ALMR INSIDER

Volume 17, Issue 3 July 15, 2023

ALMR Help Desk

In Anchorage: 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:

TDMA - Required Radio Features and Testing

This summer extensive work is being conducted to upgrade the system, to include antennas, routers, and transcoders in order to transition from frequency division multiple access (FDMA) to time division multiple access (TDMA). With FDMA radios no longer allowed to be added on the system, and all radios needing to be TDMA capable by December 2026, now is the time for members to upgrade their radios and make sure they have the required functions and capabilities to take advantage of the new upgrades.

The ALMR team routinely updates the approved equipment list on the web site which specifies which radios are TDMA capable. Every approved radio goes through a rigorous acceptance test procedure (ATP), which includes 33 separate function tests. This is done so our members can be confident the radios they are purchasing will work on the system and eliminate possible future issues.

There are several required features for newly added radios. The first is Phase 2 TDMA capability. It is highly recommended by the ALMR team that purchased radios not only be TDMA capable, but that they come already programmed when purchased. This will eliminate having to have the radios flash programmed and upgraded to TDMA enabled, to which agencies will incur an additional charge. Because new radios are required to have TDMA, this automatically adds two more requirements, which are the improved multi-band excitation (IMBE) and the Association of Public-Safety Communications Officials (APCO) P25 packet data. These two programs are the voice coding standards for several communication systems and provide superior speech quality. Additionally, because ALMR is a trunked system which uses a control channel to automatically assign frequency channels to groups of user radios, all radios must have the P25 9600 BAUD trunking option. Lastly, the advanced encryption standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) and is required to be on all radios on the ALMR system for security purposes.

A highly recommended feature is over the air rekeying (OTAR). This is extremely helpful for members who have personnel scattered in different areas and eliminates the need to physically touch the radios when they lose their programming. A simple OTAR process re-establishes the code plug to the radio through the use of ALMR towers. Many radios have Bluetooth and Wi-Fi options, and some members have provided feedback on the ease of use when using Bluetooth-capable lapel microphones. Most radios come with a programmable emergency button, but not all users have them activated, and the ALMR team recommends members familiarize themselves with the ALMR Subscriber Emergency Button Activation Policy and Procedure 300-7 before programming and using this feature.

When all the upgrades are completed, other new features should become available such as over-the-air programming (OTAP). This allows the ability to reprogram radios through the ALMR system without the need to connect physically to a radio. GPS and location on push-to-talk (LoPTT) will allow individuals to send their location via their radios to dispatch. This will increase safety for member organizations and units when they are requesting help or assistance. The GPS and LoPTT radios will be available after ALMR receives FedRamp approval and will require a GPS capable antenna.

Please contact the ALMR offices if you have questions.

(Article prepared by Paul Fussey with excerpts from the ALMR website, APCO International website, and ICTAP P25 features matrix.)

PACEing a Communications Resilience Plan

On the night of January 10, 2023, the Federal Aviation Administration's Notice to Air Missions (NOTAM) system, which communicates real-time hazards to pilots and airports, failed for an unknown reason. The backup communications provided critical updates to pilots but were insufficient to sustain operations. By morning, operations had to cease for two hours while they located and fixed the problem. In the meantime, 1,300 flights were canceled, and 10,000 others were delayed across the United States. Communications failures cannot always be avoided, but organizations must plan what to do when they occur.

Most organizations have a daily operational plan for their communications that works most of the time. When power goes out or a system goes down, many have a backup plan to get by until the problem is resolved. Unfortunately, this is where their plans often end. Occasionally, operations slow or even stop while people wait for instructions on what to do next. Military leaders have long known that operations cannot cease during an emergency for any reason, so they use a primary, alternate, contingency, emergency plan (known as P.A.C.E. or PACE) for critical operational planning tasks.

The District of Columbia Homeland Security and Emergency Management Agency (HSEMA) Office of the Statewide Interoperability Coordinator (SWIC), decided to introduce the concept to organizations in the National Capital Region. However, despite an array of business continuity training programs across the country, courses that focused on building PACE plans for civilians were not readily available. To fill this gap, HSEMA reached out to the Emergency Communications Division (ECD) of the Cybersecurity & Infrastructure Security Agency (CISA), which developed a new course and curriculum.

