ALMR INSIDER

Volume 18, Issue 1 January 15, 2024

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:

2023 - A Year in Review

The ALMR team worked extremely hard last year on the system-wide upgrade to TDMA and Smart Connect capabilities in preparation for the 2026 transition date.

One of the main questions the ALMR team received was when would ALMR get FedRAMP approval. This was not an easy question to answer, even for our Information Systems Security Manager (ISSM) who had been working diligently with our Federal sponsors to acquire approval. The ISSM confirmed ALMR would not receive approval until after the first quarter of 2024, which was disappointing to the ALMR team and many of our members since we were told we would have approval before the end of 2023 by both FedRAMP and Motorola.

In preparation, the GTR units at the radio frequency (RF) sites for Zones 1 and 2 had been upgraded and optimized with the latest software. A GTR is a single or double rack-mounted base radio that supports P25 FDMA and TDMA trunking operations for large regional systems. This upgrade enhanced radio communications and connectivity across the entire system and the logistics to complete this project was a large undertaking due to the ALMR and Motorola teams having to travel around the state to reach all of the sites, either by vehicle or by helicopter.

While the teams were at the RF sites, they upgraded the antenna brackets and stiff arm supports needed to protect the antennas from high winds and heavy snow loads, and they changed the antennas from Telewave to either Alive or DBSpectra. The antenna upgrade increased the forward gain of the sites and increased radio coverage by removing old equipment from the towers and by raising some antennas to the top of the towers. Many of the ALMR towers are over 100 feet tall, which takes nerves of steel from the ALMR technicians to complete their work.

At the Zone 1 Master Site, the Genesis system was upgraded. Genesis is the main monitoring software for the ALMR system. The upgrades included the ability to not only see radio traffic in real time but also instantly see if radios are transmitting in FDMA or TDMA. The ability to see if radios are transmitting in FDMA will help the ALMR team answer questions from our members, who have asked for this technology at past User Council meetings. Another feature of this upgrade will provide the ability to see how many radios are affiliated with each tower and if the system is reaching capacity at individual sites.

Zone 1 and 2 Master Sites also received multiple upgrades last year without any interruptions to agencies. The dynamic transcoders were upgraded, which improved interoperability between agencies and organizations, and the VMS servers were upgraded to a newer model. In anticipation of FedRAMP approval, the Master Sites received new cloud-connect servers and location on push to talk (LoPTT) servers, which will allow agencies to see the exact location of their radios on the system.

To improve the protection of the system from cybersecurity threats, the Master Sites received new Edge routers, new Key Management Facility (KMF) servers, and Zone Core Protection (ZCP) firewalls. The Edge routers and ZCP firewalls are required when the FedRAMP authority is received in order to access the new connectivity systems.

The ALMR team looks forward to installing new Juniper routers at the RF sites starting in the second quarter of 2024 and would like to thank everyone for their patience this past year as the upgrades were installed. We will continue to conduct normal periodic maintenance inspections (PMIs) to ensure operability for all our members.

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

Available ALMR Training

The Operations Management Office provides training for user agencies on policies, procedures, and best practices for the ALMR system. Generally, we provide training for users in two ways: videos/references posted to our website and live-training events several times a year which provide for direct interaction with users. These events are announced in advance and, like all training, are recorded and posted on our website for later review.

Our video vignettes are designed to be short, topical videos of interest to users, with most videos being only five to eight minutes in length. We regularly add new videos under the "Training" menu on the website. There are several topics available relating to the on-going ALMR system upgrade, including what TDMA is, the new technology that the system is transitioning to, as well as a video reviewing how the upgrade will affect individual users/agencies.

In addition to technical subjects, we cover administrative responsibilities for all agencies including inventory maintenance, talkgroup sharing agreements, and other basic tasks that are required to ensure accurate information within the system and accountability for subscriber units and other equipment.

Similar to our topical videos, the "Presentation" section includes longer recordings, including those of our recent town hall meetings, hands-on radio training, training for dispatchers, and many longer-form presentations.

We are always seeking feedback and ideas for future training. Most ALMR training is somewhat generic due to the fact that different agencies use different subscriber units, different programing, and have varied use cases. However, we welcome ideas on all subjects that will be of benefit to agencies across the state.

While not specifically related to training on the ALMR system, we record training presentations from various vendors that may provide information on new technologies and offerings to our members.

