ALMR INSIDER

Volume 18, Issue 2 April 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

International Wireless Communication Expo 2024

The International Wireless Communication Expo (IWCE) was held in Orlando from March 25-29 this year and once again provided outstanding training, seminars, guest speakers, and networking opportunities the ALMR and APSCS teams are unable to achieve in Alaska.

The IWCE is one of the largest communications events in the country with five main sponsors, over 260 exhibitors and manufacturers covering everything from radios, system software, tower lights, and equipment shelters, nine media partners, and over 3,800 registered attendees.

The sessions schedule typically would run all day from 8:00 a.m. to 5:30 p.m. with training being conducted in 1/2 hour to a full hour increment, depending on the subject and amount of questions being asked. Mr. Dan Nelson, the ALMR training coordinator gave a presentation on exercise communications at the request of the IWCE board.

The keynote speakers this year brought a wealth of knowledge and experience to the expo and reinforced their commitment to the public safety community. The Federal Communications Commissioner, Anna M. Gomez, discussed her organization's regulatory priorities, and their latest efforts to support critical communications.

Verizon's Vice President, Cory Davis and Hawaii's Deputy Chief of Emergency Management, Ryan Hirae discussed their coordinated response to the devastating fires in Lahaina and lessons learned from this tragedy.

Deputy Director Nitin Natarajan, of CISA, discussed the threats facing our emergency communications response operations and how we can be vigilant and report critical infrastructure threats. He focused on identifying federal resources that can help our individual agencies.

The final keynote speaker was a panel consisting of several fire chiefs from around the country with Chief John Butler of the Fairfax County (VA) fire department and the current president of the International Association of Fire Chiefs. The panel focused on location based services, improving firefighter effectiveness and safety and new technology in communications to enhance situational awareness.

Throughout the expo there were two major topics discussed in the seminars and highlighted by exhibiters on the showroom floor. The first was the installation of Bi-directional amplifiers (BDA) and distributed antenna systems (DAS) in buildings. Under the authority of NFPA 1221, 1225, IFC 510, and UL2524, many fire inspectors are requiring either a BDA or DAS system to be installed large buildings; however, this has created several issues. The first is the importance of following FCC rules when installing these systems to eliminate interference issues experienced by licensees. The other issue with installing a BDA or DAS is the proper documentation of the system prior to system construction.

The other major issue discussed at IWCE was the FCC adopting standards that allow for the use of Wi-Fi in the 6GHz band. The majority of public safety point-to-point microwave systems use 6GHZ. It is the most common microwave band and the premise for this rule change was that Wi-Fi 6 systems are only authorized for indoor use. This is such a major concern for the FCC and APCO they have created a webpage and QR code to report any 6GHZ interferences.

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

Inside this issue:

Band Plan Management

The Alaska Land Mobile Radio (ALMR) system is moving to a Time Division Multiple Access (TDMA) configuration effective December 31, 2026. As our members acquire new radios that are programmed and configured for TDMA, it is imperative the radios have a proper band plan configured or they will not work on the system or in TDMA.

The band plan elements in use on the system must be configured identically in the subscriber radios and in the infrastructure. Any mismatch can result in missed calls or lost audio. Problems caused by a mismatched band plan can be very time consuming and difficult to solve. Subscriber radios do not learn the band plan that is in use by the system via control channel messages but by physically configuring the information in the radio.

The frequency band plan provides radios the parameters needed to translate the channel number in a call grant to the actual TX and RX frequencies for the assigned channel. A maximum of 16 possible band plan elements may be used and are common to all the ALMR sites and are used to identify the RF frequencies that may be used.

The first step in the process is to open the radio programming software and proceed to the P25 trunking channel ID page and look at the system/channel type, either TDMA or FDMA, the channel spacing, either 12.500 or 6.250 KHz, and the transmit offset in MHz. Ultimately, the band plan in the radio must match what is in the system.

There are two numbers associated with each TX/RX frequency and to clarify you have the correct information in your radio you always start with the TX frequency and +/- the transmit offset MHz, which will give you your RX frequency.