Unlike many courses, PACE shows trainees how to teach themselves. By understanding what this type of plan is, the communication methods available, and the many causes of system failures, participants can build a pathway to transfer information under any circumstances. As such, PACE's four-step format should be a component of any communications, continuity of operations, or business continuity plan:

- Primary – the go-to method that operations personnel use as a daily solution (e.g., radios for day-to-day operations).
- Alternate – a backup method that is not preferred but may serve as a good workaround until the problem is resolved (e.g., a different radio system).
- Contingency – a fallback method that uses totally different technology, systems, etc. (e.g., satellite phones).
- Emergency – the last-resort method when the others fail (e.g., a runner).

System failures occur for numerous reasons, from user errors to intentional attacks. Identifying and reporting reasons for, and locations of, failures are critical for pinpointing problems and regaining normal operations. Regardless of the type of failure, even small details during and after an event are crucial. Be aware of what is occurring behind the scenes to consider all possible failure points and alternatives. This helps identify resources that can meet the needs and point out the potential limitations of each resource. In addition to direct communications, a PACE plan for communications also includes data and other daily operations. Consider what other jobs might not be possible if communications systems go down.

Once the PACE plan is complete, all users must learn and understand the plans. To do this, they should have opportunities to train and exercise to ensure they know how to identify when they should change from one method to the next. Developers must also regularly review and revise the plan as systems and operations change. Organizations can better mitigate operational disruptions by keeping the plan simple and managing expectations.

Six key questions to ask when a communications failure occurs include:

- What systems, operations, activities, etc., are impacted?
- Who in the ecosystem is affected (public, government)?
- Which resources and methods are affected, and which are available?
- Why are they impacted (identifying the cause can facilitate the solution)?
- Is it time to implement the PACE plan, or is it time to move to the next step in the PACE plan?

If a communications failure hinders necessary public-safety or public-service activities or puts lives or property in danger, the answer to the last question is yes. Starting with the primary method, work through the alternate, contingency, and emergency stages as needed for each situation. However, since switching to the next step is not intuitive, it must be planned and practiced ensuring all key stakeholders know what to do and under what conditions to change methods. This is why the education, training, and exercise piece is so important. Emergency communications ecosystem participants have to understand that the decision to transition to other parts of the plan may have to occur in a vacuum where communications no longer exist.

By taking a fresh look at old continuity plans, preparedness professionals can better assess their communication needs and identify multiple viable solutions to future communication failures. Lack of PACE awareness was identified as a gap during the 2021 Presidential Inauguration planning process when the preparation plans were rocked for a twelve-day period between the Nashville Christmas Day Bombing and January 6, 2021, insurrection attack on the United States Capitol. Both events challenged operable and interoperable communications, negatively impacting the emergency communications ecosystem.

(Excerpts taken form Domestic Preparedness, "PACEing a Communications Resilience Plan," by Charles J. Guddemi, February 8, 2023. Read the full article at (https://www.domesticpreparedness.com/resilience/paceing-a-communications-resilience-plan/)

Cyber Security versus Ransomware Attacks

With more and more of our public-safety communications dispatch centers and infrastructure being on the web, how secure are your systems to cyber attacks?

The Cybersecurity and Infrastructure Security Agency (CISA) Region 10 office recently gave a presentation and training on what happens when a dispatch center receives a phishing email and the disaster that could follow.

Since approximately September 2022, cyber criminals have compromised U.S. and international organizations with the Royal ransomware variant. After gaining access to a victim's network, Royal actors disable the antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the system.

The most recent and devastating ransomware attack happened in Curry County, Oregon, in April. The attack initially affected their 9-1-1 emergency operations center and their ability to access property and evidence records. This event will cost the residents millions of dollars to reload computer programs and rebuild their local network, and everything that related to county operations that was online is now gone. A similar ransomware attack occurred in Dallas, Texas, which affected the police, the court system, and multiple city websites.

Constant vigilance, cyber security training, public education, system diversity, and updated computer system firewalls will help your agency protect itself from these attacks. Agencies are highly encouraged to never store all their records in one location and to partition their systems, which could prevent bad actors from gaining access to all their records should an intrusion happen.

Alaska has seen its share of ransomware attacks and we can ill afford to let our guard down. The ALMR Help Desk team encourages everyone to update their systems immediately after a security upgrade has been completed to keep system infrastructure protected and secure. There are also two CISA advisors in Alaska who offer free cyber support and can assist with remote vulnerability scanning services.

