ALMR INSIDER

Volume 19, Issue 3 July 15, 2025

ALMR Help Desk

In Anchorage: (907) 334-2567

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

E-mail: almr-helpdesk @beringstraits.com

Follow us on Twitter: @ALMR_SOA

Inside this issue:

Tuning Your Radio	2
Federal Information Processing Standards (FIPS)	2
The Importance of System Restarts	2
FCC Sees Surge in Public-Safety LMR Licensing	3
Microwave Backhaul	4
June Metrics	4

What is the Future of LTE and Will it Replace ALMR?

Given the frantic pace of LTE development and the falling cost of ownership, the hot question of the moment is 'Will LTE replace LMR?'. It may surprise you to know that the consensus among those with the biggest stakeholders in mission-critical LTE is that, while they anticipate LTE (and eventually 5G) to take over many of the functions of LMR, we should expect to see the continued use of LMR for many years to come.

Even the operators of these major LTE systems warn that public safety agencies cannot rely on LTE alone. They see LMR as a necessary element of public safety critical communications for the foreseeable future. To quote a statement from FirstNet:

"First responders currently use land mobile radio (LMR) networks for mission critical voice communications. When the nationwide public safety broadband network (NPSBN) is launched, it will not replace their LMR systems. The network is expected to initially transmit data, video, and other high-speed features, such as location information and streaming video, as well as non-mission critical voice. Public safety entities will continue to use LMR networks for their mission critical voice needs."

One reason is that for all critical communications users (not just public safety), LMR remains the technology which is still available when others have failed. LMR was designed with a variety of failsafe options to preserve communications, even when major components of the network are damaged or become inoperable.

Thus, if the core network fails in a multi-site LMR system, each working individual site can switch to local standalone operation and can still connect any units within range. And if all sites are down, units can still talk to each other in direct (simplex/talkaround) mode without a network.

Public safety relies on these fallbacks, which at this stage LTE networks struggle to offer. LTE standards (e.g. ProSe for Direct Mode, IOPS [*Isolated E-UTRAN Operation for Public Safety*] for standalone site comms) have been developed to address these critical concerns, but it is in the early days for the commercial products. A great deal of real-life testing lies ahead before public safety feels totally safe with the delivered goods.

So far, LMR is the technology that comes closest to delivering public safety grade systems. It has taken a few decades of field and interoperability testing, customer experience, standards, and product refinement to reach this point. LTE, in the view of its developers and organization users, is still in learning mode. Their strong recommendation is to retain LMR for mission-critical voice alongside LTE for broadband data.

This recommendation has an underlying message: 'No technology is good at everything, so why stick with just one?'

LMR has been battle-tested in emergency situations and its combination of wide-area voice coverage where no telco wants to tread; tried-and-true voice call services; ultra-reliable networks with built-in failsafe; and a better handle on interoperability than its competitors. LTE brings dazzling broadband data performance, low latency, a ready platform for the development of custom applications, and a path to the future.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from the Radio Academy website)

Tuning Your Radio

Proper tuning of your ALMR radio ensures that you have clear and uninterrupted communication. This is particularly important in emergency situations where every second counts, and any miscommunication can lead to dire consequences. Tuning helps to minimize interference and static, providing a clear channel for transmitting and receiving messages.

Tuning your ALMR radio can significantly enhance signal strength, allowing for better coverage and range. This is especially important in areas with challenging terrains or in urban environments where buildings and other structures can obstruct signals. A well-tuned radio ensures that you can communicate effectively, even in the most demanding conditions.

A properly tuned ALMR radio can also help in conserving battery life. When a radio is not tuned correctly, it may have to work harder to maintain a connection, which can drain the battery faster. By ensuring that your radio is tuned, you can extend its operational time, which is crucial during long shifts or extended operations.

Regular tuning and maintenance of your ALMR radio can help in identifying and addressing potential issues before they become major problems. This proactive approach can reduce the need for costly repairs and replacements, ultimately saving your department money and ensuring that your equipment is always ready for use.

