ALMR INSIDER

Volume 19, Issue 1 January 15, 2025

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:

Care and Use of Land Mobile Radios

When most public safety employees (police, fire, EMS, or communications) are hired, they must attend some type of academy to certify they have the proper knowledge to perform their duties. They spend hours learning to operate weapons, fire hoses, life saving devices, or radio/telephone consoles. However, the device (tool) that you, as a responder, will use the most and rely on heavily throughout your career is the one you may be least trained on.

These are your radios and communication systems. Field employees are normally issued vehicles with radios, portable radios, and possibly pagers. The employee should be aware of the operations and potential dangers that accompany their tools. When you are in a situation where your life or someone else's life may depend on you being able to get a message to another person or dispatch, knowledge of those communication devices should be second nature.

With the increased use of Wi-Fi, commercial two-way radio systems, and other radio frequency devices, the agencies found they could no longer communicate without additional support. The need for repeaters increased. Multicast, simulcast, and trunking systems were designed and implemented to improve LMR service for the agencies' needs.

Today, land mobile radio (LMR) is the backbone radio network for most public safety agencies, although a few agencies have transitioned to the computerized digital networks of long-term evolution (LTE). Mobile radios are defined as transceivers mounted in mobile command posts, patrol cars, fire trucks, ambulances, or other vehicles. Portable radios consist of hand-held transceivers, pagers, and monitoring devices. Most LMR systems are privately owned and operated by the agency licensing the frequencies or several agencies as a cooperative agreement

Radios are continuing to evolve. With the need for radios to perform jobs (GPS, messaging, etc.) similar to cellular phones, manufacturers are turning out a computer with a transceiver attached to it. Today's radios, being mostly computer — are programmed the same as any other computer. The solid-state components allow for miniaturization to keep the radio an appropriate size. As the radio is also a computer, concern has arisen of the possibility that viruses or hacking of radios could be a problem for public safety agencies.

Additionally, you must treat your radio with a degree of care. Don't grasp a portable radio by the antenna or use the antenna as a handle or to hold in any case. It can damage the antenna and render the radio inoperable. When you inspect your radio, look for damage to the rubber coating on the antennas. Never use your radio for something it is not designed for. One example is a door stop — serious damage to the radio could occur. Also, always check for damage to your batteries and radio cases.

Mobile and portable communication devices are an integral part of our public safety lives. We are dedicated to washing and waxing our vehicles, polishing our shoes, and putting patches, badges, and flash on our uniforms to show how proud we are. Law enforcement officers check their weapons and defensive gear every shift. Fire and EMS personnel check their equipment and mark their checklists regularly. The little things in life (like the radio that is always there and bothersome) needs to be brought to the forefront of our attention. What would happen to teenagers without their smartphones? Can you imagine your day at work without a working radio?

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from "*Care and Use of Land Mobile Radios, Radios are a central component of the public safety communication toolkit"* by Michael A. Scales, APCO January/February 2021)

Keeping up with Cybersecurity Threats

Government agencies are a constant target for bad actors and ransomware attacks due to the large amounts of valuable and sensitive data processed through their systems. As states deploy new technologies — including web-based, modular, or interoperable solutions — the number of system boundaries, coordination touchpoints, and attackable systems have expanded leading to increased attacks.

Before launching a new IT project, agencies should assess whether their in-house cybersecurity team has the bandwidth to take on the influx of responsibility, risk, and threats related to the effort. Agencies should consider engaging an independent, experienced planning, and project management vendor to support development of a project roadmap, procurement plan, risk management plan, privacy and security assessments, and penetration testing.

During procurement of the system, agencies should also ensure strict cybersecurity requirements are established in the request for proposal (RFP) and that the resulting contract includes enforceable, performance-driven service-level agreements, key performance indicators, and metrics that align with the organization's cybersecurity strategy and goals. Agencies should work with their project vendors to periodically revisit metrics and measures to ensure they are continuously improving their posture and the contract terms are being met.

Put cybersecurity at the forefront of planning for your system enhancement and modernization projects. Engage business, technical, and security stakeholders to ensure cybersecurity is well planned and executed. Make sure security requirements are documented in RFPs and contracts integrate enterprise security frameworks, guidelines, and standards into the software development life cycle.

ALMR is continuously working on cybersecurity upgrades with our vendors and security manager to deploy them monthly and quarterly to ensure the security and vitality of the system is maintained for all of our subscribers. As a joint State and DoD system, any new development or capability is thoroughly tested and checked for FedRAMP compliance.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from the CSG Government Solutions article "*Keeping up with Cybersecurity threats across government systems*" by Dale Posont)

FCC Announces Deadline for 4.9 GHz Licensees to Update Licensing Data

On December 9, the Federal Communications Commission (FCC) issued a public notice announcing that all 4.9 GHz public safety licensees must update their granular licensing data in the Universal Licensing System (ULS) by June 9, 2025. This requirement follows FCC action to adopt a framework in which a to-be-selected band manager will hold a nationwide overlay license and enter into a sharing agreement with the First Responder Network Authority (FirstNet) to access the band in areas unused by incumbent operations. The FCC outlined the following process for licensees to provide details on their current operations and use of the band:
Licensees must ensure that all active operations under existing PA licenses are correctly documented and categorize operations into two new license types: PB (base/mobile, mobile-only, or temporary fixed operations) or PF (fixed point-to-point or point-to-multi-point operations).

Starting December 9, licensees must use ULS to file detailed licensing data for new PB and PF licenses. For PB licenses, licensees must use schedule D and H forms to provide details such as coordinates, antenna heights, and areas of operation. For PF licenses, licensees must use schedule I forms to submit data on transmission/receiver antenna parameters, frequencies, and path details. Licensees should also include a list of the relevant PA call signs in an attachment to the PB and PF service code request(s).