If you have questions on any training topic raised and how it will affect your agency, please reach out to our staff for assistance with your specific situation. To submit training ideas, visit the ALMR website and select the "Request Training" option under the "Training" menu.

(Article prepared by Mr. Dan Nelson, ALMR Training Coordinator)

Protect Your Radio Systems and Computers from Hackers

What were the worst passwords of 2023? If you guessed "123456," congratulations, you are as fast as a computer at cracking the most common password of 2023. Equal points if you also guessed "password," which was number two in the U.S. and just as easy to crack.

If you crunched the numbers from across 35 countries for the most common (and worst) passwords of the last year, the top ten should honestly surprise absolutely no one. In third and fourth place were "12345678" and "123456789," because of course just adding the next number in the sequence is something no one would predict. You could really mix it up and take out some numbers to get the top fifth and sixth passwords: "1234" and "12345," respectively.

The remaining top ten are all of the same variety and took less than one second to crack. Then there is an outlier at number 11, "UNKNOWN," which took 17 minutes to crack. That is impressive considering the rest of the top 20 were easily cracked in 11 seconds or less. If any of your passwords look like anything from this list, this is your wake-up call.

When creating a strong password to protect your system and computers, some things to avoid are four-digit years, keyboard patterns or sequences, names, personal information, or any variation of the word "password." A strong password will have ten or more characters, a number, a symbol, and upper and lowercase characters. Passphrases are longer and more complex than passwords and are easier to remember but more difficult to guess.

A strong password is our first line of defense to protect our radio system and infrastructure.

(Article by Mr. Paul Fussey, ALMR Operations Manager, with excerpts from the Government Technology article, November 17, 2023)

DOD Upgrades Critical Microwave Hops

In 2023, the Department of Defense (DOD) upgraded several of their microwave hops. Those were Clear to Kobe, Birch Hill to Quarry Hill, Fort Greely to Delta, and R1 North to Alcantra.

These upgrades, which are part of a system lifecycle refresh, occurred from August to November, and strengthened the microwave backhaul for the ALMR system. The work completed included new tower surveys for stability and weight loads, upgraded CTR8000 routers, and new antennas and brackets. While the majority of work completed was in 2023, there is still some minor follow-up work to complete this coming summer before the transition to TDMA.

The benefits of this project for the end users are more robust connectivity, fewer busies, and improved interoperability for DOD and other agencies during a disaster or day-to-day operations. As a DOD/State-led system, joint upgrade projects will run concurrently to maximize the use of all available assets.

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

The Scariest Cybersecurity Trends Impacting the Public Sector

A recent article examined two of the scariest cybersecurity trends currently impacting public-sector organizations and their networks and systems.

One concern is the fact that public-sector organizations only recently have started to understand the severity of the cybersecurity problem. Another concern is the fact that such organizations generally fail to adhere to, or even acknowledge the existence of, longstanding cybersecurity recommendations. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) have worked collaboratively with their counterparts in Europe and Australia for years to ensure that public-sector organizations are well informed regarding emerging threats and the best strategies and tactics for mitigating them. In this article, we delve into the third, fourth, and fifth scariest trends.

Scariest Trend No. 3 — Cyberattackers keep getting better at what they do.

Cyberattackers constantly evolve their strategies and tactics, seemingly at warp speed. For example, they are employing increasingly sophisticated, automated software tools that leverage algorithms to identify millions of network, system, and device vulnerabilities every second.

A corollary factor contributing to this trend is the fact that it is extremely difficult for developers to create software that is vulnerability free. This is the reason that patches are continually issued. Now consider that the software utilized by public-sector organizations interconnects to all manners of software employed by dozens, even hundreds, of other organizations, and each piece of software contains its own intrinsic vulnerabilities. It is easy to imagine a cyberattacker exploiting a vulnerability discovered in another organization's software and then worming their way into your organization's software, which in turn enables them to attack every connected network, system, and device.

Another factor is that, in most countries, cyberattacks are not considered crimes. The philosophy seems to be, "shame on you for not having the proper protections in place." The result is that cyberattackers outside the United States operate with virtual impunity.

For all these reasons and more, cybersecurity fraud is the third largest economy in the world and will only get bigger. It is the proverbial monster under the bed that keeps every cybersecurity professional working in the public sector up at night — or at least it should.

