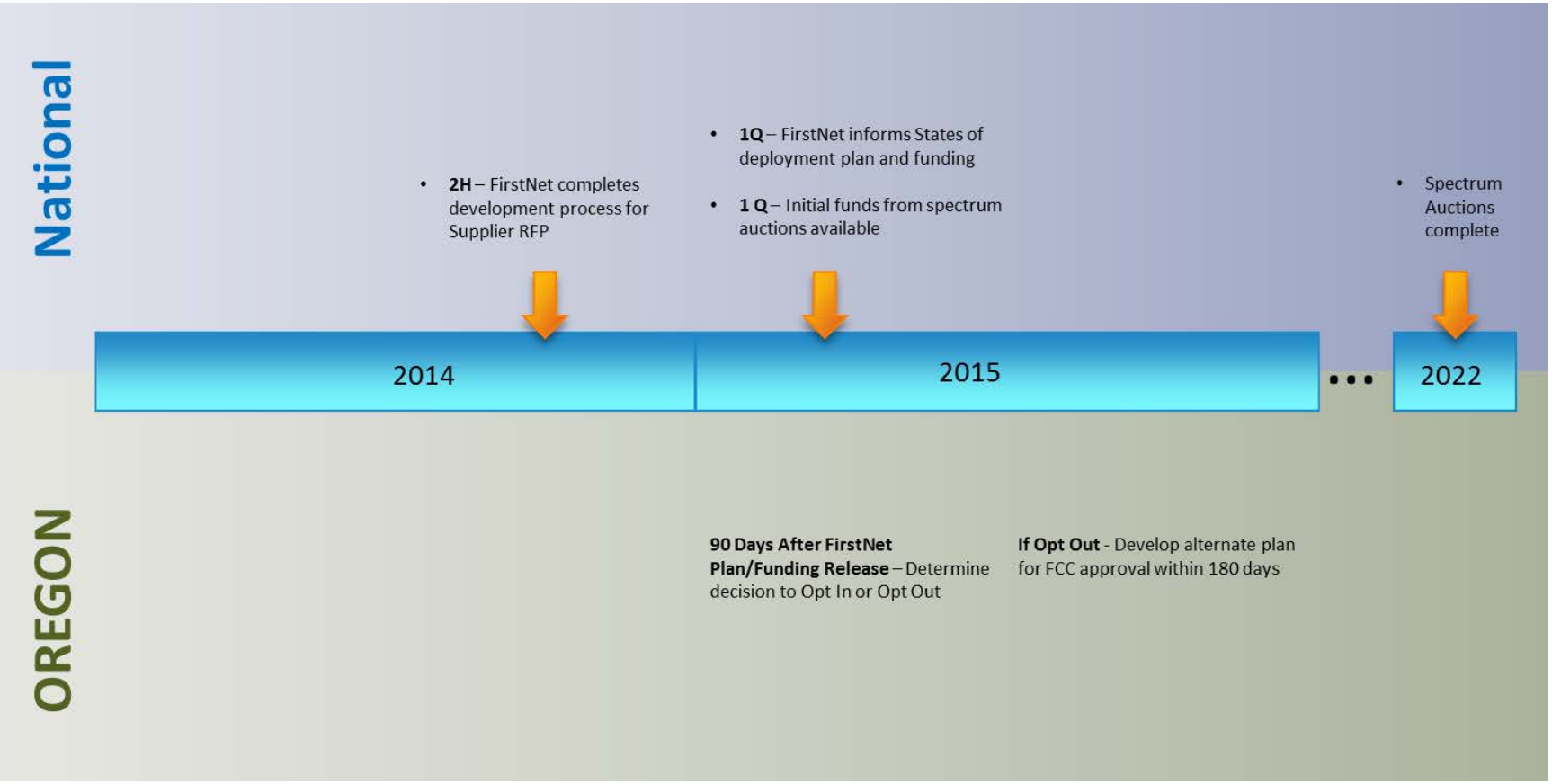


Figure 13-2 Public Safety Broadband Communications National and Oregon Timeline 2014 – 2015 through 2022

14. CONCLUSION

Broadband data applications enable exciting new possibilities for improving the operations and effectiveness of public safety activities in life changing – and lifesaving – ways. However, the road to convergence is a long one and will take many years. It will be extremely important to manage expectations as well as plan during these early implementation phases.

- **Manage Expectations**

The PSBN is an entirely new approach to public safety communications. Further, public safety users have widely differing expectations of what LTE can deliver. Users with a long history of narrow band LMR voice communications, with its extended range and high reliability, may either expect the same of the PSBN or dismiss it as not worthy of serious consideration for public safety use. Others may embrace LTE technology, seeing it as a complete replacement for mission critical voice, for which LMR has been public safety's "gold standard." Some public safety administrators are already having difficulty receiving funding approval for LMR upgrades because local government officials believe that LTE is completely replacing LMR near term.

To avoid unrealistic expectations and disappointment, it is important to manage the expectations of the public safety community by socializing these key messages:

- LTE is not a replacement for LMR technology today.
- LMR will continue to provide mission critical voice communications for a long time.
- LTE introduces new capabilities to assist the first responder. It is a supplementary technology that offers the first responder new data and video services, providing additional and timely information.
- PTT voice on LTE has not yet been standardized. However, there are proprietary solutions which can be used today. In the future, private network users will communicate with PTT voice users on commercial networks, and also connect to traditional LMR systems using standardized applications.
- LTE is a data transport mechanism. Its true power and value will be realized only after useful and interoperable applications are in the hands of users.
- To makes applications interoperable, users will need to coordinate with one another to interconnect their private networks using middleware or by implementing developing standards.

- **Plan for the Future**

With appropriate expectations set, the OEC offers these keys to planning an effective network convergence:[79]

- Maintain adequate funding for LMR and the NPSBN.
- Develop appropriate partnerships at all levels.
- Design effective policy and governance structures.
- Build consensus as required to make OPSBN effective.

To that end, this document is intended to be a hands-on, "living" planning tool to provide direction and record progress towards successful PSBN implementation in Oregon.

[79] OEC (2012, June 22). *Realizing the Future of Public Safety Communications – DRAFT*.

15. REFERENCES

3rd Generation Partnership Project: www.3gpp.org

Alcatel-Lucent (2012, March 2). *Response to RFI-EI 00060 Oregon Public Safety Long Term Evolution Broadband Spectrum Network Proof-of-Concept Pilot (LTE PSBN Pilot).*

Alcatel-Lucent (2010). *Ultimate Wireless Broadband Solution for Public Safety*.

Alcatel-Lucent (2010). *A How-To Guide for LTE in Public Safety*.