In conclusion, tuning your ALMR radio is not just a routine maintenance task; it is a critical component of ensuring reliable and effective communication in mission-critical situations. By maintaining clear communication, enhancing signal strength, improving battery life, ensuring compliance with standards, and reducing maintenance costs, tuning your ALMR radio can make a significant difference in the performance and reliability of your communication system.

(Article prepared by Mr. John Rockwell, Division Operations Manager of DPS, Statewide Services)

Federal Information Processing Standards (FIPS)

Beginning in September 2026, the cryptographic protection requirements for all criminal justice information services (CJIS) must meet FIPS 140-3 requirements. The current guidance, FIPS 140-2, has been around since 2001, and is in need of an upgrade to maintain cryptography.

Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearance but lack the necessary formal access approvals.

FIPS 140-3 protection requirements for all CJIS material is a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of al least 256-bit strength. To summarize these requirements, in the LMR world, this means all systems must use AES-256 encryption. AES-256 encryption is the most secure algorithm available today and your ALMR system is already using AES-256 exclusively.

Some agencies in Alaska use the Data Encryption Standard (DES), which is only a 64-bit encryption, and will not be CJIS compliant starting in September 2026. If it is not updated they risk losing their ability to use the CJIS system.

I encourage all public safety agencies in Alaska to review the upcoming CJIS and FIPS 140-3 requirements listed in the CJIS security policy version 6.0, which can be found at le.fbi.gov/cjis-division/cjis-security-policy-resource-center.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from the CJIS security policy version 6.0, 12/27/2024)

The Importance of System Restarts

The ALMR network has made great progress ensuring system reboots happen monthly. I will be going through the reasoning behind this policy and why it is important to the operation and security of the network.

Routine restarts are required due to Federal standards based on the Risk Management Framework, while also benefiting the user in multiple ways. Such as refreshing the systems memory allowing programs to utilize space without having to un-allocate it from other programs. It also resolves many system issues, which is why it is the first step in troubleshooting most computer problems.

Finally, it is essential to network security.

From a security mindset, restarts are required for maintaining the status of the network. By restarting, you allow the computer to perform necessary patching on the systems key files. A system not restarted will remain vulnerable even after the patch has been applied. I want to thank everyone for their efforts in this area maintaining the security posture for all ALMR users.

(Article prepared by Mr. David Reed, ALMR Information Systems Security Manager.)

FCC Sees Surge in Public-Safety LMR Licensing

Public-safety land mobile radio (LMR) licensing activity has increased significantly thus far this year—in fact, the current pace would represent more than 40% jump, if continued throughout the rest of 2025—according to information from the Federal Communications Commission (FCC's) online Universal Licensing System (ULS) database.

The FCC LMR database is part of the FCC's ULS, which contains all radio licenses issued in the U.S. You can use it to search, view, and download data on both public safety and private-sector LMR systems.

Through the first five months of the year, the FCC has received 1,787 licensing applications and has granted 1,452 of them, according to the online ULS database. If this pace of licensing activity is maintained throughout 2025, the number of granted licenses thus far project to 4,867 licenses for the year, which would be a 16.7% increase compared to last year and the highest total since 3,959 public-safety LMR licenses were granted in 2016.

This is particularly noteworthy, given the lackluster LMR licensing activity in the sector during the past seven years, when the annual total of public-safety LMR granted has been less than 3,200 every year and dipped below 3,000 last year—the second-lowest total since the online ULS database was established fully in 2001.

Projections for 2025 could be even more remarkable, if the 335 pending public-safety LMR applications are approved. This top-end potential total of 1,787 applications through the end of May projects to a year-end total of 4,291.1—a figure that would be the largest for the sector since 2015, when the FCC granted 4,248 public-safety LMR licenses. If realized, this total would represent a 43.7% increase when compared to 2024.

While such a total would be very significant in light of the lackluster public-safety licensing during the past eight years, it would have been considered closer to a baseline total just a decade ago, as the FCC granted at least 4,248 public-safety LMR licenses during each of the 14 years from 2002 through 2015.

