

ALMR INSIDER

Volume 20, Issue 3

July 15, 2026

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:

Land Mobile Radio (LMR 101) 2

Public Safety Radio Threat Landscape 2

ALMR Membership Agreements 2

Wi-Fi for Public Safety In-building Communications 3

Firewall Exploits Facilitate 9-1-1 4

ALMR Equipment 4

FCC Approves New Disaster-reporting Rules for Public Safety

FCC commissioners today unanimously approved rules requiring public-safety broadband providers to report disaster-related network outages publicly in the Disaster Information Reporting System (DIRS), but in a manner that is designed to be relatively streamlined.

FCC Chairman Brendan Carr said he believes the language in the new report and order can help address some of the issues he observed in the wake of Hurricane Helene's devastating impact in North Carolina less than two years ago.

"One thing that stood out to me in the aftermath of Hurricane Helene was how many resources were still being tied up by outdated paperwork-filing requirements," Carr said during the FCC's open meeting, which was webcast. "In the middle of a disaster-recovery effort, the FCC should be focused on helping crews reconnect communities, allowing them to clear barriers that slow down recovery efforts. Limited manpower shouldn't be spent on unnecessary red tape.

That's why I am pleased we are taking action today to modernize the FCC's disaster-reporting system in a way that reduces burdens while still ensuring that we have the accurate, up-to-date information on service and restoration efforts that we need. This will be especially important for small, rural providers that may already be stretched pretty thin during times of emergencies."

FCC Commissioner Olivia Trusty echoed this sentiment.

"In addition to making DIRS easier to use, this item will provide federal, state, and local officials with a more precise and comprehensive understanding of network availability in the aftermath of disasters so they can help restore connectivity when communities need it most," Trusty said during the meeting.

"When providers should be focused on the maintenance and restoration of communications services, they should be met with a simple and functional system that is easy to navigate, and this Third Report and Order helps to achieve that objective."

Under DIRS, network providers always have been required to provide daily updates about the status of cell towers in designated areas that has been impacted by a natural disaster, such as a wildfire, hurricane or earthquake. Under the new rules, this requirement is extended to public-safety offerings—for example, FirstNet, Verizon Frontline and T-Priority.

FCC Commissioner Anna Gomez said there was consideration that the FirstNet Authority should be subject to DIRS reporting. However, Gomez—who helped oversee the earliest days of the FirstNet Authority while working with the NTIA in 2012—offered an accepted edit that allows FirstNet contractor AT&T to submit the public-safety information.

"What I requested was that we take out the direct order to FirstNet [the FirstNet Authority] to file and instead make that an order for AT&T, which is operating the network on behalf of FirstNet," Gomez said during a press conference conducted after the FCC meeting.

"It [the FirstNet Authority] is an independent authority housed at the Department of Commerce, and I didn't think it was appropriate for the FCC to directly order them to do that."

The ALMR team will continue to monitor this new regulation and work with the statewide dispatch centers for any future updates for disaster declarations.

(Article originally posted on the Urgent Communications website by Donny Jackson, May 20, 2026)

Land Mobile Radio (LMR 101)

LMR systems are the primary means of voice communications among public safety personnel. LMR systems are designed to meet the unique needs of public safety, and deliver secure, reliable, mission-critical voice communications in a variety of environments, scenarios, and emergencies. LMR technologies have been used by public safety personnel for many years, and provide the most reliable means of voice communications for public safety available.

LMR technology has progressed over time from conventional, analog voice service to complex systems incorporating digital and trunking features that enable such features as rapid voice call-setup, group calling capabilities, high-quality audio, and guaranteed priority access to the end-user. These enhancements have improved the interoperability, spectral efficiency, security, reliability, and functionality of voice and low-speed data communications for public safety personnel.

Public safety agencies are trained and skilled in the use of LMR technologies. LMR technologies and features

have been integrated into response protocols and training curriculum, and tested through planned exercises and real-world events. While new technologies are entering the market every day, emergency responders are most familiar with how LMR technologies work. This familiarity has helped public safety agencies plan for various scenarios and execute effective response operations.