Barnett Jr., J.A. (2012, September 24). *What Should FirstNet Do First? State Integration into the National Public Safety Broadband Network*. www.potomacinstitute.org/attachments/article/1294/FirstNet%20NPSBN%20Report.pdf

Boubez, Dr. Toufic, InterAct Public Safety (2012, October 7). *Cloud Computing and Public Safety Services*. www.interact911.com/wp-content/uploads/overview/cloud-computing-public-safety.pdf

Department of Commerce (2012, August 20). *FirstNet Board Members Appointed by Acting U.S. Commerce Secretary Rebecca Blank: Member Statements.* http://www.commerce.gov/news/press-releases/2012/08/20/firstnet-board-members-appointed-acting-us-commerce-secretary-rebecca

DHHS, Public Health Emergency, Emergency Support Functions. http://www.phe.gov/preparedness/support/esf8/pages/default.aspx

DHS (2012). *Public Safety Broadband: Fulfilling a 9/11 Commission Recommendation*. www.dhs.gov/files/programs/public-safety-broadband.shtm

DHS Command, Control and Interoperability Division Basic/Futures Research program video to illustrate broadband's potential within emergency management. www.precisioninformation.org

Farrill, F. Craig. (2012, September 25). First Responders Network Authority Presentation to the Board, *FirstNet Nationwide Network (FNN) Proposal*. http://www.ntia.doc.gov/files/ntia/publications/firstnet_fnn_presentation_09-25-2012_final.pdf

FCC (2012, July 30). *Order FCC-12-85A1*.

FCC (2012, March 16). *Order DA 12-423*.

FCC (2010, December 10). *PS Docket No. 06-229, DA 10-2342*.

GPO (2004, July 22). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Retrieved from www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf

Harris Corporation (2012, March 2). *Response to the State of Oregon's Request for Information and Expression of Interest (RFI-EI) for Public Safety Long Term Evolution Broadband Spectrum Network Proof-of-Concept Pilot (LTE PSBN Pilot).*

Hatch, L. (2012, June 5). [E-mail]. *Frequently Asked Questions*. (Texas)

Lawson, S. (2012, June 15). US pushes forward on public-safety LTE network. *Network World*. www.networkworld.com/news/2012/061612-us-pushes-forward-on-public-safety-260253.html

Lum, D. (2011, July 12). "Sizing Up PMR Devices," *Radio Resource Magazine*. www.mccmag.com/onlyonline.cfm?OnlyOnlineID=255

McEwen, H. (2012, March 15). *Nationwide Public Safety Broadband Network*. NTIA Communications & Technology Committee presentation.

Motorola Solutions, Inc. (2012, March 2). Executive Summary. *Response to the State of Oregon's Request for Information and Expression of Interest (RFI-EI) for Public Safety Long Term Evolution Broadband Spectrum Network Proof-of-Concept Pilot (LTE PSBN Pilot).*

National Governors Association (2012, June 28). Preparing for Public Safety Broadband. *White Paper*. www.nga.org/files/live/sites/NGA/files/pdf/1206PREPAREBROADBANDPAPER.PDF

NECP Goal 2 Overview. www.siec.wa.gov/success/files/NECP_Goal_2_Overview.pdf

Network World (2009, June 10). *LTE devices must support IPv6, says Verizon.* http://www.networkworld.com/news/2009/061009-verizon-lte-ipv6.html

Noel, S. (2011). *Oregon LTE at a Glance*. Internal planning document.

NPSTC (2012). "High Level Statement of Requirements for FirstNet Consideration." *NPSTC Public Safety Communications Report*.

NTIA (2012, November 16). FirstNet Praises FCC for Granting Spectrum License. http://www.ntia.doc.gov/press-release/2012/firstnet-praises-fcc-granting-spectrum-license

NTIA (2012, September 25). FirstNet Board Actions 9/25/12. http://www.ntia.doc.gov/other-publication/2012/firstnet-board-actions-09252012

NTIA (2012, August 24). NTIA Releases Requirements for State and Local Implementation Grant.

NTIA (2012, August 22). *APCO Session: Preparation for the State and Local Grant Program*.

NTIA (2012, August 21). Development of Programmatic Requirements for the State and Local Implementation Grant Program to Assist in Planning for the Nationwide Public Safety Broadband Network (NPSBN). http://www.ntia.doc.gov/files/ntia/publications/fr_sligp_08212012.pdf

ODOT (2012, December). "E-Citing things are happening with law enforcement data." *Inside ODOT*.

ODOT (2012, December). *Oregon's FirstNet (Broadband) Implementation*. Oregon Department of Transportation State Radio Project Draft Discussion Paper.

ODOT/MPB (2012, June 8). OPSBN Business Plan Kickoff Working Session.

ODOT (2012, December). *Voice Radio Communications*. Oregon Department of Transportation State Radio Project Draft Discussion Paper.

OEC (2012, June 22). *Realizing the Future of Public Safety Communications – DRAFT*.

OEC (2012, June 21). Oregon Broadband Survey Workshop, Portland, Oregon.

OEC (2012, June). *Review of Public Safety Wireless Data Usage, State of Oregon, Portland Area*.

OEC (2012, May). *NECP Goal 2 Analysis with Workshop Findings & Recommendations*.

OEC (2012, April 17). *Statewide Communication Interoperability Plan (SCIP) Implementation Workshop*, Oregon.

OEC (2011, November). *Interoperability Planning for Wireless Broadband*. www.publicsafetytools.info/oec_guidance/docs/Interoperability_Planning_Wireless_Broadband_Web_111711.pdf

OEC (2011, November). *Public Safety Communications Evolution*. www.publicsafetytools.info/oec_guidance/docs/Public_Safety_Communications_Evolution_Brochure.pdf

Public Law 112-96, "Middle Class Tax Relief and Job Creation Act of 2012." FirstNet is found in Title VI of PL112-96, entitled "Public Safety Communications and Electromagnetic Spectrum Auctions." www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf

Roberts, M. R., (2012, May 1). Fire's Case for Broadband. *Urgent Communications*. www.urgentcomm.com/networks_and_systems/mag/fire-ems-broadband-needs-201205/index.html

SAIC (2012, May 2). *Numbering Scheme Document for Public Safety Broadband Network (PSBN) National Network Identifiers*.

State Interoperability Executive Council, www.oregon.gov/SIEC

State of Oregon, *Business Case Template Appendix v1.6*, Risk and Mitigations.

