ALMR INSIDER

Volume 15, Issue 2 April 15, 2021

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:

ALMR Coverage and Site Prioritization Survey

The ALMR User Council (UC) routinely looks at areas with coverage or capacity issues. Last October, the council members tasked the Operations Management Office with sending out a coverage and site prioritization survey to member agencies, which was designed to collect information on areas with poor or no coverage for future consideration of expansion should funds or partnering opportunities become available.

The survey was distributed to the 130 ALMR member agencies in mid November and responses were accepted through the end of calendar year.

Some areas mentioned in the survey had been previously identified by the UC and placed on their watch list. They are:

- Chena Hot Springs Road
- Nenana
- Nikiski
- Taylor Mountain
- Tok Cutoff

Other areas identified through the survey for consideration were:

- Chitna (Edgerton Hwy, mile 16 - 35 and Richardson Hwy south past 70 mile)
- City of Cordova
- Delta Junction (second site at the Shaw Creek repeater)
- Fairbanks (Goldstream Road/Murphy Dome Road/Rosie Creek)
- Hope (Hope Highway from Seward Hwy mile 1 to the townsite)
- Kachemak (East End Road past 14 mile/ Ohlson Mountain/some areas west of the Sterling Hwy)
- Kennicott-McCarthy (McCarthy Road corridor/McCarthy proper)
- Ketchikan (limited to no coverage mile 5.5 to end of road system/South on South Tongass Hwy)
- Naukati Bay (everywhere in, near and around Naukati)
- North Pole (Badger Road/Moose Creek/ Plack Road/ Hurst Road/Freeman Road/ Roseanne Court)
- Prince of Wales Island
- Steese (intersection of Elliot and Steese Hwy/various spots past mile 10 of the Steese Hwy/past 1 mile on the Elliot Hwy)
- Sutton (to Tahneta Pass area)
- Turnagain Pass (restroom stop)
- Valdez (Richardson Hwy mile 0 to 16)

The UC understands the importance of adequate coverage and will continue to work with the State of Alaska and member agencies to expand capacity and increase coverage as resources become available.

(Article written by Ms. Sherry Shafer, Operations Management Office

Training Update

With the new Operations Management Office (OMO) contract, fulfilled by Wostmann Associates, a renewed focus on training is underway.

Borrowing from current trends across video sharing sites, the OMO is working on short on-topic “Video Vignettes” which will focus on radio operations, programming tips, and best practices. The first two in the series have been recorded and are in final editing. Watch the website training section at alaskalandmobileradio.org for them to post.

Since July, traditional style training videos covering the basics of trunking concepts and equipment familiarization have been completed and are posted on the website. Other previous training presentations covering affiliation and trunking, radio concepts, radio operations, encryption, and scanning and programming can also be found. Future trainings will also be delivered online. This allows anyone to take training as they have time.

Alaska Statewide Communications Interoperability Plan (SCIP) Update

In FY2019, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Agency (CISA) began supporting states and territories by baselining state emergency communications progress against 25 state interoperability markers to measure the interoperability "health." This tool was developed by looking at best practices along the SAFECOM continuum to highlight emergency communications strengths and gaps, support measurement of 2019 NECP implementation, and provide a framework for developing SCIP goals.

The SCIP is a stakeholder-driven, multi-jurisdictional, and multi-disciplinary statewide strategic plan to enhance interoperable emergency communications. A SCIP serves as a single document for stakeholders throughout a state's communications ecosystem to prioritize resources, strengthen governance, identify future investments and address interoperability gaps. It also serves to complement other state plans such as Homeland Security or Disaster Preparedness Plans. A current SCIP (within 36 months) is also a requirement of the Homeland Security Grant Program (HSGP).

In February, DHS provided technical assistance for the development of a survey to better understand the challenges the State of Alaska is facing, with input from the Department of Public Safety and the ALMR Operations Office,. It was distributed to the 9-1-1 community, Federal partners, and the ALMR user community.

Responses obtained from the survey helped to form the basis of the discussion at the Alaska SCIP Workshop Governance Webinar where priority objectives were set. The next two steps in the process were the technology webinar, which identified technology-related goals and objectives and a funding webinar, which identified the funding-related goals and issues.

The final review and validation workshop/webinar occurred on April **14** and the SCIP is expected to be delivered around May 1. In the end, Alaska will have an updated SCIP that is fully compliant with the SAFECOM grant guidance, as well as a list of goals to help drive forward progress on emergency communications for the next three years.

