ALMR INSIDER

Volume 19, Issue 4 October 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:

APCO and MTUG 2025 Conferences

From July 27th to August 1st, I traveled to Baltimore, MD to attend back to back conferences and seminars. The week started with the Genesis Users Forum (GUF), followed by the Association of Public Safety Communications Officials (APCO) and the Motorola Trunked User Group (MTUG). The APCO and MTUG associations have many members, in Alaska and I attend these events to advocate for our interests.

The GUF opened with introductions of participants and it was a great networking event, being able to talk with my peers and share information. I was able to gather new FCC information on bi-directional amplifiers from my counterpart in Indiana and share it with the State engineers.

This was followed by optimizing the system to gather data such as total radios, TDMA vs FDMA transmissions and total ALMR tower usage during large scale vents or emergencies. The Genesis system has expanded enhancements for the MCC7500 and AXS dispatch consoles, which are used by many public safety dispatch centers across the state.

APCO began with me meeting with fellow members from Alaska to compare notes on sessions we were scheduled to attend to make sure we did not all attend the same sessions to take advantage of the training. After the opening statements from the Mayor of Baltimore, and the keynote speaker, we dispersed for our training sessions.

Cybersecurity for public safety agencies, dispatch centers, and radio communications is being increasingly attacked by nefarious agencies and constant vigilance is needed to maintain a viable system. I attended the Cybersecurity and Infrastructure Security Agency (CISA) briefing on emerging threats to technology and what security protocols are available from CISA to counter these attacks.

Another seminar I attended regarding cybersecurity was dispatch and 911 center centric, specifically IP based radio systems. It focused on the recent policies form the National Institute of Standards and Technology (NIST), specifically their cybersecurity and privacy reference tool (CPRT). The latest update which went into effect August 2025, maintains that in order to be NIST compliant, organizations need to have third-party security monitoring. This also applies to the updated Criminal Justice Information Services from October 2024.

When the exhibit hall opened I made my rounds to meet with multiple radio and equipment vendors to see their latest products, schedule acceptance testing for the ALMR system and to gather brochures which I sent out to dispatch centers back in Alaska.

ALMR is a Motorola system which is why it is important people from Alaska attend MTUG. This gives us a platform to listen to what is new from the engineers, voice complaints, and meet with other Motorola product users and attend the national MTUG meeting.

Some of the sessions I attended included the latest on bi-directional amplifiers and how they are part of the complete public safety distribution antenna systems (DAS). I learned of the updated International Fire Code, section 10 and the newest version of the National Fire Protection Association standard 1225, which sets the guidelines for DAS and their public safety communication certifications.

A major concern I learned regarding public safety radio systems is they are increasingly being targeted in the lower 48 by vandals for the copper wiring. Due to the remoteness of many ALMR sites, tower security is a new trend for possible grants.

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

A Basic Guide to the ALMR Website

Did you know that the ALMR website contains a plethora of valuable information that can assist member agencies? The journey begins by going to the ALMR website at https://alaskalandmobileradio.org.

The homepage has the Upcoming Events Calendar, which contains information on upcoming events such as webinars, conferences, conventions, etc. It also houses the Security Announcements for ALMR Users, which shares important security and cybersecurity information from reputable sources; and SAFECOM Grant Guidance 2024, which provides resources for members to obtain possible grant funding.

The "Who We Are" tab provides information on the Executive Council and its representatives: the User Council, which lists the primary representatives; the agencies on ALMR; and the ALMR team and point of contacts (POCs). All of the Executive and User council meetings are uploaded under this tab and you can download the meeting agendas, minutes, and listen to the meeting recordings. These are updated within 5 days after every scheduled meeting and go back to 2005.

The "About ALMR" tab provides access to ALMR's governing documents, which includes the Cooperative and Mutual Aid Agreement; Plans and Strategic Documents; Policies and Procedures; and Definitions and Acronyms. Besides these important documents, you can learn the history of ALMR, program objectives, coverage areas and more.

