# ALMR INSIDER

Volume 19, Issue 2 April 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:**



## IWCE EXPO 2025

The International Wireless Communications Expo (IWCE) was held this year March 16-19 and brought together critical communications experts and speakers. Attendees experienced groundbreaking innovations, learned about existing and emerging technology solutions, and gained insights from industry leaders during expert led sessions and multiple networking events.

IWCE 2025 had over 5,000 attendees, over 300 speakers, 250 sponsors and exhibitors, with the first two days hosting training sessions focusing on first responders, government and enterprise, school and campus safety, transportation and logistics, and utilities. The keynote speaker on day three, before the expo hall opened was Clare Hopper, the Director of Commercial Satellite Communications Office, assigned to the Space Systems Command, United States' Space Force.

Members from the ALMR help desk, Operations management office and personnel from the Alaska Public safety Communications Services (APSCS) attended IWCE in a coordinated effort to maximize the experience and to meet with as many vendors as possible.

As the Operations Manager, I met with several radio vendors to see what their latest products were and if they would be viable options to have tested for the ALMR system. It is imperative we maintain close working relationships with radio companies to conduct testing for our members and because of IWCE, I am working with a vendor to test some of their radios, in the coming months.

One of the sessions held was from the State of Connecticut pertaining to LMR encryption and P25 compliance. They have begun to expand their interoperability with help from their Statewide Interoperability Coordinator (SWIC). They work with the National Law Enforcement Communication Center (NLECC) to create talkshare agreements, AES256 encryption, hex keys and their KMF. ALMR has been using these systems since the beginning and it was encouraging to see other states are adopting the same construction for their systems.

Motorola's SmartConnect recently received Federal Risk and Authorization Management Program (FedRAMP) approval. I attended a seminar on how we can use it to our advantage. SmartConnect provides a way for specific radios to connect to ALMR through Wi-Fi and LTE service when they are outside of the ALMR coverage area. As sensitive information and mission-critical data are increasingly stored and managed in the cloud, FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. As ALMR develops critical communication solutions, FedRAMP not only ensures compliance with federal standards but also builds trust and provides assurances to our members that data and communication channels are secure.

During the time the expo floor was open we visited with the majority of the vendors and discussed with them possible testing of their equipment to see if it would be better suited for ALMR or the SATS system. This included ALMR tower lights, shelters, generators, towers, routers, monitoring systems, and HVAC. Being able to make these connections in person instead of online or over the phone is imperative for close working relationships.

I encourage any agency that works on or maintains an LMR system to attend the IWCE at least once to gain additional insight to what is available on the market, new trends, training options, and equipment.

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

## ALMR Microwave Backhaul (SATS)

The State of Alaska Telecommunications System (SATS) is the backbone network in which ALMR operates. The network is a multi-protocol wide area network built using public safety grade equipment. The network primarily uses microwave connections to connect tower sites and other facilities (e.g. dispatch centers) to the ALMR core equipment.

SATS includes much of the physical infrastructure required for ALMR to operate such as towers, equipment shelters, generators, HVAC, and other needs. In addition to ALMR, the system carries other two-way radio traffic in areas not served by ALMR, highway call boxes, aviation cameras, railroad communications, seismic data, utility systems control and monitoring data, television and public broadcasting data, and other uses that are related to public safety services.

The backhaul represents a key component of most LMR systems and is usually where your radio network and your IP network come together. Without SATS, ALMR would not work and agencies would only be able to talk to each other locally and the benefits of dispatched served, wide-area communications would be lost. The SATS system does come at a cost. It is not only important to build and maintain a public safety grade system but it is imperative agencies budget for yearly maintenance cost. The SATS infrastructure is not a build it and forget it system. Many sites are on the tops of mountains with over 50 locations being helicopter access only, requiring large expenditures for preventive maintenance and repairs. The infrastructure owners must adequately resource their sites in their budgets to avoid a systemwide failure impacting all services.