Scariest Trend No. 4 — Not enough cybersecurity experts to go around.

Nearly all public-sector organizations are dealing with an acute staffing shortage across the entire enterprise. This includes information technology (IT) and cybersecurity personnel. It should be noted that not every IT professional has the experience and expertise required to work in the cybersecurity realm. Indeed, cybersecurity professionals possess very specific skill sets, which make it more difficult to recruit, hire, and retain them. Because their skill sets are so specialized, cybersecurity professionals tend to require compensation that puts them out of reach of many public-sector organizations, especially if they are competing with private-sector organizations that have deeper pockets.

A related factor is that smaller municipalities and counties often share cybersecurity personnel across multiple agencies. The result is that personnel typically are spread very thin, so much so that they find it exceedingly difficult, if not impossible, to execute even the most basic elements of a cybersecurity program for a single agency, much less all of them, and to keep pace with constantly evolving threat vectors.

Scariest Trend No. 5 — LMR systems are just as vulnerable as every other system.

This is a trend that primarily affects public-safety agencies, which rely extensively on two-way voice communications during emergency response. In fact, it has been said, with some justification, that the most vital tool that law-enforcement officers and fire/rescue personnel carry is their land mobile radio (LMR). In the past, LMR systems, whether analog or digital, have been isolated, standalone, self-contained, and not connected to the internet, which generally meant that no pathway existed for cyberattackers to infiltrate them.

Unfortunately, however, a plethora of vulnerabilities exist that increase the risk profile for LMR systems exponentially. This is true even for Project 25 (P25) systems, despite the existence of certain protections that are baked into the standard, such as encryption, use of multiple frequencies, and a feature called "radio inhibit," which enables system managers to identify a rogue radio and essentially turn it into a brick.

Arguably, the greatest vulnerability is that the systems used by public-safety agencies to backhaul radio traffic from the tower(s) to the facility leverage the Internet Protocol (IP), which has inherent security flaws — ergo, IP-based networks and systems are intrinsically vulnerable to cyberattacks.

The reality is that most public-safety agencies tend to think of their LMR systems in terms of radio frequencies and not IP, thus, they fail to grasp the criticality of this vulnerability. A corollary factor is that backhaul systems often are shared by public-safety agencies with other entities — and each of them has its own vulnerabilities. The result is a dramatically diminished cybersecurity posture for all concerned.

Cybersecurity is a big, messy problem that will get bigger and messier as time passes.

(Article from Mission Critical Partners Monthly Newsletter, posted September 19, 2023, by Jason Franks)

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

A Fond Farewell

It's hard to know what to say when it's time to go. I'm not one to make a big deal about myself, so writing a farewell article is something I almost did not do.

Long before ALMR, when I was still in the Air Force, I helped the ALCOM J6 office prepare the surveys that were sent to Federal agencies to gauge their interest in having an Alaska-wide radio system. Who would have thought this is where I'd be over 20 years later.

When I started with ALMR as it was being stood up, I worked in the Project Management Office. There were contracts to manage and councils to establish with the new cooperative State and local partners and not just Federal agencies, as before. Along with all of this came putting together an office for the staff to work in. There was also the site build out which was completed in phases with both the State and the Department of Defense building sites simultaneously. Teams were traveling to site locations to take pictures and produce drawings and perform coverage projections. Other teams were preparing system design and implementation documents and holding weekly meetings to review work breakdown structures to ensure each individual site project remained on schedule. It was controlled chaos most days.

After the project phase was completed, the Operations Management Office was stood up and now, five Operations Managers and 16 1/2 years later, it is time for me to close out my own file. As one of the last of the "old guard," it is time for some new blood to come in and make their own mark.

Will I miss ALMR? Of course! It's been a pleasure to work with and fight for a system I truly believe in.

I hope I was able to make a difference, and I want to thank everyone who has supported me throughout the years. I wish you all the best as I transition into retirement.

(Ms. Sherry Shafer, ALMR Documentation 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

2023 ALMR End-of-Year Statistics

Member Agencies: 134

Subscribers: 25,810
(9,729 TDMA/16,081 non-TDMA)

*Group and Individual Calls:
18,036,066

*Push to Talks: 29,582,880

*Busies/Percentage rate of calls:
7,209/.0003

(*Totals are cumulative)