ALMR INSIDER

Volume 11, Issue 4 October 15, 2017

ALMR System Slated for Update to 7.17 Operating Platform

Public safety mission-critical communications systems typically run in 5 to 15-year life cycles for the hardware and equipment components. Like any other computer, the hardware and software components that make up the system require continuous updating and patching to maintain cyber security protections.

The current Alaska Land Mobile Radio (ALMR) Motorola-based system has been in operation since 2003 and many of the components are at the end of their life cycle and need to be refreshed. Additionally, Motorola provides a new software release each year to keep up with the latest technology standards and mitigate ongoing security threats. They are only able to support the last five releases due to the cost, dedicated man hours and equipment required.

In 2013, the ALMR System underwent an update of its major core components, known as zone controllers, along with other incidental hardware components, as well as a system software update. Those components and the current software platform reach the end of their support beginning fall of 2017.

A core system update is required in order to maintain support and security services within the ALMR System and must also follow the Gold Elite console replacement project that is currently underway at several dispatch locations.

All three zone controllers must be updated simultaneously in the shared ALMR System. The Department of Defense (DOD) and the Municipality of Anchorage partners have implemented plans to fund the update of their zone controllers as well as needed system software updates and also fund the System Upgrade Assistance (SUA) II maintenance program for their zone controllers.

The State of Alaska recently procured their funding through Capital, and Operating and Maintenance appropriations.

Once all funding is in place, the project will take over a year to plan and implement.

(Article prepared by Ms. Sherry Shafer, Operations Management Office with excerpts from SOA FY18 appropriations documents)

FirstNet Update - Governor Opts In

On August 24, Governor Bill Walker signed the opt-in letter for the State of Alaska to participate in the First Responder Network Authority (FirstNet) plan, which will bring a secure wireless broadband network to the public safety community.

Alaska incurs no risk or cost for the network, which will expand coverage for Alaska, including rural areas. By growing network access for first responders, a reliable, high-speed connection will be available in areas currently with little to no connectivity.

Emergency communications are often accomplished through many technologies, and in addition to using land mobile radio (LMR) systems, many public safety agencies are using commercial cellular data services or wireless broadband services to augment LMR capabilities.

Public safety agencies see a future in which LMR systems and wireless broadband services will converge to complement each other, but they do not see FirstNet replacing LMR.

Public safety agencies recognize LMR systems provide key mission-critical voice communications, which is currently not available through FirstNet and, at best, is years away from realization.

(Article by Ms. Sherry Shafer, ALMR Operations Management Office)

ALMR Help Desk

In Anchorage:
334-2567

Toll Free within Alaska (outside of Anchorage):
888-334-2567

E-mail:
almr-helpdesk
@inuitservices.com

Follow us on Twitter:
@ALMR_SOA

Inside this issue:

NPSTC Radio Interoperability Best Practices #3 - Training and Proficiency in the Management and Usage of Interoperability Equipment and Systems

This is a final installment of the Best Practice ongoing effort on the part of the National Public Safety Telecommunications Council (NPSTC) to identify recommendations for a variety of topics dealing with interoperability. The Radio Interoperability Best Practices Report companion document link is located at end of article.

Radio interoperability equipment and systems should be used and managed only by personnel who have been properly trained and who have demonstrated proficiency with the appropriate technical, operational and procedural aspects. This Best Practice applies to technicians, responders, dispatchers and managers and includes both operational and interoperability issues.

Training can be the easiest, but also the most important, of the Best Practices to implement. Most agencies already have a training program in place into which this Best Practice can be incorporated. Insufficiently trained personnel have incorrectly activated radio gateways/ patches, programmed radios incorrectly, and failed to identify readily available interoperability solutions, all of which have led to major communications failures.