(Article prepared by Paul Fussey with excerpts from the CISA Advisory AA23-061A and Region 10 training presentation.)

ALMR System Change Request Management Process

The Operations Management Office (OMO) and System Management Office (SMO) must provide a safe, secure, and interoperable communications system that meets the needs of Alaska's emergency first responders. To do so, they must ensure system changes do not detrimentally affect its availability and performance.

The OMO and SMO offices recognize agencies on the system may wish to enhance their operational capabilities. Therefore, a Change Request Form can be submitted by any ALMR stakeholder, user agency, or system operations and maintenance personnel. Some examples where a Change Request Form is required are adding/replacing/removing dispatch consoles, removing system components, updates to system software programs, or adding a channel to an ALMR site.

To ensure the system is protected from unnecessary risks, all proposed changes must be properly documented, reviewed, evaluated, coordinated, and approved prior to implementation.

The requesting stakeholder, agency, or individual must submit a Change Request Form and any associated documentation pertaining to the requested changes for evaluation prior to starting any work. If the requested change is for new technology or an enhancement to existing technology, additional technical and security reviews are conducted within ALMR to ensure the proposed enhancement/technology is compatible with the system operating platform and also that it does not present a risk that could affect the system's Authority to Operate (ATO).

Each change request is reviewed by the OMO, the SMO, the State, the DOD, and the User Council Chair before being presented to the Executive Council who has the final approval authority for all system changes.

(Article prepared by Ms. Sherry Shafer, with excerpts taken from the System Change Request (CR) Management Policy and Procedure 400-3.)

eNIFOG Mobile App and NIFOG are Available for Download

The National Interoperable Field Operations Guide (NIFOG) is now available as the eNIFOG mobile app on Apple® iOS™ and Google® Android™ devices. The NIFOG is a technical reference for emergency communications planning and for technicians responsible for radios that will be used in disaster response. It includes rules and regulations for use of nationwide and other interoperability channels, tables of frequencies and standard channel names, and other reference material.

Be sure if you already have a prior version downloaded that you delete/uninstall before downloading and installing the new version.

The NIFOG is also available in pdf at: https://www.cisa.gov/sites/default/files/video/NIFOG%202.01_508%20FINAL%20VERSION%205%2011%2022.pdf

For printed copies of the NIFOG email: nifog-requests@commscollabcenter.com

(Excerpt taken from the FEMA Region 10 RECCWG Tid Bits Newsletter, January 30.)

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

System Upgrade – Where We're At and Where We're Going

The current system upgrade began long before the kickoff meeting in July 2022 with the State's replacement of their Quantar sites radios with GTR 8000s beginning in late 2020 and finishing up in August of 2022. From there, it was a flurry of activity throughout September as the system migrated from software platform 7.17 to 2021.1. Along with the core software upgrade, activities that closed out the year included upgraded network management (NM) client workstations, hardware refreshes at the zone core (master sites), customer enterprise network (CEN), dispatch centers, and the replacement of the antennas at many of the State sites. There were also software refreshes at each key management facility (KMF), CEN, key variable loaders (KVLs), RF sites, and consoles sites along with third party loggers and the Genesis system.

This year, continuation of the antenna replacement/repair work has already begun, microwave hops from Kobe to Clear, Birch Hill to Quarry Hill, Delta to Fort Greely, and R1 North to Alcantra will all be upgraded, TDMA capabilities and dynamic transcoding will be added to double the voice channel capacity, and Juniper routers will be added to all sites for TDMA added bandwidth and ethernet capabilities.

With the expectation of FedRamp approval, location-on-push-to-talk (LoPTT), radio management, and radio over Wi-Fi/LTE through the federal cloud are new features expected to become available to ALMR users contingent upon having the required equipment and software.

In concert with the State- and DOD-funded upgrade activities, member agencies should be working to obtain the necessary funding to replace all non-TDMA radios by December 31, 2026.

Question regarding the upgrade or new products/features can be directed to the Operations Management Office or System Management Office.

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

Did You Know?

System Management Office (SMO) technicians visit every ALMR radio site annually to test and tune the site radio equipment, look for safety hazards, and perform a visual assessment of all other internal and external equipment at the site. SMO technicians are trained by the original equipment manufacturer to ensure they understand how the equipment should operate in order to keep ALMR at optimum performance levels at all times.