A very important tab is the "Training" tab where a variety of training videos are categorized by topics, which are helpful to agencies and their members to learn how the system is managed and operates. The five different categories, includes Administrative, Subscriber Units, System, Interoperability, and Other Topics. Members may also request specific training through this tab.

The last tab, "Membership," contains a link to the forms that agencies may need to use, past newsletters, a list of approved equipment, and more. If your agency is preparing to buy new radios or mobile units, be sure to view the list of approved equipment, it tells you what units work on the ALMR system and which are TDMA compatible.

Please take the journey through the ALMR website today.

(Article prepared by Ms. Mary Burnham, ALMR Document Specialist)

National Emergency Response Information System (NERIS)

As of January 1, 2026, the National Fire Incident Reporting System (NFIRS), the legacy system that has guided federal fire data collection for five decades, will cease operation. Taking its place is the National Emergency Response Information System (NERIS): a modern, cloud-based platform developed to enable faster data collection, smarter reporting, and deeper analytics for fire departments across the country.

NERIS is not just about fire. While fire response remains central, NERIS reflects the full spectrum of emergency response. For Emergency Communications Centers (ECCs) and Public Safety Answering Points (PSAPs), the transition represents a significant shift from underrecognized support roles to core contributors.

Because CAD systems are often operated by law enforcement or shared public safety agencies, ECCs play a foundational role in shaping the data that enters NERIS. The incident record starts at dispatch, and for the first time, ECCs are structurally recognized in the national fire data platform.

Key Dates Mandated by Congress:

December 31, 2025: Final day to use NFIRS

January 1, 2026: NERIS becomes the primary reporting method.

January 31, 2026: Deadline to close out 2025 NFIRS records.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from "Modernizing Incident Intelligence: What leaders need to know about NERIS," by Mr. Dustin Andres, PSC Magazine, Sept./Oct. 2025)

Active Radio Audits

The ALMR system is licensed for 33,000 subscriber licenses and we are currently reaching this number.

The Operations Management Office (OMO) is actively contacting each agency on the system to update their radio inventories, to include subscriber units that have not been seen by the system for at least three years.

The OMO realizes many of the thousands of radios on the system that have not been seen are deployed to areas around the state that do not have ALMR coverage, such as Western Alaska. Several agencies have reported that they are keeping radios in a cache to hand out during large emergencies.

The OMO recommends agencies conduct quarterly radio checks with all of their subscriber units. This entails checking the batteries, affiliating them to an ALMR tower and conducting radios checks using the PTT button. This will validate the radios on ALMR and will assist with subscriber license inventories.

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

SBC Petition Seeks FCC Clarity on BDA Deployments

A recent Safer Buildings Coalition (SBC) petition filed with the FCC proposes the establishment of a framework that is designed to let land-mobile-radio (LMR) licensees appropriately review the installation of signal boosters that often provide critical in-building coverage that supports for public-safety response efforts.

For more than a decade, FCC rules require Part 90 signal-booster operators to obtain "express consent" from frequency licensees before operating signal boosters, such as bi-directional amplifiers (BDAs), but there are no specific guidelines for obtaining the consent of LMR licensees, according to the SBC petition. This guidance gap has resulted in signal boosters being deployed in ways that could create life-safety risks, the petition states.

BDAs address the well-established problem of "wireless dead zones" inside buildings that block critical public safety communications. The FCC has recognized that "signal booster systems play a crucial role in allowing public safety first-responders to communicate in buildings, tunnels and other areas where signals would normally be blocked."

"Improperly deployed signal boosters are interfering with, degrading, and disrupting public safety communications during critical emergency responses, potentially placing first responders and civilians in jeopardy," according to the SBC petition.

SBC Managing Director John Foley said his organization's petition was filed in hopes of encouraging the FCC to establish a clear framework for signal-booster installers to obtain "express consent" from Part 90 licensees. Foley said he met this month with representatives from four FCC bureaus about the petition.

