

ALMR INSIDER

Volume 11, Issue 3

July 15, 2017

ALMR Help Desk

In Anchorage:
334-2567

Toll Free within Alaska (outside of Anchorage):
888-334-2567

E-mail:
almr-helpdesk
@inuitservices.com

Inside this issue:

NPSTC Radio Interoperability Best Practices #2	2
FirstNet Deployment and Functionality	2
Duplicate Subscriber IDs Cause Problems for Agencies and the ALMR System	3
LMR and LTE Convergence	3
FirstNet Becoming a Reality for Alaska	3
Did You Know?	4

The High Cost of Providing Public Safety

Ensuring that citizens have a safe environment in which to live and work is of the utmost importance to local and state governments. They strive to promote the health, safety and welfare of all their citizens. Unfortunately, providing a high level of public safety does not come cheap.

Ensuring public safety historically has included traditional fire protection and EMS activities and traditional police protection services, such as officers patrolling streets for traffic violations and criminal activity and responding to numerous 9-1-1 calls. However, in today's world, the task of providing public safety has expanded as threats have increased and citizen expectations have grown. Public safety now encompasses the following, along with a host of other activities:

- Earthquakes and other natural disasters
- Preventing and responding to terrorist threats and attacks
- Federal homeland security mandates
- Hazardous materials response
- Drug task forces
- Search and rescue

For most citizens, it is almost an automatic response to turn to government in times of need. This translates to the need for spending tax dollars on public safety services. As is the case in Alaska, counties, boroughs and cities throughout the country expend considerable resources anticipating what the public at large generally doesn't want to think about—emergencies.

As the previous list illustrated, police, fire and EMS are now expected to protect our homeland and be ready to respond to terrorist attacks with chemical, biological and even the possibility of weapons of mass destruction. That's a

tall order, considering the cost of maintaining the required standard public safety equipment, the training to operate that equipment and employing the proper personnel.

Unfortunately, it does not stop at just having the necessary gear and personnel for these agencies. There must be a robust and reliable communications system available at all times to support their day-to-day operations, as well as the capability for them to talk to each other immediately when unexpected and catastrophic events occur that may encompass multiple agencies from multiple jurisdictions.

Imagine calling 9-1-1 and no one answers with the emergency help you need. What would you do? This scenario isn't something any of us would ever want to encounter, but when governments fail to see the criticality of public safety, along with the absolute necessity to fully-fund the backbone communications system, they are in as much as saying there is no need for emergency responders.

Public safety is a crucial service; it's not a nice-to-have commodity, it's a "must have." Governments must commit themselves to supporting their public safety enterprise by embracing the necessity of adequately planning for, and fully executing, the long-term funding for critical public safety communications infrastructure operations and maintenance. Without doing so, they may be putting everyone at serious risk.

(Article excerpts taken from Texas Municipal League at <https://www.tml.org/HCW/HighCost-ProvidingPublicSafety.pdf>)

Two New ALMR Sites Installed

Installation of new, five-channel VHF sites at both Delta Junction and Knik was completed on May 26. The Delta site will replace a previous Department of Defense site that moved to Fort Greely, which resulted in coverage de-

ficiencies in the area. The New Knik site will cover gaps in the Knik area, as well as improve coverage in the Eklutna Lake area. Both were declared operational June 26. (Article by Sherry Shafer, OMO)

NPSTC Radio Interoperability Best Practices #2 - Interoperability Systems Change Management Practices

This is a continuation from the January *Insider* article of the Best Practice ongoing effort on the part of the National Public Safety Telecommunications Council (NPSTC) to identify recommendations for a variety of topics dealing with interoperability. The Radio Interoperability Best Practices Report companion document link is located at end of article.

Change management practices and policies should always be used to ensure that any changes to operational policies, system modifications, additions, or deletions of interoperability system infrastructure are communicated to all affected agencies.

An interoperability system is comprised of infrastructure, people, policies, and processes and is dependent on all of these working together in order to be successful. Each individual item within this system can always change for any reason at any time requiring system adjustments. When this happens, it is critical that the change is communicated in appropriate detail to each person involved.

Change management processes are frequently not developed or memorialized in policies when it relates to technical systems or their support. This is generally very different from the majority of operational management processes for others within a public safety organization. Radio system or system use changes should always be submitted through an established organizational change management process in order to be successful when implemented. As an example, this can assure that when a radio site or channel is inoperable that everyone who should be informed is informed and assures they are also notified when the site or channel is back in operation.

Following an agreed upon change management process will ensure anyone granted use of an interoperability system is aware of any changes, is communicating these changes across their organization, and is also reviewing a change before it takes place, if it could in anyway impact

how they operate, as proactively as possible.