Successfully managing the communications aspect of a critical incident involves significant investment by each participating agency. This is an investment in human resources and management priority. Personnel with responsibility for interoperability components include:

- Radio and information technology (IT) technicians who design, implement and maintain the solution
- Users including communications center dispatchers/ telecommunicators, emergency responders and incident Communications Unit personnel
- Supervisors, in their role as instructors, mentors, schedulers and evaluators, and management who have the overall responsibility for policy and budget

Every department member should receive at least a minimum baseline of awareness training, including terminology and an overview of available resources and assets to include:

- A basic understanding of portable and mobile radio features by field personnel, including how to change groups/zones/channels, expectations of performance coverage for each channel (especially as it relates to tactical, simplex, or interoperability channels), and troubleshooting
- Information on interoperable channel assets and options available during major or multi-jurisdictional incidents and system failures
- Opportunities for advanced training including communications technician (COMT) and communications leader (COML) for highly qualified individuals
- Familiarity with agency and regional Tactical Interoperability Communications Plan (TICP) and Statewide Communications Interoperability Plan (SCIP), as appropriate

All personnel should receive both orientation and focused training appropriate for their specific role and should demonstrated proficiency to the level documented by agency policy.

- Technicians, users, and supervisory personnel need generalized training on the overarching view of the interoperability system including:
  - ♦ Knowledge of all subscriber unit radios, consoles, gateways, features, and accessories, including recovery (back up) from system failure
  - ♦ Knowledge of radio network infrastructure and capabilities, including specialized interoperability resources managed by the Public Safety Answering Point (PSAP), dispatch center and field users
  - ♦ A variety of delivery systems to supplement formal classroom instruction, including the use of multimedia components to engage the student and maintain their attention and the use of systems that simulate the live environment or the use of the live environment, when available
- Technical personnel, who program, maintain or repair interoperability equipment and systems need training on existing and/or new systems and system enhancements including:
  - ♦ The ability to maintain the systems, troubleshoot problems, program subscriber devices, deploy the equipment and knowledge of console operations
  - ♦ The ability to demonstrate proficiency in the operation and maintenance of those networks
  - ♦ Training on all relevant radio frequency (RF) and network systems and software applications
- Users need initial and recurring training on the proper use of interoperability resources and have demonstrated proficiency in effective decision making and operational use of equipment and systems and how and when to contact appropriate support personnel when systems do not operate as expected
- Communications center personnel need specific training and readily accessible information (such as TICPs, Operations Guides, contact information both internal and external to their agency, etc.) on interoperable channel options including the:
  - ♦ Knowledge of resources, proper usage, coverage area limitations and console capabilities and functions
  - ♦ Process to identify and secure available options or resources during major or multi-jurisdictional incidents or system failures

Training touches every lane of the SAFECOM Continuum, which proves its importance in the overall success of any interoperability challenge.

(Article excerpts taken from NPSTC Radio Interoperability Best Practices, January 2017)

(Best Practices Report - http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_IO_Best_Practice_Overall_Report_Final.pdf)

Harris County P25, LTE networks critical to Hurricane Harvey Response, Recovery

Other than a few sites that flooded because of unprecedented water levels, the Harris County, Texas, land mobile radio (LMR) and Long-Term Evolution (LTE) networks withstood Hurricane Harvey and its aftermath, which included more than 50 inches of rain, according to county officials. The county operates a regional Project 25 (P25) network called the Texas Wide-Area Radio Network (TxWARN).

"The network performed well," said Shing Lin, director of public-safety technology for Harris County. "We did have some locations that had really high water, but our engineering team found a way to get to them during the storm and bring them back up. We didn't lose any communications although the sites did go down briefly. We had capacity issues more than anything else."

During construction, LMR sites are often hardened to withstand extreme environmental factors the general public-accessible communications systems are not, providing continued validation that LMR has a vital role in public safety communications today and well into the future. Instances like these will continue to emphasize the importance of maintaining and updating public safety interoperable communications systems like ALMR.

(Excerpts taken from Mission Critical Communications article, September 12)

FCC Continues Path to Eventual 6.25 kHz Narrowbanding

This effort began more than 20 years ago in 1995, when the commission announced that as of Jan. 1, 2005, it would no longer certify equipment that could not operate on 6.25-kilohertz channels or with equivalent efficiency. This deadline was later pushed back several times until it finally took effect Jan. 1, 2015; however, the prohibition does not actually require users to operate in 6.25-kHz mode. Equipment certified prior to the deadline may still be sold, whether or not the device has 6.25 kilohertz capability, but any manufacturer seeking to obtain certification for new equipment or making changes to an existing model that requires recertification must include the capability to operate in 6.25-kilohertz mode or equivalent efficiency.