The systems are designed with redundancies to fail-over and recover so quickly that when something goes wrong, those errors are not generally noticed by the radio system operator or owner. Prior to this technology, there were frequent outages impacting multiple sites and services throughout the system. Without those visible outages, we must be careful to avoid mistakenly thinking that if it works, why should we allocate additional resources? SATS has experienced several millions of dollars in cuts over the past decade. Those reductions increase the risk of failures.

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

## Public Safety Agencies are Targeted by "Ghost" Ransomware Attacks

An alert from the Cybersecurity and Infrastructure Security Agency and the FBI said threat actors known as "Ghost" are conducting ransomware attacks on multiple targets in more than 70 countries. Believed to be working out of China, the group goes by many names, including Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada and Rapture.

The group doesn't typically use phishing techniques, a common scammer method that involves impersonating a legitimate source to prompt someone to click on a phony link or provide personal information. Instead, Ghost uses publicly available code to exploit security vulnerabilities in software and firmware that have not been corrected. The group does this to gain access to Internet-facing servers and strike with ransomware payloads.

"Beginning early 2021, Ghost actors began attacking victims whose Internet facing services ran outdated versions of software and firmware for financial gain. Affected victims include critical infrastructure, schools and universities, healthcare, government networks, religious institutions, technology and manufacturing companies, and numerous small- and medium-sized businesses."

Some of the ransomware files Ghost used during the attacks were Cring.exe, Ghost.exe, ElysiumO.exe, and Locker.exe.

To prevent the attacks, the FBI advises to maintain regular system backups. "Ghost ransomware victims whose backups were unaffected by the ransomware attack were often able to restore operations without needing to contact Ghost actors or pay a ransom," the FBI alert noted.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from the Government Technology February 24, 2025 website article by Leada Gore)

## What is the Average Downtime after a Ransomware Attack?

Security researchers have determined just how costly ransomware attacks can be for public entities. The team tracked 1,133 confirmed ransomware attacks on government agencies between 2018 and 2024 and analyzed the data. They found that on average, a ransomware attack on a government entity resulted in nearly a month of downtime — 27.8 days, to be exact.

And that downtime doesn't come cheap. The average cost of each day an agency was out of commission due to a ransomware attack was $83,600. They estimate that downtime alone for all the tracked attacks cost public-sector entities roughly $2.2 billion.

They also found that while government entities typically take longer to recover from ransomware attacks, this downtime doesn't cost them as much as other sectors. Health-care companies suffer an average of 16 days of downtime from ransomware attacks, but each of those days costs them about $900,000.

(Article prepared by Mr. Paul Fussey, with excerpts taken from the Government Technology March 20, 2025 website)

## Land Mobile Radio Reliability and Network

Public safety LMR systems typically are designed to deliver uptime of 99.999 percent per the National Public Safety Telecommunications Council (NPSTC).

Ensuring consistent and uninterrupted communication during both routine and emergency operations is of paramount importance. Robustness of the backhaul that connects radio sites and core systems is a key factor — backhaul failures are a significant point of vulnerability for many LMR systems, particularly when relying on third-party providers for connectivity.

Redundancy in core infrastructure components, e.g., zone controllers, prime sites, and master sites is another key factor, especially given the uptick in devastating natural disasters like hurricanes, floods, tornados, and wildfires. A significant number of public-safety radio systems do not have redundant controllers, meaning that a failure of the prime site controller can lead to severe service outages.

Given the critical importance of redundancy and the plethora of threats to it, many public-safety agencies are ramping up their efforts. This includes enhancing backhaul redundancy through diverse routing and alternative topologies — for example, ring or mesh configurations — ensuring adequate power supplies with well-maintained backup generators, fuel storage, and adopting physical and geographic redundancy to eliminate single points of failure.

Additionally, automated failover systems with geographic redundancy are becoming more common. They are designed to ensure that when a component of the LMR network fails, the system automatically switches to a backup without requiring manual intervention. This type of redundancy is becoming a necessary feature for maintaining reliability, especially during off-hours when personnel may not be immediately available.