If the TX and RX frequencies are not calculated correctly a subscriber radio may only hear radio traffic but not transmit any audio due to having the wrong frequency, and if the channel/system type is not accurate, the radio will only transmit in FDMA, even if it comes TDMA capable. We recommend all ALMR users work with their radio suppliers and programmers to make sure they are accurately configured for correct use or contact the ALMR Help Desk.

(Article by Mr. Paul Fussey, ALMR Operations Manager, with excerpts from the Fleetmapping and Band Plan management Feature Guide, November 2021 edition)

2024 Emergency Management Conference

The Alaska Division of Homeland Security and Emergency Management (DHS&EM) put on another successful Emergency Management conference in downtown Anchorage, April 9-11, with the local emergency planning committees and the State Emergency Response Commission meeting on the 12th.

The conference had vendors for the first time and over 300 individuals attended the three day event for community networking, skill building, and to attend multiple workshops. I was asked to give a presentation on the Alaska Land Mobile Radio (ALMR) system on how it is used across the state by agencies and how it contributes to interoperability during disasters. My one hour session was attended by 69 people from varied backgrounds and agencies across the state.

I encourage all ALMR members to attend this conference as it is a unique opportunity to meet with other public safety entities and emergency managers face to face in a calm setting and not during an emergency situation. These connections are vital for our communities and agencies. The ALMR operations management office works hard to create and maintain working relationships across the state and conferences, such as this one put on by DHS&EM are perfect segways for this to happen.

Some of the topics covered during the conference were ALMR, FEMA individual assistance, Cyber risk mitigation, managing food emergencies, evacuation preparedness, Division of forestry and fire protection, and the USCG.

For more information on this conference and other training opportunities being developed and offered by DHS&EM contact Emergency Management Specialist III, Michelle Torres by email michelle.torres@alaska.gov.

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

CISA Updates Cyber Toolkit

The United States Cybersecurity and Infrastructure Security Agency (CISA) released an updated toolkit for public-safety defenders. The toolkit is designed to help defenders evaluate current cyber resiliency, improve that resiliency, and develop strategies to reduce the likelihood and impact of attacks.

The toolkit is an interactive graphic which contains multiple topics and resources. This includes sections on technologies such as Land Mobile Radio (LMR) and Next Generation 9-1-1 (NG9-1-1) as well as broader categories such as ‘Cyber Incidents’ and ‘Ransomware.’

The toolkit is meant to be a “living document” and is intended to grow as new strategies become available. Public-safety defenders are encouraged to review the toolkit as new resources and sections are added to protect against a ransomware attack against a law enforcement or dispatch network. By establishing resiliency measures, public safety communications can better withstand potential disruption to services.

(Article by Mr. Paul Fussey, ALMR Operations Manager, with excerpts from the 27 February—12 March 2024 PSTA Cyberbytes and CISA.gov)

911 Professionals and Telecommunication Technology

Technology is changing the game in public safety telecommunications. The landscape has evolved exponentially since I began my career in public safety telecommunications in 1990 and particularly over the last decade. The needs and expectations of the public and emergency field responders served by us have evolved as well. Never would I have imagined having the tools to streamline data sharing, enhance real-time communications with video, and improve situational awareness with cutting edge technology advancements. We, at the Soldotna Public Safety Communications Center (SPSCC), have joined the ranks of countless agencies across the United States benefitting from implementing these innovative solutions.

Over the last year, SPSCC began using text-to-911 technology as well as cloud-based software that allows our 911 professionals to initiate live stream video and photos with on-scene callers, providing us the ability to glean valuable information about the emergency. Additionally, 911 professionals can share this data with emergency responders, providing them with relevant details to identify the location of calls for service, ensure the safety of responding units, and allow EMS and fire responders the ability to "size up" a scene before they arrive. This functionality helps public safety as a whole to assist in making informed decisions regarding the level of response and resources needed. We have used this technology across all disciplines—law Enforcement, EMS, fire and other calls for service

In spite of the technological advances in the public safety telecommunications profession, the core duties remain the same. Each moment of a 911 professional's shift is unknown. With each ring of 911 there could be a child screaming for help; an elderly male who woke to find his wife passed away in her sleep; an irate driver stuck in traffic because a mile ahead someone has been killed in an accident the driver can't see; or a multitude of other emergency calls for service. We provide services to people who are in life and death circumstances, the outcomes of which are unpredictable.