Successful Change Management depends on identifying, generally before a system or process is employed, who will be assigned the four key roles of a change management process. These are:

- **Responsible:** This is the role assigned to someone or the group that will be implementing a change and has likely proposed the change that is being made. The role also has developed a back-out / back-up plan in case the change has any negative impact. This role also initiates the change management procedures established and ensures that all roles that have been identified
- **Accountable:** This is the highest level of involvement within a change management process. Any change to a system or process always requires review and approval before a change is made
- **Consulted:** This role is assigned to someone who may be involved with helping to implement a change or will need to be a key adviser or tester of a change
- **Informed:** This role is assigned to anyone and everyone who may need to know that a change is taking place and that it may or may not impact normal operations in any way

Change management touches the Governance, Standard Operating Procedures, Training and Exercise, and Usage lanes of the SAFECOM Continuum.

ALMR Change Request Management Policy and Procedure 400-3 cover the process for the System and are posted on the web site (www.alaskalandmobileradio.org/documents.htm)

(Article excerpts taken from NPSTC Radio Interoperability Best Practices, January 2017)

(Best Practices Report - http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_I_O_Best_Practice_Overall_Report_Final.pdf)

FirstNet Deployment and Functionality

Now that the First Responder Network Authority (FirstNet) is closer to being a reality, questions arise when considering continuing to invest in land mobile radio (LMR) systems such as ALMR. The nationwide public-safety broadband network (NPSBN) will accommodate both voice and data with perhaps redundant coverage in some areas. However, the earliest projections indicate the NPSBN will be operational in 2022 and will initially include only data transmissions, not voice service. Furthermore, even the most optimistic projections cannot establish when FirstNet will provide the proven and reliable network necessary for mission-critical applications.

Agencies must give serious thought to the layers of deployment and functionality. Where will the systems first

be deployed and will they immediately serve rural areas? Given these concerns, along with operational and functional considerations and ongoing development of standards, it is clear Project 25 (P25) networks are here to stay. As such, agencies must continue to maintain, optimize and build out P25 systems with an eye on future integration into Long Term Evolution (LTE) networks.

Given the current unknowns of when and where, with regard to the NPSBN, it is imperative that systems like ALMR be kept technologically current and in position to complement the additional capabilities that NPSBN will provide.

(Article by Mr. Del Smith, ALMR Operations Manager, excerpts from July 2017 Mission Critical e-magazine)

Duplicate Subscriber IDs Cause Problems for Agencies and the ALMR System

ALMR agencies were recently advised of this issue, but it cannot be emphasized enough.

An increasing number of duplicate subscriber IDs have been detected by the ALMR Help Desk in recent weeks. It appears that some agency subscriber units may not be properly programmed prior to activation on the ALMR System, particularly when “cloning” is used to program the subscriber unit. It is critical that only personnel that have been adequately trained, and have a full understanding of the process, program subscriber units for ALMR member agencies.

The impact of duplicate IDs on the end user can be an inability to access the System if another subscriber unit with that ID is also active on the System at that time. Also, “crosstalk” can occur, wherein the user will poten-

tially hear traffic from multiple separate talkgroups, depending on how many subscriber units with that same ID are active on the System at the same time.

As the ALMR Help Desk detects apparent duplicate IDs, the agency will be contacted and advised of the situation. In coordination with the agency involved, duplicate IDs will need to be deleted from the System, which has the potential to disable numerous agency radios, depending on the number of improperly programmed subscriber units. Radios with duplicate IDs will also need to be re-programmed with a corrected ID by the agency prior to being put back into service on the System.

(Original information provided by Mr. Del Smith, ALMR Operations Manager, June 1, 2017, and re-used for this article.)

LMR and LTE Convergence

The replacement of land mobile radio (LMR) by long-term evolution (LTE) for public safety agencies has been a much discussed and debated topic for several years. Now that AT&T has begun the implementation of the long awaited National Public Safety Broadband Network (NPSBN) known as FirstNet, the discussions are likely to gain intensity as to the if, when and how.

Current thinking among numerous public safety officials, LMR industry representatives and FirstNet personnel focuses on NPSBN as initially being a supplemental communications asset for public safety, providing data and voice; however, not initially a replacement for critical voice communications over LMR. As the technology continues to evolve and standards are developed, LTE devices may be able to support device-to-device (simplex) or talk-around communications, which is a critical requirement for public safety users.

If for no other reason, the use of simplex or talk-around should be enough to justify keeping an LMR system in place at least for the foreseeable future. What will happen in years to come no one knows, but in the meantime, numerous vendors are working on combination LTE and LMR devices to try to solve the two-device-per-person issue. It will be interesting to see how this plays out over time.