While the community considers new and emerging technologies to supplement communications, current LMR capabilities must be sustained until other technologies exceed the reliability that LMR offers. Decision-makers should consider the impact of funding decisions on their agencies' ability to communicate during day-to-day incidents, emergencies, and natural and man made disasters. The federal government and public safety agencies have spent billions building a vast LMR infrastructure and training users. Without continued investment to operate and maintain LMR systems, emergency communications could be compromised.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager from the CISA, February 2026, LMR 101 flyer)

Public Safety Radio Threat Landscape.

Attacks against public safety radio systems remained consistent in 2025, totaling three observed incidents, a slight reduction from four in 2024. While the volume decreased marginally, the sustained targeting of these networks indicates continued adversary interest in compromising public safety radio infrastructure. These attacks remain relatively infrequent compared to compromises of other mission-critical systems.

In 2025, ransomware remained the most disruptive threat to public safety radio. The Qilin group was attributed to two of the three observed attacks, including one that disrupted communications for a fire and rescue service in Zlin, Czechia. The second Qilin attack impacted peripheral radio services for a sheriff's office in Texas. Furthermore, 2025 saw a diversification of malicious activity beyond traditional extortion, as defenders suc-

cessfully blocked an attempted Log4Shell exploit intended to install crypto mining software on a public safety radio network.

Observed malicious activity demonstrates that adversaries are actively probing remote access pathways and public-facing radio devices, exploiting weak identity controls, legacy equipment, and network visibility gaps. Public safety agencies are strongly advised to prioritize the identification and remediation of unknown or legacy devices, the deployment of Endpoint Detection and Response (EDR) solutions, and the implementation of more rigorous access controls.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager from the May 21, 2026 Public Safety Threat Alliance threat report)

ALMR Membership Agreements.

To become a member of Alaska Land Mobile Radio (ALMR), and organization must meet two requirements. Is it a part of a Federal, State, Local, or Tribal government or does it provide a public safety service? Once these questions are answered then an agency is encouraged to become a member of ALMR.

A membership agreement will be sent to the agency and the agreement is valid for one year. It runs concurrently with the State of Alaska budget year, July 1 through June 30 of the following year.

Any new member is encouraged to read the new user policy and procedure, 300-4, which can be found on the ALMR website in the policy and procedure section.

Member agencies are responsible for complying with all terms and conditions as outlined in the signed membership agreement and complying with all policies and procedures. This also includes conducting and verifying a yearly inventory of all of their radios.

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

Wi-Fi for Public Safety In-building Communications.

Widely deployed Wi-Fi technology could be leveraged to help address longstanding in-building wireless coverage issues for first responders and the citizens they protect, according to multiple speakers providing their insights on the topic during a webinar hosted by the Wireless Broadband Alliance.

Steve Devine, CTO of the Association of Public-Safety Communications Officials (APCO), said he believes Wi-Fi can be a valuable augmentation—particularly inside building and other structures—to the land-mobile-radio (LMR) and 4G/5G cellular technologies already used by public safety. The recent evolution of public-safety devices suggest that a multi-network approach is more realistic now than it was several years ago, he said.

“We’re seeing now LMR devices that have LTE capabilities in the them, and they have Wi-Fi capabilities in them,” Devine said during today’s webinar. “So, we’re really seeing the opportunity for our first responders to have a deeper toolbox, with a number of connectivity options before them and the devices are agile enough to navigate across those opportunities.

“In the end, the first responder may have four or five or six different connectivity options, and they may all have their own imperfections. But there’s a degree of resiliency and redundancy in that effect. We really see that it’s a better experience for the responder to see Wi-Fi as an in-building capability.”

“I can envision a future where a responder has the ability to decide which connectivity solution is going to work best for them—this one, then this one, then this one—and to be able to build profiles within the interfaces of devices in order to do so for this particular scenario or that particular scenario, where they can manage the opportunistic capabilities of the device itself,” Devine said. “They’re less concerned about how it works; they just want it to work.”

All of the webinar speakers applauded the efforts of the Safer Buildings Coalition (SBC), which has focused attention on the in-building wireless-coverage challenges faced by first responders and the general public that must notify public-safety agencies when emergencies occur.

SBC board member Eric Toenjes said “when we can’t communicate, we’re less safe.” To this end, SBC has devoted considerable effort to helping develop fire codes and other regulations that are designed to improve in-building communications for first responders.