(Article written by Ms. Sherry Shafer, ALMR Operations Management Office with input from Mr. Bruce Richter, DHS, and Mr. John Rockwell, Alaska Statewide Interoperability Coordinator.)

Encryption Key Management

Encryption key management is the administration of policies and procedures for protecting, storing, organizing, and distributing encryption keys. Encryption keys (also called cryptographic keys) encode and decode data and voice transmissions. Effective encryption key management is crucial to the security of land mobile radio (LMR) communications and sensitive information those communications contain. In addition to ensuring security, key management also ensures encryption does not impede the interoperability among agencies on LMR systems.

There are several reasons to encrypt LMR transmissions, the being operational integrity. Scanners and smartphone applications enable almost anyone to monitor public safety radio traffic and eavesdrop on everything from tactical law enforcement communications (potentially endangering law enforcement personnel) to emergency medical communications containing sensitive patient information. Encryption can keep such transmissions private within the public safety sphere. This does not mean all channels need to be encrypted; each agency should determine which information and channels require encryption.

Encryption keys are managed using key management facilities (KMFs) and key fill devices (KFDs). KMFs generate encryption keys, maintain secure databases of keys, and securely transmit keys to KFDs. Keys are distributed to subscriber units either by direct connection via KFD or by over-the-air-rekeying (OTAR) from a KMF.

The secrecy and security of encryption keys are the foundation of effective encryption. Key management maintains secrecy and security by controlling distribution of keys and reacting immediately if an encrypted radio is lost or stolen. A lost or stolen radio that falls into the hands of an unauthorized user can compromise the security of an entire LMR system. Key management requires a lost radio be disabled remotely and new encryption keys be issued.

Key management maintains the interoperability of LMR systems and radios by ensuring all radios within the system have the same encryption algorithm and keys, enabling them to talk to one another. Just as important, good key management policies ensure encryption keys are shared with partner agencies to maintain fully interoperable communications in mutual aid situations. Balancing security and interoperability is a core objective of key management.

Encryption keys should be changed regularly to minimize risk to LMR communications. The use of static keys—keys used more than once over a long period of time without being changed—is strongly discouraged.

Lastly, Federal Information Processing Standard 140-2 requires all federal agencies to use AES encryption and, as mandated by the Cybersecurity Enhancement Act of 2014, any state or local agency wishing to interoperate on a federal LMR system must also have AES encryption in their subscriber units.

(Article excerpts from the Encryption Key Management Fact Sheet, Federal Partnership for Interoperation Communications (FPIC), undated)

Safer Buildings Coalition: No Noise

As any public safety agency knows, most portable radios do not work well in buildings due to their low power. This means some sort of signal booster must be utilized to boost the subscriber's signal into a building's interior. Without proper installation and maintenance, these signal boosters can create their own set of problems.

The Safer Buildings Coalition (SBC) is calling for the immediate convening of a task force to address public safety radio interference caused by the improper use of "signal boosters" commonly deployed to remediate poor in-building public safety and commercial wireless coverage."

In addition to the steering committee that will guide the task force forward, so far, more than seventy other individuals have signed up to assist and they will become members of the various task-force working groups.

The SBC, an independent non-profit organization focused on eliminating in-building "Wireless Dead Zones," is calling for immediate convening of a task force to address public safety radio interference caused by improper use of Signal Boosters commonly deployed to remediate poor in-building public safety and commercial wireless coverage.

The National Institute for Occupational Safety and Health (NIOSH) issued a recommendation to "provide all fire fighters with radios and train them on their proper use." Since a high percentage of first responder (especially firefighter) work happens inside buildings, it is common sense that these radios must function reliably inside buildings. On February 20, 2013, the Federal Communications Commission (FCC) issued a Report and Order that affirms the local governments' authority to adopt ordinances, and/or fire or building codes that require signal boosters to be installed in certain buildings to ensure First Responders have reliable communications.

Adoption and enforcement of codes and ordinances requiring effective in-building wireless coverage is steadily increasing in the US, Canada and other countries. While many buildings have benefitted from signal booster deployment, there have been recurring challenges. The increase in incidents where improperly deployed signal boosters have degraded or totally disrupted public safety radio systems is concerning and must be addressed.

Key objectives of the call to action are:

- Combat RF interference (noise) caused by improperly deployed in-building signal boosters.
- Affirm and reinforce the essential role of Frequency License Holders in the deployment of signal boosters.
- Affirm the essential need for reliable wireless coverage inside buildings for both first responders and the public,
- Reinforce essential role of consistent codes and standards interpretation and enforcement in achieving that goal.