Svensson, P. (2012, August 3). "AT&T 2G Shutdown To Be Complete In 2017: Get Ready To Upgrade," *Huff Post Tech*. www.huffingtonpost.com/2012/08/03/att-2g-shutdown-2017_n_1739175.html

Technical Advisory Board for First Responder Interoperability (2012, May 22). Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network, *Final Report.*

Verizon (2012, October 11). Policy Blog. *Verizon and IPv6.* policyblog.verizon.com/BlogPost/780/VerizonandIPv6.aspx

Verizon, Total Equipment Coverage. support.verizonwireless.com/clc/features/calling_features/equipment_protection.html

16. ACRONYM LIST

2G	Second Generation
3G	Third Generation
3GPP	Third Generation Partnership Program
4G	Fourth Generation
AMPS	Advanced Mobile Phone System
APCO	Association of Public Safety Communications Officials
APN	Access Point Name
ATIS:INC	Alliance for Telecommunications Industry Solutions: Industry Numbering Committee
AUC	Authentication Center
AVL	Automatic Vehicle Location
BATF	Bureau of Alcohol, Tobacco & Firearms
BB	Broadband
BBWG	Broadband Working Group
BS	Base Station
BSC	Base Station Controller
BTOP	Broadband Technology Opportunities Program
CAD	Computer-Aided Dispatch
CAI	Common Air Interface
Capex	Capital expense
CBP	Customs and Border Protection
CCTV	Closed Circuit Television
CD	Compact Disc
CDPD	Cellular Digital Packet Data
CDMA	Code Division Multiple Access
CDMA2000	Code Division Multiple Access – Third Generation
CIO	Chief Information Officer
CISO	Chief Information Security Officer

COML	Communications Unit Leader
CTO	Chief Technology Officer
dB	Decibel
DAS	Department of Administrative Services
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DOD	Department of Defense
EDGE	Enhanced Data Rates for GSM Evolution
EIDD	Emergency Incident Data Document
EM	Emergency Manager
EMS	Emergency Medical Service
eNodeB	Evolved Node B
EPC	Evolved Packet Core
ERIC	Emergency Response Interoperability Center
ESF	Emergency Support Function
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FFO	Federal Funding Opportunity
FirstNet	First Responder Network Authority
FNN	FirstNet National Network
FY	Fiscal Year
GIS	Geographic Information System
GPO	Government Printing Office
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HSA	Homeland Security Advisor
HSS	Home Subscriber Service
ID	Identification
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPTV	Internet Protocol Television
IT	Information Technology
kbps	Kilobits per Second
LCOG	Lane Council of Governments

LMR	Land Mobile Radio
LTE	Long Term Evolution
M2M	Machine-to-machine
MAC	Media Access Controller
MCC	Mobile Country Code
MCS	Mission Critical System
MDT	Mobile Data Terminal
MEID	Mobile Equipment Identifier
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
MNC	Mobile Network Code
MOCN	Multi-Operator Core Network
MOU	Memorandum of Understanding
MPB	Major Projects Branch
MPLS	Multi-Protocol Label Switch
MSIN	Mobile Subscriber Identity Number
mW	Milliwatt
NASEMSO	National Association of State EMS Officers
NCIC	National Crime Information Center
NECP	National Emergency Communications Plan
NENA	National Emergency Number Association
NG 9-1-1	Next Generation 9-1-1
NGA	National Governors Association
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NPSBN	Nationwide Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
NYPD	New York City Police Department
OA&M	Operations, Administration & Maintenance
OAC	Operator Advisory Committee
OBAC	Oregon Broadband Advisory Council
ODOT	Oregon Department of Transportation
OEC	Office of Emergency Communications
OIPP	Office of Innovative Partnerships Program
OMB	Office of Management and Budget
OPSBN	Oregon Public Safety Broadband Network
OPSBO	Oregon Public Safety Broadband Office

OSP	Oregon State Police
OWIN	Oregon Wireless Interoperability Network
P25	Project 25
PCRF	Policy and Charging Rules Function
PCS	Personal Communications Services
PDN	Packet Data Network
PGW	Packet Data Gateway
PLMN	Public Land Mobile Network
POC	Point of Contact
PPD-8	Presidential Policy Directive 8
PS	Public Safety
PSAC	Public Safety Advisory Committee
PSAP	Public Safety Answering Point
PSBL	Public Safety Broadband License
PSBN	Public Safety Broadband Network
PSBB Block	Public Safety Broadband Spectrum
PSCR	Public Safety Communications Research
PSEN	Public Safety Entity Network
PSST	Public Safety Spectrum Trust
PTT	Push-To-Talk
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RFI	Request for Information
RFP	Request for Proposal
RMS	Record Management System
SAA	State Administrative Agency
SCIP	Statewide Communication Interoperability Plan
SGW	Serving Gateway
SIEC	State Interoperability Executive Committee
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SLIGP	State and Local Implementation Grant Program
SME	Subject Matter Expert
SMS	Short Message Service
SOP	Standard Operating Procedure
SoR	Statement of Requirements
SRP	State Radio Project
SWIC	Statewide Interoperability Coordinator/Coordination
T1	T-carrier 1

TDMA	Time Division Multiple Access
TICFOG	Tactical Interoperable Communications Field Operations Guide
TICP	Tactical Interoperable Communications Plan
TTL	Time-to-live
TXT2SMS	Text-to-Short-Message-Service
UASI	Urban Areas Security Initiative
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long Term Evolution
VPN	Virtual Private Network
W	Watt
WCCCA	Washington County Consolidated Communications Agency
WCDMA	Wideband Code Division Multiple Access
WGA	Western Governors Association
WiMAX	Worldwide Interoperability for Microwave Access
WR	Waiver Recipient
XML	Extensible Markup Language

APPENDIX A - INTEGRATING LOCAL AND NATIONAL NETWORKS AND APPLICATIONS

This appendix analyzes the challenges and implications of integrating local networks and applications with the NPSBN. Various integration aspects are analyzed in the areas of network operations, local applications, and network security.

A.1 NETWORK OPERATING CHALLENGES

Deploying a high speed data network is a challenge; operating it is quite another. There are many issues and resulting implications of operating a public safety broadband network that must be addressed during planning stages as well as in network design, engineering, and installation. The following sections raise several important areas for consideration regarding the provisioning and operation of the PSBN.

- **User Management**

An overarching element of the PSBN is the management of users. One important consideration is whether user management will be centralized under FirstNet, with the states sending in requests to add or delete users. Or, whether this should be a state or local agency function, where devices and users are controlled and provisioned at the state or local level, and the information transmitted to FirstNet central databases. Of the two approaches, it is unlikely that federal users of the network, such the DOD, would agree to the hands-off, centralized model. Therefore, a decentralized user management system with some form of local control may be required. This is similar to the "authorized retail agent" model used by commercial cellular providers and could involve the use of certified state or local agencies to perform the function.

- **Commercial Roaming**

Given the limited initial funding, it is generally understood by first responders that the PSBN will likely cover less geographical area than commercial networks for some time. Therefore, to maximize public safety benefit, it is clear that public safety users would need to also rely on commercial coverage, especially during the early stages of network deployment. This arrangement generates some challenges, because:

- Commercial systems do not implement QoS on their networks.
- Commercial networks do not implement preemption. All calls are of equal value from the perspective of a service provider’s business and legal model.
- Commercial networks do not implement user priority under normal operations.
- Commercial networks do implement application priority.