As stated above, public safety telecommunications is an ever-changing profession with new and exciting technologies and opportunities happening all the time. This is the way of the future, and we must prepare as we lean into the next generation of technology. It is imperative that 911 professionals, their leadership, joined by other 911 stakeholders share responsibility for 911 professional's health and performance. Success can be optimally achieved if stakeholders rally the same level of dedication to public safety telecommunications that has produced extraordinary technological advances in the industry since the first 911 call made in 1968.

(Article by Mrs. Tammy Goggia-Cockrell, ENP, 911 Emergency Communications Coordinator, Soldotna Public Safety Communications Center)

Protecting Your Information on the Cloud

As more companies and public safety entities move their files and documents to the cloud to streamline information sharing they must protect themselves from cyber attacks.

The new global report captured how trends in cyber attacks evolved in 2023 and are likely to keep evolving throughout 2024. Nationally, there was a 75 percent increase in intrusions in the cloud environments from 2022 to 2023, although not all of these were deliberate. Some of these cases involved actors who appeared either unaware that they had compromised a cloud environment or which otherwise "did not take advantage of cloud features."

Threat actors are also increasingly taking advantage of the cloud and security information stored on it. In some cases, attackers move between cloud and on-premise environments. For example, Scattered Spider, the group known for attacking the MGM hotel sometimes looks to get access to a targets Microsoft 365 environment, then searches SharePoint online to find VPN setup instructions. With that, the group can log into the victim's VPN and travel laterally to its on-premise servers. Another group was seen deleting the victim's cloud-based files.

By gaining access to files on the cloud, more cyber extortionists are stealing data and threatening to leak it unless they are paid, without bothering to deploy ransomware malware. This method is expected to ramp up in 2024, even as malware-based ransom extortion remains significant.

Public-safety entities should refrain from storing all of their files on one system to reduce the chance of losing all of their documents from a cyber attack. Backup files must be maintained on secure servers, so if an entity becomes a victim, they can quickly restore their systems.

As organizations look to defend themselves and their cloud-based files, they can take various steps. Some of those include adopting a phishing-resistant multifactor authentication, training teams about social engineering methods, and taking steps to get better visibility into their cloud environments, including catching and correcting any misconfigurations.

(Article by Mr. Paul Fussey, ALMR Operations Manager, with excerpts from the Government Technology Cybersecurity report from February 22, 2024)

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

ALMR Supports Military Training Exercise

One of the largest military training exercises in Alaska took place near Fort Greely this winter. Joint Pacific Multinational Readiness Center-Alaska 24-02 occurred from February 8-22, with more than 10,000 soldiers, marines, airmen, and Canadian military conducting operations to include airborne assault training, combat maneuvers, and convoy operations.

With such a large influx of personnel into an area with an anticipated jump in radio traffic and push to talks (PTT), the ALMR team used this exercise to see how the ALMR system can sustain and support the military.

The ALMR towers monitored were Donnelly Dome, Fort Greely, Birch Hill VHF, Independent Ridge, and Canyon Creek, which all saw a significant jump in radio traffic due to the exercise.

The total affiliated talk groups in January were 779,552 compared to 811,364 in February for an increase of 31,812, which is a larger jump than normal for day-to-day operations.

The main concern for the ALMR team was radio busies, and after the exercise the total for the five towers was 2,068, with Donnelly Dome having 1,011 and Fort Greely having the second largest at 249 with the remaining towers in single digits. When these numbers are combined with the rest of the system data, the percentage of busies for the month of February was only .0008%.

This exercise and the performance of the ALMR system proves, once again, the DOD and the public-safety sector of Alaska can depend on ALMR to provide them with constant and adequate radio coverage. As a joint State and DOD system, everyone benefits from the use of such a robust interoperable network.

(Article 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

Zone Controller Rollover

The quarterly zone controller rollovers were conducted on February 27 & 28. Rollovers are used to install security and operating system patches to the master sites in all zones.

The process takes place during the early hours to minimize disruptions in radio traffic. All dispatch centers are contacted before and after the process.