To ensure the task force is widely represented by industry experts, key stakeholders are being sought from the following disciplines and industry veterans:

- Frequency license holders and radio system administrators;
- Codes and standards bodies;
- Fire and building code officials;
- Public safety agencies;
- Industry members involved in manufacturing, engineering furnishing and installing signal boosters;
- Federal agencies and authorities (FCC, FirstNet Authority, NIST, DHS, NTIA, others);
- Wireless broadband carriers;
- Related industry associations; and
- Property owners and managers,

The SBC, through stakeholder collaboration and consensus, will refine, adopt, and actively advocate principles for safe and effective in-building communications.

(Article prepared Ms. Sherry Shafer, OMO, with excerpts taken from Safer Buildings Coalition Position Paper, "No Noise! Safer Buildings Coalition Affirms FCC Rules for Signal Boosters – Issues Call to Action," December 21, 2020, and from All Things FirstNet e-newsletter, March 4, 2021)

Keep ALMR Cyber Safe - Reboot Your Consoles!

Once a month, Motorola Solutions releases the most current security patches for their ASTRO 25 systems ensuring the safety and security of all assets operating on those systems. At the beginning of the month the patching team will push the initial attempt to patch systems that are ready for patches, and at the third week to the end of the month, a second attempt to patch with the latest patches will be made to those systems that were missed due to pending reboots, network availability, etc.

The System Management Office (SMO) sends out emails to the console points of contact twice a month notifying them Motorola has scanned and applied security patches to all available devices that were rebooted and are ready to receive new monthly patches. The SMO also includes a status sheet of all consoles, playback devices, and network management (NM) clients at either primary or alternate locations that still require reboot.

Agencies are required to reboot their devices if they have not already done so since the latest scan date. Devices not powered on must still be rebooted to ensure security patching remains up to date, and they do not present a vulnerability once turned on for use. The optimal time for rebooting is during the work week 7:30 to 4:30, so the SMO can assist with account maintenance issues that may occur.

NOTE: To reboot consoles, close the console application first to avoid system hang ups and restart the console. When there are multiple consoles, before rebooting the next console ensure the last one comes up without any issues.

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

ALASKA
MUNICIPAL
LEAGUE

Spotlight on the Department of Transportation and Public Facilities

The mission of the Alaska Department of Transportation & Public Facilities (DOT&PF) is to "Keep Alaska Moving through service and infrastructure." DOT&PF is responsible for design, contraction, and operations and maintenance of State transportation infrastructure and publicly owned facilities used by Alaskans and visitors.

DOT&PF manages over 5.6K miles of roads/highways (including 837 bridges and tunnels), 237 airports (including Ted Stevens Anchorage International and Fairbanks International), 12 ferry vessels, and 837 public buildings totaling nearly $12B worth of infrastructure with approximately 3,300 employees at 83 locations around the State. They also act as the vehicle pool for most State agencies, provide statewide commercial vehicle compliance/inspection, law enforcement services at the two international airports, and fire and rescue services at 24 other airports.

With such a distributed workforce and widespread responsibilities, reliable communications are essential, and ALMR is a vital component. In many parts of Alaska, cell phones don't work or have intermittent service, and satellite phones don't have the necessary reliability. Trunked repeaters are often the only way to reach field staff or an operator in a piece of equipment from a district office, and ALMR allows dispatch services that easy contact.

The wide adoption of ALMR also allows prompt and reliable interagency communications - both routine and coordinated incident response. Alaska State Troopers and the Division of Forestry regularly communicate with DOT&PF during traffic disruptions in urban areas or coordinated wildland fire response. When many cell phones wouldn't work during the 2018 Anchorage Earthquake, ALMR facilitated rapid, successful responses from DOT&PF and other agencies. ALMR is a vital piece of Alaska's infrastructure and contributes greatly to the mission to Keep Alaska Moving. (Article by Henry Cole, P.E., Northern Region, DOT&PF)

Help Desk (In Anchorage Bowl):
334-2567

Toll Free within Alaska:
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 next quarterly Zone Controller rollovers are scheduled for May 26 and May 27. Rollovers are used to install security and operating system patches to the master sites.

The process takes place during the regular State maintenance window from 4a.m. to 6a.m. and normally takes less than one minutes to complete each day. Dispatch centers are contacted by telephone prior to the start of the process to ensure there are no active incidents in progress.