Further, due to the staged build-out of a national system, many rural public safety users may not be equipped to use the NPSBN band for some time and may instead be limited to using the commercial networks for their broadband services. Hence FirstNet, the states, and NPSBN users

who roam onto these networks need to be prepared for the implications of the realities of operating on commercial networks. Suitable operational protocols may need to be devised to mitigate any problems. It is likely that the initial applications that first responders use via the commercial networks will not require a dedicated private network in terms of bandwidth, response time, and availability.

Session and call continuity across these networks will need to be thoroughly tested. Presently, session continuity is provided by certain middleware, which could also help to maintain a secure session across the networks. For example, a commercial network provider representative at the August 2102 APCO conference stated that his company is working on seamless, drop-free roaming of voice calls between these networks. If true, its effectiveness will not be known for a while.

- **Network Reliability**

First responders pride themselves on the ruggedness and physical reliability of their LMR networks. This is achieved through codes of construction and deployment, as exemplified by the Motorola R56 document. For example, these guidelines include requirements for eight hours of battery backup, generator backup with several days of fuel on site, and siting the location of generators to be above flood level and shielded from wind damage.[80] Commercial cellular systems, on the other hand, are typically not designed for more than three hours of battery backup unless a site covers a large area. On a promising note, a commercial provider representative at the same APCO conference did indicate that battery backup periods may be improving for commercial networks. This is due to strong pressure from customers and legislators who are heavily dependent on their cellphones and have a growing need for the higher reliability.

The level of commercial network reliability varies with each provider and is site dependent. Therefore, ensuring the availability of the PSBN could be difficult, especially when infrastructure is collocated with commercial LTE systems or shares common elements. For example, installing extra battery backup may require considerable additional floor space in addition to the PSBN equipment being installed in the equipment shack. This will need to be clarified as part of operational SLAs.

Finally, evaluating renewable or “green” technology, such as solar and small wind technology, may offer alternatives for reducing the need for external and backup electrical power. These new sources, when combined with low power consumption electronics, provide innovative ways to improve overall network reliability.

[80] Motorola (2006). *Standards and Guidelines for Communications Sites*. Also known as R56.

- **Coverage Requirements**

In its public safety broadband requirements, the FCC mandated data speeds of 768 kbps uplink and 256 kbps downlink at the cell edge.[81] However, commercial networks today are built with cell spacing that is not designed to provide this rate of data throughput at all locations. Raising throughput would require LTE cell sites to be spaced closer. Therefore, it may be difficult to leverage commercial tower and backhaul infrastructure, since towers may be farther apart than is required by public safety. The added cost could be considerable to deploy these additional radio sites.

The FirstNet Board has proposed the use of mobile satellite communications for rural coverage. This is an appropriate solution to cover these vast sparsely populated areas. From the point of implementation and cost, there are few mobile satellite network operators in the U.S., and with satellites using different air interfaces. Hence the practical issues of integrating these in a cost effective manner into first responder terminals, inherent data transmission delays, relatively lower data rates, and separate network operations involved are yet to be resolved.

- **Network Security**

A nationwide network such as FirstNet is only as secure as its weakest link. The plethora of local public safety data networks across the nation represents a serious concern as agency networks with varying security levels connect to FirstNet. FirstNet will be a very inviting target, not only for mischief makers, but also for espionage. Infiltrating it could provide information endangering public safety during a crisis. It could also reveal tactics and operational methods which could be damaging in the hands of the infiltrators. Federal agencies using FirstNet could have their data compromised as a result.

Therefore, it's expected that local network administrators will be required to perform security audits and take corrective actions to secure their systems. States can support these local efforts by helping to survey and stress test the existing network security, coordinate the implementation of remedial actions, and finally, to certify to FirstNet that the networks are secure for interconnection to the national network.

States, and FirstNet, will also need to develop security policies regarding information's time of validity and time-to-live (TTL). Policies will be needed to specify whether an agency can forward incident-related information it receives from one agency to another agency. It's widely known that most information carried by the Internet is never deleted and can be recovered by third parties, often without cost. This must not be allowed to happen within FirstNet. Policies concerning information retention and forwarding must take their place among those addressing other privacy and sensitivity concerns.

[81] FCC (2010, December 10). *PS Docket No. 06-229, DA 10-2342*.

- **Access and Use by Other NPSBN Users**

The Act also permits the use of the public safety spectrum by federal and other commercial agencies under the control of FirstNet. This has several implications, including:

- Federal users, in general, may demand authentication and communications security at a higher level than first responders. Further, there is no single federal agency that can speak on behalf of the entire federal government as to what federal requirements should be.
- Specific federal agencies, such as the FBI, CBP, and BATF may require additional access controls into the network.
- The DOD may impose even more stringent requirements on the encryption of packets, access control, and other security aspects.
- The National Guard is based in each state and works closely with that state. Hence, it could be argued that the National Guard's UE numbering should come from the state's allocated pool.
- Similarly, the DOD has bases in Hawaii with operations that are tied most closely to Hawaii, and to a lesser extent, to the mainland. Hence, requests have been made by the State of Hawaii that the DOD bases there should be closely integrated with the state in terms of communications, and not relegated to a separate network.
- To share traffic on the network across this wide diversity of users, first responders may need to accept additional security and authentication.
- A single sign-on protocol is being requested so that users are automatically assigned to the appropriate security level based on what they are doing at a particular time.

Since most concerns relate to user management and the flow of each agency's data via the common EPC, one way to accommodate this diversity of users could be to configure multiple sub-networks, each with its own core. There could be a separate DOD EPC, a Federal EPC, and others. Sensitive agencies like the FBI, CBP, and BATF may request their own EPCs, which they can individually manage according to their security needs. These, together with FirstNet's own EPC, would then be combined into a system of virtual networks sharing the same RAN under the overall control of FirstNet.

An alternative solution is to allow RAN and spectrum sharing while keeping the security sensitive core networks separate, using a concept called Multi-Operator Core Networks (MOCNs). This capability has been built into LTE Release 8 and later. It allows several EPCs to connect directly to a common set of RANs, which then stream all the networks' data packets over the air on the same spectrum. The individual network packets may be identified by different PLMN IDs. Hence terminals will only pick up packets from their authorized networks. The RAN is set up to treat all packets fairly, so that eNodeBs will not be swamped by any one network's traffic.

Commercial users' devices and applications may be provisioned at a lower priority level. Where commercial networks choose to use the PSBN for machine-to-machine (M2M) communications for automated meter reading, for example, these applications could be set to the lowest priority level, leaving public safety traffic relatively unaffected.