When and how the transition to 6.25 kilohertz will happen is anyone's guess. But the Federal Communications Commission (FCC) continues to remind licensees that the transition is still in the commission's future plans. The most recent example came in the FCC's June 30 order denying a request for waiver filed by the International Municipal Signal Association (IMSA).

In its waiver request, IMSA argued that the commission's certification deadline effectively required new radios to be digital because analog technology generally does not meet the 6.25-kilohertz requirement. IMSA claimed that the "6.25-kilohertz channelization requirement prevents manufacturers from improving current products" unless they also include 6.25-kilohertz capability, which customers may not want or even be able to use to the extent their current deployment is analog. IMSA believed this to be an undue burden on public-safety users. The hardest hit users likely would not be large urban agencies, which may have already transitioned or are planning to transition to digital networks, but would almost certainly be smaller volunteer fire departments and other similar public safety providers, that often are forced to make the most of very limited budgets.

On June 30, the commission ultimately rejected IMSA's arguments and issued an order denying its request for waiver, choosing instead to leave the Jan. 1, 2015, deadline in place. The commission took the opportunity to again reiterate that it intends a further migration from 12.5 to 6.25-kilohertz licensing at some point in the future. One question the FCC did not answer is when the transition to 6.25 kilohertz will occur. Logically, if the transition is soon, it does not make sense to allow manufacturers to continue to certify new equipment that will need to be replaced within its expected lifetime.

(Article by Greg Kunkle, August 1, 2017, Mission Critical Communications E-magazine)

SAFECOM Nationwide Survey

The SAFECOM Nationwide Survey is a data gathering effort that will equip government officials and emergency responders with critical information to make decisions about future emergency communications policies, funding and programs.

The data collected will depict the capabilities necessary for establishing operable, interoperable and continuity of communications. Both SAFECOM and the Department of Homeland Security Office of Emergency Communications encourage organizations with emergency communications responsibilities for federal, state, local, tribal and territorial governments to participate in the survey and help shape the future of emergency communications.

The survey is expected to be released in Fall 2017. Updates will be posted to the SAFECOM website. (https://www.dhs.gov/safecom/sns)

(Article Information provided by Mr. Bruce Richter, OEC Region X Coordinator.)

Keys to Encryption

Encryption is the protection of sensitive information. As data and voice networks continue to converge, encryption will be an integral part of network architecture. Encryption can benefit first responders in the field by protecting sensitive information, but it is up to individual agencies to determine their encryption requirements.

The law requires agencies to protect certain types of information. Other kinds of information could and should be safeguarded better. According to the Federal Partnership for Interoperable Communications (FPIC), situations where encryption could be considered when defining requirements include:

- Safety of personnel and enhanced safety of the public and property;
- Sensitive law-enforcement information including active investigations and surveillance;
- Personally identifiable information (PII), sensitive PII and/or protected health information (PHI) privacy act or health privacy data;
- Tactical/investigative data that may jeopardize law-enforcement operations; and
- Disaster incident information that may reduce the reaction abilities of public-safety officials.

The digital encryption standard used on the ALMR P25 System is the advanced encryption standard (AES) 256, a National Institute of Standards and Technology (NIST) standard defined in Federal Information Processing Standard 197 (FIPS 197). Additionally, FIPS 140-2 defines how AES-256 is employed in cryptographic modules. AES is an open standard and, therefore, is free.

(Excerpts from Mission Critical Communications Magazine, August 2017)

Help Desk (In Anchorage Bowl): 334-2567

Toll Free within Alaska: 888-334-2567

Fax: 907-269-6797

Email: almr-helpdesk@inuitservices.com

Website: http://www.alaskalandmobileradio.org

Follow us on Twitter: @ALMR_SOA

Did You Know?

The System Management Office coordinates, oversees and performs daily incremental backups of the System and weekly backups of dispatch console configuration files and the Key Management Facility. All network device configurations including, but not limited to, domain controllers, routers, firewalls and switch configurations are backed up before and after System changes.
(System Backup and Recovery Procedure 400-5)

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

ALASKA
MUNICIPAL
LEAGUE