The network should be able to communicate with disparate systems inside and outside the jurisdiction. Ideally, this is accomplished natively, for example, when two systems both comply with the P25 standards, but it also can be accomplished via patches, interfaces, gateways, and equipment caches.

Interoperability continues to be achieved natively, i.e., when two or more LMR systems are P25 compliant, but also via interfaces (e.g. the Inter-RF Subsystem Interface, which is a P25 element) and patches (console and field), which are effective, but take significant time and effort to implement.

While FirstNet, which is being built in partnership with AT&T, initially was thought to be the answer to nationwide interoperability, it hasn't panned out. However, mission-critical push-to-talk (MCPTT) has advanced, as has the idea of implementing some LMR infrastructure in the cloud.

FirstNet originally was envisioned as a nationwide solution to provide interoperability through broadband communications. However, LMR systems are still predominant. Further, Verizon and T-Mobile have also launched public-safety broadband offerings, which means a single unified, nationwide broadband network, and the resultant native interoperability, is unlikely. However, while more MCPTT-compliant applications that can communicate across different platforms are emerging, they are still extremely limited and have not yet altered the communications landscape. Finally, some solutions have emerged that aim to improve interoperability by hosting ISSI in the cloud. While this offers flexibility and scalability, it is seen as only one small part of the broader interoperability picture and hasn't led to widespread change—yet.

While these advancements and more are transforming emergency responses by enhancing situational awareness, operational efficiency, and resource allocation, there are several counterbalances to consider. One significant challenge is the limited number of vendors in the LMR space, leading to dependency on a small group of suppliers, which stifles competition, and limits the ability of agencies to switch vendors without significant financial investments.

The increased reliance on commercial cellular networks also presents challenges. While cellular networks provide excellent data capacity, they are not as tightly controlled by public-safety agencies as are LMR networks. Time continues to prove that purpose-built LMR networks outperform cellular networks for voice communications in terms of coverage and reliability.

In addition to the advantages described earlier, multimode radios can switch to a cellular network where LMR system coverage is weak or unavailable and provide a stable communications path by intelligently determining the best network to use based on signal strength.

Radios equipped with LTE modems can transmit real-time GPS information over the cellular network, providing incident commanders with accurate locations of all personnel, which is particularly useful in dynamic or large-scale incidents where knowing the position of responders is critical for effective coordination.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from the 2025 State of the Industry Report by Mission Critical Partners)

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

## ALMR Policies, Procedures and Other Documents

Did you know that every ALMR policy, procedure, plan, and strategic document, plus definitions and acronyms commonly used by ALMR, are located on the ALMR website https://alaskalandmobileradio.org/ under the heading "About ALMR?"

Each document undergoes an annual review, which is scheduled for different times throughout the year, by the document specialist. During the review, the documents will be checked for any grammatical or spelling errors; updates to definitions, acronyms, charts, etc. will be added; and references to government documents or articles will be checked and updated, if necessary, as well. These reviews are performed to ensure that all the information contained within the policies, procedures, plans, strategic documents are current and relevant for daily or emergency operations.

Once the document specialist is done with their review and updates, have been completed, if required, the document is then reviewed by the operations manager. Some documents require that they also be reviewed by the systems manager, security manager, Department of Defense, and/or the Alaska Public Safety Communications Service manager. If any substantial revisions are made, then the document must be presented to the User Council for their approval.

All documents play a vital role and serve as the foundation of ALMR. They also provide the guiding principles for the management and operation of ALMR is managed and operated. All ALMR members are encouraged to read and review the policy and procedures to ensure they are complying with the governing documents.

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

**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 Reliability

The ALMR RF equipment, zone controllers, SATS system, communications transport network and other infrastructure are required to have an uptime of at least 99.999%. This is documented in the service level agreement policy and ALMR strives to meet this for all of our members.

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