- **IPv6 Considerations**

Most local public safety data networks are based on the Internet's main communications protocol, Internet Protocol Version 4 (IPv4). However, IPv4 is reaching the end of its useful life in large scale networks since it is running out of address space, among other issues. LTE uses Internet Protocol version 6 (IPv6), which is the upgrade to IPV4. The DOD and other entities in the federal government have already transitioned, or are in the process of transitioning, to IPv6.

Commercially, Verizon requires that any device connecting to the 700 MHz LTE network "shall support IPv6" and "the device shall be assigned an IPv6 address whenever it attaches to the LTE network." [82] IPv4 support is optional. However, any device supporting IPv4 "shall be able to support simultaneous IPv6 and IPv4 sessions." The latter is often known as dual stacking. Other carriers have similar policies.

Therefore, administrators of local networks which will be connected to an LTE network should begin planning for integration with IPv6. At the start, this would include using dual stacked border gateways for interconnection to the NPSBN. Deploying IPv6 in the local network itself can be a long term proposition. To prepare, network administrators should consider adding requirements for IPv6 support in future procurements of network elements and applications such as CAD systems.

- **NPSBN Statement of Requirements (SoR)**

To begin documenting and addressing the considerations, implications, and challenges mentioned in the preceding sections, the public safety community has been developing a Statement of Requirements (SoR) document to convey its needs to FirstNet.[83]

The following SoR sections are particularly relevant (section numbers may change in later drafts):

- Section 5.3.2 of the SoR recommends the required Security policies.
- Section 5.3.3 recommends Data Sharing policies.
- Section 5.3.4 recommends Public Safety Entity Network (PSEN) policy, especially with regard to access to the NPSBN and for applications to be accessible via the NPSBN.

[82] See http://www.networkworld.com/news/2009/061009-verizon-lte-ipv6.html and http://policyblog.verizon.com/BlogPost/780/VerizonandIPv6.aspx

[83] NTIA NPSTC (2012). "High Level Statement of Requirements for FirstNet Consideration." *NPSTC Public Safety Communications Report*.

- Section 5.3.5 requests that FirstNet provide guidance for policies regarding migration of the applications in the PSENs to the PSBN.
- Section 5.3.6 requests FirstNet to develop interoperability requirements.
- Section 5.3.7 deals with provisioning.

In addition, device management issues also arise to be addressed by FirstNet.

Another important reference is the Technical Interoperability Requirements document that was issued by the congressionally chartered Technical Advisory Board.[84]

It would be incorrect to assume that all these challenges could be solved by FirstNet alone. They also require suitable actions by Oregon, other states, and local agencies to better integrate their networks so that they may connect to FirstNet; not only for operation within the state, but also when interworking between states and localities.

- **FirstNet National Network (FNN)**

On September 25, 2012, the FirstNet Board of Directors during its first meeting presented a conceptual network architecture referred to as the FirstNet National Network (FNN).[85] This emphasized a network-of-networks concept, where any first responder would have access to three or more wireless networks – first, the dedicated private public safety network on frequency Band 14, next, commercial cellular service provider A, then commercial cellular service provider B, and so on, to finally satellite communications as a last resort for remote rural areas. This will require multi-band devices, something that cellular carriers and equipment manufacturers have been hesitant to provide commercially, both due to cost and competition concerns. During the meeting, Sam Ginn, FirstNet Board Chair, stated that he's received pledges of commitment from the major service providers to support multi-band equipment for public safety use.

A.2 Application Integration

Challenges will also arise when integrating and interworking existing local applications with the new nationwide network. The following paragraphs highlight some of the issues to be addressed when migrating applications to the new NPSBN architecture.

- **Applications Integration and Standardization**

Oregon's state and local agencies already operate several data networks. These PDNs, described in Section 6.2, are referred to as PSEN in the SoR. PSENs tend to be agency-specific. Different types of agencies in an area, such as police and fire, often do not share their PSENs. The agency-

[84] Technical Advisory Board for First Responder Interoperability (2012, May 22). *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network.*

[85] Farrill, F. Craig. (2012, September 25). First Responders Network Authority Presentation to the Board, *FirstNet Nationwide Network (FNN) Proposal*. Retrieved from http://www.ntia.doc.gov/files/ntia/publications/firstnet_fnn_presentation_09-25-2012_final.pdf

specific, localized applications that run in these PSENs include services such as PTT voice, application layer authentication, QoS management, CAD, Record Management Systems (RMS), and Public Safety Answering Point (PSAP) call taker systems. Some of these services are not interoperable across agencies. Furthermore, even the same type of agencies, such as police in different cities, each have their unique PDNs and applications. Even common application types, such as license plate readers may be different and not interoperable. They may also use different databases.

Under LTE, the apps in each agency's broadband terminals, such as smartphones, have APNs which correspond to the specific PDNs serving the applications described above. Supporting these unique applications creates challenges because:

- Each agency's terminals would have to be programmed specifically for that agency, with its own applications and APNs.
- Programming devices even in a regional manner within a state could become complex since each terminal will have to be custom programmed to its agency's requirements.
- While later versions of LTE are capable of analyzing the entire UICC ID to determine the agency association of each terminal, it is often more efficient not to evaluate the lower order data bits, but analyze the UICC ID only down to a block level to determine its home agency. This requires that IDs for agencies be clustered together in blocks. Hence, programming would also be most efficient at the block level.
- As discussed in APPENDIX C -, the Network Numbering Authority may issue blocks of IDs to a state for distribution to its agencies. At the state's request, they may be partitioned by agency types. Any finer partitioning could become very problematic, since there is always a concern about "stranded" IDs. This can occur when the limited sets of IDs are issued in large blocks to agencies that may never use them all, leaving large number of agency-specific IDs unused while exhausting the available pool of IDs for the state. Hence, common programming becomes desirable.

FirstNet is expected to standardize a common set of national applications and APNs. However, existing legacy applications need to be integrated as well. Therefore, based on the above, it is advantageous for common agency types, such as law enforcement, to:

- Consolidate their PDNs into a common or a few local PDNs.
- Standardize the applications which run on their common or local PDNs.
- Integrate the databases which are connected to these applications.

Statewide agencies such as the state police may already have a common PDN. It is also possible that state fire and EMS have their own network. However, it is not clear if these could be integrated into a statewide PDN serving all the different types of statewide public safety

agencies. At minimum, there are a manageable number of statewide PDNs that could be operated, provisioned, and managed at the state level.