But the impact of such codes can be limited, which is why SBC supports the notion of public safety being able to bolster its in-building communications by leveraging Wi-Fi connectivity, Toenjes said.

“The reality is that enforcement of those codes—while it is gaining every day—is very scattered, is different

everywhere you go, and it is primarily aimed at the land mobile radio and making that work, which is great,” Toenjes said. “But we really believe today that an all-of-the-above strategy is what’s needed. If we don’t make multiple different types of networks function in a critical-communications way, then we’re missing a large percentage ... of buildings.

“I think we’ve accomplished a lot, as a group, but it’s still a small scratch on the surface of the number of buildings out there that really have coverage problems and communications issues that are going to rear their ugly head at some time. So the more technologies we can employ to try to solve for this—and I think Wi-Fi is an important part of that equation—the better chance we have that we can communicate in an emergency when we really need to.”

Howard Buzick, American Bandwidth’s senior vice president of business development, echoed this sentiment, noting that Wi-Fi connectivity can address in-building coverage issues relatively quickly and is more economically viable than many customized in-building solutions for LMR or cellular systems.

But existing Wi-Fi systems often do not provide coverage to all areas where public safety needs to communicate, according to Buzick.

“As we’ve been deploying this and realizing that it’s useful for critical communications, there still are gaps,” he said. “Wi-Fi in a school is deployed in classrooms and administrative offices, but not in stairwells, parking garages and things like that. I believe there is still an opportunity to densify and harden Wi-Fi networks for this purpose.”

“No one network is perfect, because everything is prone to failure at some point, so laying on Wi-Fi is fantastic,” Toenjes said. “What I want to caution against is, if we start to look at Wi-Fi as the primary connectivity methodology [for in-building wireless], then we need to look at our Wi-Fi networks differently.

“Someone earlier mentioned that Wi-Fi today is mission-critical-ready. Maybe it’s ready, but I don’t know that it’s done. If it becomes that primary connectivity path, we have to realize that our Wi-Fi networks are now a life-safety system, and that means that we need to address single points of failure, which largely [is not done] in Wi-Fi networks today. Is that Wi-Fi network connected to backup power source—like UPS or a generator—so, if there’s no power source, I don’t lose all of my communications?”

(Article originally posted on the Urgent Communications website by Donny Jackson, May 27, 2026)

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



Firewall Exploits Facilitate 9-1-1 Cyberattacks

Threat actors have exploited firewall vulnerabilities to compromise protected 9-1-1 call-taking systems and deploy ransomware. The Public Safety Threat Alliance (PSTA) Threat Intelligence team has identified multiple cyberattacks targeting 9-1-1 infrastructure within U.S. public safety organizations.

These incidents caused operational downtime, necessitating the emergency isolation of network segments to contain the threat. Observed attacks exclusively targeted law enforcement agencies by leveraging known firewall vulnerabilities.

Given the scale of the credential exposure, organizations should operate under the assumption of compromise. To mitigate the risk of unauthorized initial access, network administrators should immediately rotate all firewall and VPN credentials and mandate multi-factor authentication (MFA).

The sustained targeting of public-facing edge infrastructure mandates the im-

mediate remediation of all known firewall vulnerabilities. Adversaries are increasingly utilizing automated tools and AI to exploit these security gaps, making delayed patching a severe risk to network perimeter integrity.

Public safety organizations should conduct proactive network audits to identify and secure misconfigured services and unauthorized shadow IT.

Furthermore, end-of-life (EOL) hardware poses a significant initial access vector due to the lack of security updates; these devices must be decommissioned immediately. If removal is not feasible for mission-critical operations, they should be isolated using robust compensating controls.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager from the June 18, 2026 Public Safety Threat Alliance threat report)

**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>

**X: @ALMR_SOA
YouTube: www.youtube.com/**

ALMR Equipment

Currently, there are four aircraft radios, three base station/consolettes, twenty-three mobiles, and forty-one portables approved on the Alaska Land Mobile Radio (ALMR) system. There are multiple manufacturers approved on the system.

Each radio goes through extensive testing by the ALMR team before they are approved and certified for use on ALMR.