As the technologies involved continue to merge in the LMR and LTE worlds, it will require users to understand the language used by the other technology. LMR users are generally familiar with LMR base stations, repeaters, simulcast systems, trunked systems, P-25 digital systems, talk-groups, time-out-timers, and many more terms. On the LTE side, there is the Radio Access Network (RAN), the Evolved Packet Core (EPC), IP, Asynchronous Balanced Mode (ABM), Access Class (AC), Quality of Services (QoS), and priority, pre-emption, and ruthless pre-emption, which seem to be used interchangeably even though each carries a different set of implications. For antennas, the term Multiple Input, Multiple Output (MIMO) is confusing to LMR users. MIMO antenna technology has an impact on the number of antennas needed on a tower, on a vehicle and in a handheld device. Today there is 2X2 MIMO and 3X3 MIMO, each offering more throughput and capacity, and work continues on adding even more antennas to an antenna array.

Suffice to say, that both LMR users and LTE users will take some time to understand how the two technologies can best be combined and utilized to maximize the benefits of both for public safety first responders.

(Article prepared by Mr. Del Smith, ALMR Operations Manager, with excerpts from Public Safety Advocate: Translating for LMR and LTE Worlds, May 11, 2017)

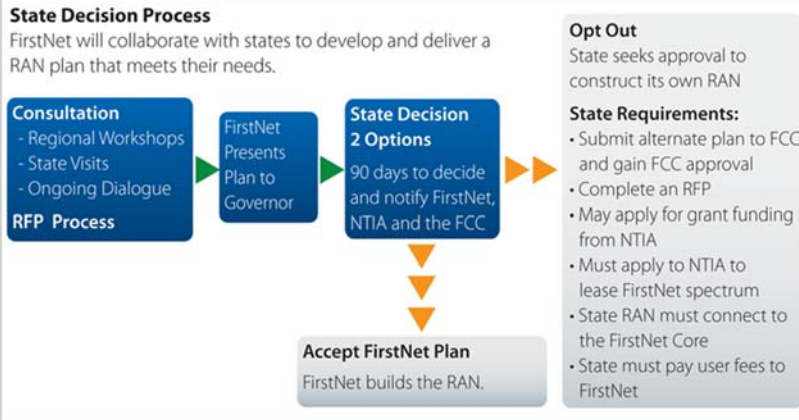
FirstNet Becoming a Reality for Alaska

FirstNet was created by Congress to fulfill one mission: provide emergency responders with the first nationwide, high-speed, broadband network dedicated to public safety.

Signed into law on February 22, 2012, the Middle Class Tax Relief and Job Creation Act of 2012 created FirstNet. The Act provides state Governors with a choice to **Opt-In** and immediately take advantage of the FirstNet net-

work, or **Opt-Out** and initiate the process for deploying, maintaining and operating a state-specific Radio Access Network (RAN) that interoperates with the FirstNet (core) network. The Governor has 90 days to decide, once FirstNet delivers notice of the completion of the request for proposals (The Plan) process for Alaska (per 47 U.S.C § 1442(e)(1)). The State Plan outlines FirstNet’s approach to coverage, products and (continued on page 4)

FirstNet Becoming a Reality for Alaska (continued)



Help Desk (In Anchorage Bowl):
 334-2567

Toll Free within Alaska:
 888-334-2567

Fax: 907-269-6797

Email: almr-helpdesk@inuitservices.com

Website: <http://www.alaskalandmobileradio.org>

Follow us on Twitter: @ALMR_SOA

Did You Know?

All new users are required to complete the appropriate level of training before they are granted access to the ALMR System. To request new user access and training, the member agency POC shall contact the ALMR Help Desk and initiate a New User Access Request. All Level II and Level III System users are required to renew their training certificate yearly .

(Cybersecurity Procedure 200-5)

services, and pricing for Alaska’s public safety users. FirstNet has provided full details of the “draft” State Plan to the Alaska SPOC and public safety community for their comprehensive review. The critical dates in the Alaska process are:

June 19: FirstNet opened the State Plan Portal (SPP) to the Alaska SPOC and public safety community for their comprehensive review.

June 28: FirstNet and AT&T met with the Alaska Public Safety community to review the State Plan with comments due August 4.

August 4 thru Mid-September: FirstNet reviews all comments submitted and makes necessary refinements to provide the final State Plan.

Mid-September thru Mid-December: Governor Walker should make the decision whether to opt-in or opt-out.

(Article by Mr. John Rockwell, SOA FirstNet Single Point of Contact [SPOC])

**Alaska Land Mobile Radio
 Operations Management Office
 5900 E. Tudor Road, Suite 121
 Anchorage, AK 99507-1245**