However, when local PSENs are considered, the problem becomes complex. Discussions with local agencies should begin now to see if networks could be standardized or integrated, perhaps by agency type. For example, since these PSENs are funded locally today, it may be more realistic to consider a local common PDN to serve all the agency types in a city. This reduces the number of APNs required in a city to one, with an applications gateway within that PDN directing the data packets to the appropriate applications server. Who controls the common local PDNs must also be decided. This could prove to be a difficult political as well as operational decision.

- **Applications Interconnection and Middleware**

While common applications across several agencies may be a longer term goal, there are several steps that are being implemented or developed today to facilitate interconnecting applications. These are being driven by the advent of Next Generation 9-1-1 (NG 9-1-1) driven features such as Text-to-Short-Message-Service (TXT2SMS), photo, video, and other multimedia and voice reports of an incident. All of these need to be integrated into a single developing incident report and portions forwarded to the appropriate agencies and responders. The different types of data that may be needed to manage a complex incident today also requires information that comes from different sources. Public safety is recognizing that it could be very useful for key applications to talk to each other to exchange data. Some of this is being accomplished today by commercial middleware such as HipLink®. However, these are custom solutions from these specialized vendors who have, over time, built translation middleware to facilitate interoperation between various applications.

- **Applications Interconnection Standardization using EIDD**

Meanwhile, a joint working group of APCO/NENA is working on a data interchange model for PSAP-to-PSAP communications using Extensible Markup Language (XML). Oregon is represented in this effort. An Emergency Incident Data Document (EIDD) is being developed to transfer the information across systems. This is a National Information Exchange Model (NIEM) conformant approach that will enable application vendors to build systems that can communicate with each other. Oregon should verify that new applications will support the EIDD approach when it is released by the EIDD Working Group. It can also write it into contracts as a required update when preparing to replace key applications.

A.3 Provisioning User Equipment and Services

The SoR, in Section 5.3.7 requires FirstNet to develop the methodology for adding, removing, and provisioning users in the network. This is appropriate, and is in keeping with the model of the commercial cellphone networks. An approach to this could be similar to that of local cellular equipment retailers who are able to add devices, UICC, and appropriate services to the devices using barcode scanners. This could be done at the local agency level. A website for the local

agency to add the required services will also be needed. However, this will most likely be accessible only to the local UE manager, and not to the device end-user. This is in contrast to commercial cellphone networks, where individual customers can add or remove services by creating a login and password and logging into the service provider's provisioning system.

When administrating any device, it is always a challenge to keep track of it at all times, know when it should be disabled, ensure if it is disabled that it is also retrieved, etc. While this is best done at the local level, it is also here that vigilance could be compromised. To reduce this risk, one strategy is to lock the UE to the PSBN in the same manner that commercial networks lock phones to their networks. The one exception to the commercial case is where service providers are required to provide unlock codes to users if they plan to use their phone outside the country; for example, after the contract period is over (usually after one or two years). This is a requirement that should be eliminated for public safety equipment, leaving devices permanently locked to the NPSBN.

Shops that unlock cell phones exist in almost every city. This ability will have to be thwarted in some manner to prevent these terminals from leaving the PSBN. There is anecdotal evidence that even LMR radios are sometimes sent for disposal with encryption keys and other agency specific information still in the memory. The potential for this problem will only increase with the PSBN. Procedures need to be developed to ensure that devices are accounted for and properly deactivated, removed and disposed of, or assigned to a different user, as appropriate.

To start, the State of Oregon can begin planning the process and procedures for provisioning its users. If using a retailer model, it should be determined whether this is done at the agency level or at a larger county or regional level. An authorized agent in each local agency or similar provisioning entity should be designated. The plans can later be modified if FirstNet requirements differ. Ultimately, the State needs to take the lead in ensuring that a common approach is undertaken throughout the state, possibly by using the processes it has developed for itself as a model.

APPENDIX B - USER EQUIPMENT EVOLUTION

Responders to the Oregon PSBN RFI identified a variety of mobile and handset terminals for use in the PSBN. These include tablets, smartphones, and mobile routers that act as local hotspots; e.g., offering an umbrella of Wi-Fi coverage surrounding a vehicle. The following paragraphs highlight important aspects of the rapidly changing LTE user equipment market, including the blurring of categories as they branch out beyond the traditional ruggedized "public safety grade" hardware.

- **Multiband Devices**

The possibility of commercial networks sharing spectrum with public safety in frequency Band 14 would increase the economic attractiveness of the band for commercial vendors. Commercial smartphones which also operate in the PS band under certain network permitted conditions could be sold in large quantities, making them less expensive. Until that happens, the cost of producing a limited number of dual band LTE smartphones to support only public safety could be quite high.

The dual band chipsets necessary to support a commercial band are under development. At the present, external data cards are needed to operate on both the PS and one commercial band. Tri-band chipsets that would cover the two commercial networks and the PS band have not been announced to date. It is not clear if or when they would be available and installed in the smartphones of all the network device suppliers, since there is little financial incentive to add the capability for a phone to operate in a rival network's band.

- **Making Changes in a Standards Environment**

Public Safety devices operating in Band 14 have been proposed to be installed as mobile terminals in vehicles. In an analogous manner to public safety LMR terminals, recent requests have been made to build higher transmit power mobiles for this use. However, unlike LMR, LTE device characteristics are defined by the global 3GPP standards body.[86] This body has not authorized higher power mobiles to date. Nonetheless, this and other public-safety related proposals, such as permitting direct mode operation (or terminal to terminal operation without going through the network, much like talk-around in LMR technology) when off network or deep inside buildings, are now being taken up as study items for possible future inclusion in the standards. Until that is done, any use of higher transmit-power terminals would be non-standard and prohibited by the FCC. Non-standard terminal configurations would also remove the economies of scale inherent in commercial technology and raise the equipment cost considerably. Hence attention needs to be placed on better antenna placement, minimizing power loss in cables and similar aspects, since every dB of cable loss further reduces the relatively

[86] 3rd Generation Partnership Project: www.3gpp.org

small cell sizes of LTE systems by reducing the available transmitter power or by increasing the received signal loss.

- **Commercial Grade vs. Public Safety Grade User Equipment**

PS radio manufacturers have sought to differentiate their products by building "public safety grade" hardened and ruggedized terminals. This raises important issues that are especially relevant when making business decisions regarding their purchase.