In contrast, the pace of business-industrial LMR licensing this year is hovering at levels comparable to recent years. The sector's 4,229 applications through the month of May—644 of which are pending approval from the FCC—project to 10,155.2 for the full year. Last year, the FCC granted 10,733 business-industrial LMR licenses, which marked the first time the sector topped the 10,000 threshold in five years.

And the 2024 business-industrial licensing activity still ranked among the lower totals in the 24-year history of the FCC's only ULS database. The 2024 figure marked the eighth consecutive year that the business-industrial entities has failed to have 11,000 LMR licenses granted by the FCC—a stark contrast to the previous 16 years, when the agency annually approved at least 11,256 LMR licenses for the sector.

Based on the business-industrial LMR licensing pace set during the first five month of 2025, it appears doubtful that this string of sub-11,000 licenses granted in the sector will be broken this year.

Although the LMR infrastructure can be costly upfront, LMR systems do not rely on monthly carrier fees, making them a cost-effective solution for organizations over time. Regular maintenance and technical support are crucial to ensure the reliability and longevity of the LMR system. LMR technology uses conventional digital mobile radio (DMR), narrowband, and trunked systems in the United States.

Another reason organizations use LMR is that it operates on the FCC licensed frequencies reserved for specific users, reducing the risk of interference that affects cellular of unlicensed systems

While specific data for Alaska is not delineated in these national figures, the state's reliance on the ALMR system and its structured licensing approach suggest that Alaska is aligned with these broader trends, focusing on maintaining and enhancing its LMR infrastructure to meet public safety needs.

Many people do not realize how large of an area or how many agencies have a Part 90 LMR license. Agencies recognize the ALMR System and how it provides coverage for the majority of the road system, the Southeast and Kodiak areas; however, there are many smaller LMR systems both public and private.

In Alaska, private LMR systems are essential for various industries and organizations that require reliable, secure, and wide-area communication solutions. These systems are particularly vital in Alaska's challenging terrains and remote locations, where conventional communication infrastructures may be limited or nonexistent.

A search of the FCC ULS database for Alaska documents 2033 active licenses. These licenses are valid for 10 years and include both conventional and trunked systems. The majority of these licenses are owned by the State of Alaska, the federal government, and local cities but smaller agencies recognize the importance of an LMR system and have them installed in their buildings, such as hospitals and warehouses.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from the Urgent Communications article *FCC sees surge in public-safety LMR licensing*

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

Microwave Backhaul

What is microwave backhaul in ALMR? Microwave backhaul provides point-to-point wireless connectivity between two fixed locations. In ALMR it is used to carry voice traffic from remote tower sites back to the system core, supports trunked radio system control signals, enables dispatch and network management, and ensures redundant, high-reliability, high-resilient, communication paths network in mission critical systems.

Microwave backhaul in ALMR works the best in remote locations where fiber or copper is unavailable or cost prohibitive. It has low latency, which is critical for push-to-talk and trunked system signaling. It brings reliability to the system and is designed for high uptime with redundancy and protected paths, is cost effective and cheaper over time and can be encrypted and isolated from the internet.

A microwave site is more than just a tower, antennas, and dishes. Each microwave site may include, repeaters, base station radios, network interface devices, equipment racks, generators, dehumidifiers, heating and cooling systems, shelters, and cameras. Some mountaintop sites have other agencies equipment, such as the FAA, DoD, AKRR.

The ALMR coverage area includes the majority of the road system and includes several mountain ranges. Microwave sites are an integral part of the coverage area. They have a range of up to 50 plus, depending on terrain, line-of-site, and frequency.

They use a 6GHz frequency for the long range connections, which need a larger dish and 11GHz or 18Ghz for the shorter connections, utilizing smaller dishes.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager)

Help Desk (In the Anchorage Bowl): 907-334-2567

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

Fax: 907-269-6797

Email: almr-helpdesk@beringstraits.com

Website: http://www.alaskalandmobileradio.org

Follow us on Twitter: @ALMR_SOA

June Metrics

Calls	1,712,397
Push-to-talks	2,807,730
Busies	1,733 or .0010%
Subscriber units	32,226
State of Alaska	8,709
DoD	9,522
Local/Municipal	12,103
Federal	1,892