These signal boosters are the core component of Emergency Responder Communication Enhancement Systems (ERCES) - the current standard terminology in fire and building codes and standards. ERCES are complete solutions that include signal boosters, cabling, antennas, couplers, power supplies, and other components needed to provide reliable in-building coverage. While the entire ERCES system is needed for a complete solution, signal boosters and their performance are specifically referenced in FCC Part 90 rules, which is the focus of this petition.

Fire and building codes and standards have required solutions to ensure adequate first responder communication coverage inside buildings since 2009, though these requirements have been continuously refined over time. Authority Having Jurisdiction (AHJ) and code official awareness of these requirements has grown significantly, leading to increased enforcement and more ERCES deployments.

Rapid growth in coverage solution deployments driven by fire code requirements has exposed the absence of rule-based coordination procedures, creating a regulatory gap during significant deployment growth.

"It was a good discussion," Foley said during an interview with *IWCE's Urgent Communications. "We're optimistic that this will go out to comment, and we're very interested to hear what the community has to say on the topic."*

Under the SBC proposal, the FCC would create "a structured authorization framework—using proven frequency coordination precedents—to establish clear procedures for requesting, evaluating, granting, and tracking rebroadcast consent, while maintaining frequency licensee control over their spectrum rights."

SBC's petition notes that FCC rules approved in 2013 established a "comprehensive" regulatory framework for consumer signal boosters but "left significant implementation gaps" regarding the deployment of if industrial signal boosters.

"As a result, poorly deployed or designed signal booster systems are now causing critical problems that directly impact public-safety operations and first-responder safety," the petition states. "Root cause analysis reveals three primary categories of problems requiring immediate attention:

"• Failure of System Installers and Designers to Follow FCC Rules;
"• Lack of RF Design and Installation Competency;
"• Regulatory Framework Gaps from 2013 Rulemaking."

In addition to the SBC proposal addressing these public-safety issues, having a clear process for obtaining Part 90 licensees consent to deploy signal boosters should remove confusion for building owners and allow regulatory bodies to operate more efficiently, according to information included in SBC's web page summarizing the petition.

SBC is not alone in identifying the issues associated with Part 90 signal-booster implementation.

"Multiple organizations have documented these coordination process gaps," the SBC web page states. "The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) established the Bi-Directional Amplifier Focus Group specifically to address these issues, documenting that 'unknown implementations and operations of uncoordinated Bi-Directional Amplifiers is causing harmful noise and interference to public safety radio systems.'

"An APCO survey of public-safety agencies confirmed widespread deployment challenges, while SBC's No Noise Task Force brought together industry veterans to develop solutions for these coordination problems."

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from "*SBC petition seeks FCC clarity on BDA deployments,"* by Mr. Donny Jackson, Urgent Communications newsletter, August 2025 and the SBC's FCC filing dated July 22, 2025)

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

Cybercriminals Target Law Enforcement Portals

As of August 2024, FBI noted an uptick in criminal forum posts regarding conducting fraudulent emergency data requests and released a notification for industry awareness. Cybercriminals are likely gaining access to compromised US and foreign government email addresses and using them to conduct fraudulent emergency data requests to US based companies, exposing the personal information of customers to further use for criminal purposes.

The FBI recommends government and other organizations that receive emergency data requests take steps to improve their security posture in response to the noted attack trends and possible outcomes using more resilient security protocols. The FBI recommends organizations establish and maintain strong liaison relationships.

The FBI further recommends organizations review and, if needed, update incident response and communication plans that list actions an organization will take if impacted by a cyber incident

Timely software and firmware patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should prioritize patching of vulnerabilities on CISA's Known Exploited Vulnerabilities catalog.

The FBI recommends you require all accounts with password logins (for example, service account, admin accounts, and domain admin accounts) to comply with National Institute of Standards and Technology (NIST) standards for developing and managing password policies.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from FBI notice 20241104-001, 4 November 2024)

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

ALMR Towers

The ALMR system is divided into zones. Zone One has 60 towers which includes Kodiak, S.E. Alaska and the central area. Zone Two includes the Fairbanks and surrounding Northern communities and has 25 towers. The third zone covers the Anchorage area and has 14 sites.

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