Commercial networks have sought to keep their costs low by mass producing low-cost terminals, priced in the hundreds of dollars. They compete on visual appeal, ease of use, features, and functionality. If a smartphone is damaged, it is usually replaced for about $45 deductible by the carrier's insurance plan if a per-monthly insurance fee is paid.[87] Also, most cellphones are replaced every two years as their subsidized contract period expires. Some are even replaced yearly by early technology adopting consumers seeking the latest and greatest device. This is accelerated by the fact that the network itself has sustained an evolutionary pace of upgrade every five to seven years (from 2G to 3G, to 3.5G to 4G, for example). In some countries, 2G service is being turned off in favor of higher capacity later generation networks, rendering their 2G phones useless. In the United States, AT&T announced that it plans to phase out 2G service by the end of 2016.[88]

Public safety land mobile radios could cost thousands of dollars and are expected to perform over a seven to ten year life span. The network over which they operate may be designed for a 15 year lifespan. A public safety LTE network that, by necessity, has to interoperate with commercial networks cannot continue to run older versions of the network. While some of these may be software upgrades, major system upgrades such as the Multiple Input Multiple Output (MIMO) LTE Release 10 revision, that has already been standardized to significantly increase speed and capacity, will require separate new radio equipment and user devices to take advantage of their capabilities.

The industry is struggling to define what constitutes ruggedized public safety grade smartphones. Therefore, smartphone costs continue to change. At the outset, public safety specific mobile terminals will be much more costly than commercial mass market devices simply due to their small production volume. The additional cost of producing more rugged versions of MDTs is also not known. It must be noted that this ruggedness cannot be simply obtained by enclosing a regular device in a tough external case. They conform to higher standards of protection against the ingress of water, dust, damage from shock, heat, etc. As a highly simplified example, consider the difference between an ordinary laptop and a "Toughbook" class of computer. Hence, a major decision that faces the public safety community is whether it will be more cost effective to buy "throw away" commercial grade equipment wherever possible and to specify a

[87] http://support.verizonwireless.com/clc/features/calling_features/equipment_protection.html
[88] Svensson, P. (2012, August 3). "AT&T 2G Shutdown To Be Complete In 2017: Get Ready To Upgrade," *Huff Post Tech*. Retrieved from http://www.huffingtonpost.com/2012/08/03/att-2g-shutdown-2017_n_1739175.html

compromise grade of "robust" (as opposed to "rugged") mobile terminals. These would be built to withstand the mobile (vehicular) environment, yet not cost so much that they could be affordably replaced if they fail in a year or two. They could even be leased from a commercial provider using a contract that includes periodic equipment refresh. If the current LMR market is any indication, several manufacturers who already build less rugged LMR terminals for well under $1,000 could step into the LTE market, increasing competition and further lowering cost for "robust" mobile terminals as well. However, there will continue to be a market for equipment that will not fail in a hostile environment, such as under high ambient temperature conditions. These do not have the option of simple replacement upon failure, since the primary criterion is that they cannot fail while in operational use.

As part of this technology convergence, it is expected that manufacturers could start integrating broadband into their traditional LMR radios, possibly as a plug-in. However, this may also be driven by a lower cost LMR terminal market. Otherwise, merging a 15 year lifespan ruggedized LMR with a two year lifespan smartphone may not make sense unless that module is easily replaceable or upgradeable at low cost.

The differences between public safety and commercial grade equipment are summarized in Table B-1 below.[89]

Table B-1 Comparison of Public Safety LMR and Commercial Grade LTE Equipment

Equipment Characteristic	Public Safety Grade LMR	Public Safety Grade Cell Phones	Commercial Grade Cell Phones
Availability	Today	No	Today
Cost	Portables: $1000s	NA	$100s
Nominal Useful Life	7 Years	NA	1-2 years
Ruggedized	Yes, standards exist	No standards	No. Modest ruggedizing may be obtained by putting them in tougher external cases
Safety in Hazardous environments	Yes, with Intrinsically Safe radios	NA	No
High Power Portables and Mobiles	Available today	None defined	None defined in standards
Encryption	Strong Encryption is an Available Option	NA	Some encryption available by design. End-to-End encryption provided separately.

[89] Note: Includes information from Lum, D. (2011, July 12). "Sizing Up PMR Devices," *Radio Resource Magazine*. Retrieved from http://mccmag.com/onlyonline.cfm?OnlyOnlineID=255

Equipment Characteristic	Public Safety Grade LMR	Public Safety Grade Cell Phones	Commercial Grade Cell Phones
Direct Mode	Yes	NA	Not defined in Standards
Loudspeakers	High powered audio	NA	Low powered audio
Usability with Heavy Gloves	Yes	NA	No
Interoperability	Protocol standardization is far advanced. Multiband radios available at additional cost.	NA	Standardized. Routinely cover multiple bands and protocols.
IP Capability	No	NA	Yes, built in

In summary, evaluating equipment and making broadband UE purchases for public safety requires both a different set of criteria and a different way of thinking about these devices than in the past.

APPENDIX C - PSBN NUMBERING & OPERATIONAL IMPLICATIONS

The association of the device information, the network information, and the subscriber is a key element of provisioning a user device, and has to be performed for every device that is permitted to use the network. In commercial systems, this provisioning process is started at the retail store upon purchase of a cellphone. The same operation needs to be performed in FirstNet, both for user devices and for network equipment.

Driven by the LTE 3GPP standard, a foundational element of the PSBN will be the establishment of a consistent numbering scheme. The PSBN is uniquely identified by its Public Land Mobile Network Identifier (PLMN ID), which was assigned by ATIS:INC (Alliance for Telecommunications Industry Solutions: Industry Numbering Committee). The PSBN PLMN ID is 313-100, and is made up of the Mobile Country Code (MCC) of 313, and the Mobile Network Code (MNC) of 100. Hence all sub-networks of the PSBN would carry the same PLMN ID. This ID is incorporated into several other key System Identifiers which are used to provision the various elements of the individual EPCs and RAN. It would also be used in the programming of SIM cards which are used to identify and personalize the UE associated with the PSBN. The makeup of the PSBN PLMN ID is shown in Figure C-1 and is described in detail in the PSBN numbering document.[90]

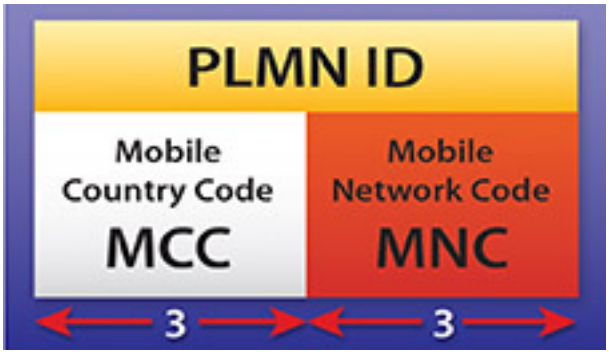


Figure C-1 Public Land Mobile Network Identifier (PLMN ID) = 313-100

- **Mobile Subscriber Identity Number (MSIN)**

Each user device has certain built-in device-specific numbers such as its unique Mobile Equipment Identifier (MEID) and its Media Access Controller (MAC) address. Additionally, every UE is assigned a Mobile Subscriber Identity Number (MSIN) for networking purposes. When the MSIN is joined to the PLMN ID it creates the globally unique IMSI (International Mobile Subscriber Identity) which identifies each device uniquely to all networks. See Figure C-2.

[90] SAIC (2012, May 2). *Numbering Scheme Document for Public Safety Broadband Network (PSBN) National Network Identifiers*. Prepared for Public Safety Spectrum Trust Operator Advisory Committee.

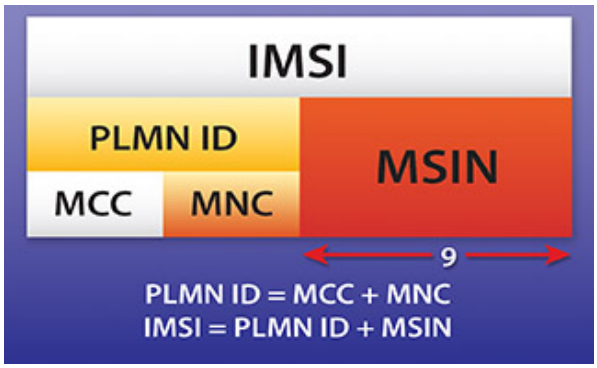


Figure C-2 International Mobile Subscriber Identity

Contiguous allocations of the MSIN are given to groups of recipients for more efficient handling by the network by the network numbering authority. In the present network numbering scheme MSINs are issued in blocks of 50,000. Hence, the numbering authority could give initial allocations to 50,000 to each agency with reserved buffers on both sides. More blocks can be allocated as these are used up. This would be performed separately with each agency or small group of agencies and not given as a large block to the state, in order to maximize the limited resources of IDs.

A unique IMSI is assigned to each UE within a network through a SIM card. When the card is inserted into the device, the device is identifiable on its home and visited networks. Note that even if firefighters travel from Oregon to another state to provide assistance, they will most likely still be in the same network, perhaps operating in a different sub network of the larger NPSBN, unless they roam onto a commercial network in the visited area. The SIM card also carries additional information to permit communication on the network. Hence an operational part of provisioning user equipment is to scan the device-specific information such as its MEID and MAC address into the subscriber information database and then scan the information regarding the SIM Card that will be inserted into that device. Several elements of the subscriber and device information reside in the Home Subscriber Server (HSS).

- **Access Point Names (APN)**

PSBN devices are essentially IP terminals. Hence their value to public safety users is based on the applications that are run on them. In the commercial LTE network, these apps are small segments of code (or thin clients) that are linked to software applications hosted in servers in the jurisdiction's IT Packet Data Network (PDN), and are connected via secure application gateways within those networks. The application gateways are identified by their Access Point Name (APN), enabling application servers to be found by the network when a connection is requested by an app on a user's device.

However, public safety agency IT networks and the applications that are run on these networks may be different or incompatible, even within the same agency types. Hence the database query on a license plate or a driver's license performed by the county sheriff and the police department in a city in that county could be linked to different networks, databases, and back-end

applications.[91] This can cause difficulties, since the number of such APNs that can be supported by the UE at any given time is limited in present LTE implementations. The standard operating procedures in these agencies could also be very different, and this may be reflected in their applications. Hence, unless care is taken, each agency's UE would need to be loaded with applications that are specific to it with different APNs.

It is assumed that FirstNet will define national APNs that will be standardized across the nationwide network. These may include APNs for the IP Multimedia Subsystem (IMS), future mission critical voice services (MCS), and others. Today, a handful of APNs are similarly defined in commercial networks, for example, for IMS.

The FCC, in its order DA12-423, chartered Science Applications International Corporation (SAIC) as the Public Safety Broadband Numbering Administrator.[92] The Administrator has worked with the early adopters, as represented in the Operators Advisory Committee (OAC), to define a **network ID numbering scheme** including a **naming convention** for local APNs. However, local APNs, in themselves, have not been standardized. Also, as indicated before, APNs point to specific PDNs to which they are bound. This could be a potential problem for first responders who have come from a different part of the country to help in a major disaster, for example, since their local APNs may not be relevant in the visited area or connect to the visited sub-network. A non-standardized push-to-talk (PTT) capability from one state may be incompatible with the PTT application in the visited state, and may also be bound to their home network.

[91] Hence a person ticketed by one agency may be stopped again by another, without the officer knowing about the previous ticket.
[92] FCC (2012, March 16). *Order DA 12-423*.

APPENDIX D - OREGON BTOP GRANT APPLICATION SUMMARY

This appendix contains a high level summary of the information proposed in Oregon's BTOP OPSBN grant application. This information can be used as a rough baseline to compare incoming FirstNet data collection information for consistency and reasonableness. It can also be used to pre-populate financial models in advance of receiving FirstNet offer details.

From the BTOP grant application:

> The OPSBN will be distributed throughout the State of Oregon, with some overlapping coverage in the neighboring states of California, Idaho, Nevada, and Washington. Last-mile services will cover approximately 40% of the State's land area and more than 85% of the population. 531 public safety community anchor agencies are included in the project area and the OPSBN will be constructed using four types of locations:
>
> - 225 existing OWIN radio sites will be upgraded with LTE equipment. These sites will use the existing OWIN microwave and/or fiber optic cable backhaul.
> - 27 greenfield sites will be constructed and will use fiber and, where necessary, short haul microwave for backhaul.
> - 86 sites will be collocated on existing commercial cellular sites, and will lease additional commercial backhaul to ensure adequate capacity to manage disaster situations.
> - 50 micro-cell sites will be constructed in highway rights of way. These will be linked with fiber and/or microwave as is most appropriate and cost effective.
>
> State public safety users are estimated at 15,000 within 3 years of project start, with an additional 10,000 federal, tribal, and local users expected within the first 5 years. Oregon does intend to partner with one or more commercial entities to develop, operate and maintain the OPSBN system, but these partners will not be identified until the completion of an RFP process.
>
> In addition to the network size assumptions made by the State of Oregon there are additional Capital expense (Capex) assumptions that are provided by the FCC:
>
> - Cell sites in rural America are treated as a blended build of new sites on existing structures and new sites.
> - $95,000 blended average per site Capex for adding public safety broadband to commercial LTE cell site.
> - $35,000 hardening per site for commercial LTE sites.
> - $216,000 average per site Capex for adding public safety broadband to existing sites in most rural areas, including $75,000 per site for hardening.
> - $363,000 average per site Capex for public safety broadband new sites in the most rural areas, including $75,000 per site for hardening.

- Priority wireless service on commercial networks, deployable and in-building supplementation provides for capacity surges, more extensive coverage and more resiliency, thus lowering site requirements on the core network.

Using the estimated network size and required Capex the project costs are estimated to be $214,285,714 with the State of Oregon is providing a 30% cash match of $64,285,714 to the BTOP application request of $150,000,000.