Once licensees' new PB and PF licenses are issued, licensees must cancel any existing PA licenses. After June 9, 2025, any remaining PA licenses will be cancelled automatically. Incumbent public safety licensees in the 4.9 GHz band must follow this process and provide the granular licensing data to remain authorized to operate in the band.

(Article prepared by Mr. Paul Fussey, with excerpts taken from the APCO December 13, 2024, PSC eNEWS)

What is NIFOG and how does it Pertain to ALMR

The National Interoperability Field Operations Guide (NIFOG) is the national guide for possible use in a situation where no other radio interoperability arrangement was promulgated by local authorities, or where emergency responders are unaware of such an arrangement. The NIFOG does NOT supersede any federal, state, tribal, territorial, local, or regional emergency communications plan.

The latest version of the NIFOG is 2.02 and is a pocket-sized listing of land mobile radio (LMR) frequencies that are often used in disasters or other incidents where radio interoperability is required, and other information useful to emergency communicators developed by the Cybersecurity and Infrastructure Security Agency (CISA).

If you are dispatched to a disaster or incident scene and have no other information, the NIFOG provides useful suggestions for which frequencies to use to attempt initial contact. The NIFOG can be downloaded from CISA.gov.

(Article prepared by Mr. Paul Fussey, with excerpts taken from the NIFOG manual, January 2025)

Cyber Risks to Land Mobile Radio

Land Mobile Radio (LMR) systems are designed to provide instant, reliable, and secure critical push-to-talk communications to the public safety and first responder community. However, the evolution of LMR systems from analog to digital has made these networks, devices, and data susceptible to cyber threats. Cyber risks manifest when a cyber attacker gains unauthorized access to a network, device, or data and affects the confidentiality, integrity, or availability of the system or information. Some consider LMR networks closed systems that are not exposed to cyberattacks and do not see cybersecurity as an important component of their communications system. However, LMR systems are vulnerable to multiple cyber risks that could negatively affect critical communications.

LMR systems are terrestrially based, wireless communications systems commonly used by federal, state, local, tribal, and territorial public safety, first responders, public works, commercial companies, and the military in tactical and non-tactical environments. Supporting voice and low-speed data communications, LMR systems typically consist of handheld radios, in-vehicle radios, control stations, base stations, and repeaters and a core network which ties the components together.

There are those who may perceive LMR systems to be analog or separate from other systems directly connected to the internet. However, the Confidentiality, Integrity, and Availability (CIA) information security triad applies to LMR networks, devices, and data because the information being transmitted is sensitive and critical to public safety operations. Thus, LMR systems are a vector for malicious cyber actors to target public safety organizations. LMR systems are vulnerable to compromises such as unauthorized monitoring, eavesdropping, encryption hacks, disruptions of the physical infrastructure, and jamming of frequencies.

Maintaining secure and reliable communication modes is vital to the success of public safety missions. Cyber risks in LMR systems could result in loss of life or property, injuries, job disruption for affected network users, and financial costs associated with data misuse and subsequent resolution. Therefore, cybersecurity cannot be ignored or become an afterthought in the design, operation, and maintenance of LMR networks.

There are many vectors that malicious actors can use to gain access to LMR systems, causing loss of the confidentiality, integrity, or availability of the system. Mitigating these risks is the first step in ensuring LMR systems remains secure.

Public safety community members should use comprehensive cybersecurity best practices to plan for and mitigate cyber vulnerabilities and incidents. For example, the National Institute of Standards and Technology (NIST) recommends that public safety organizations routinely plan, prepare, and conduct drills for cyberattacks and incidents. In addition, NIST recommends including responses to cyber incidents and system outages as an extension of the organization's contingency plan. The contingency plan suggests having incident response plans and procedures, trained staff, assigned roles and responsibilities, and incident communications plans established well in advance. It is recommended to periodically review and update the plan to ensure efficacy (e.g., on an annual basis, when there is a significant change in leadership, when new components are acquired and implemented).

NIST developed a cybersecurity framework to help critical infrastructure owners and operators identify and reduce risks. The framework comprises three parts: Framework Core, Framework Implementation Tiers, and Framework Profiles. Following such a framework can help system owners navigate the five phases of cyber risk management: Identify, Protect, Detect, Respond, and Recover.

Agencies should identify what is on the network, inventory all hardware and software assets to distinguish what items could be vulnerable to cyberattacks, and establish a monitoring strategy to identify unusual activity that could indicate an attack. Additionally, the inventory process is not a one-time event and policies and procedures must be in place to ensure the LMR system's inventory is monitored regularly to ensure equipment that remains in the organization's possession is working properly and has strong software/firmware versions, authentication, and encryption keys.

All equipment owners should consider implementing a centralized patch management system to enable automatic updates whenever possible. If feasible, obtain, test, and deploy the latest operating systems, applications, updates, and "patches" before installing them on a "live" system.

Knowing when an attack occurs could further minimize damage to an LMR system instead of discovering an intrusion much later in the attack stage. Additionally, once the threat is detected, having an established plan in place will potentially reduce the impact on the system.

Agencies should implement a predetermined incident response plan and follow the established internal and external reporting structure and should be prepared to potentially deviate or adjust the procedures as the cyber incident could render parts of the plan inapplicable.

It is important to maintain process improvements and incorporate lessons learned into future activities to improve the recovery planning processes and strategies. Agencies should train response personnel on the latest security, resiliency, continuity, and operational practices and maintain in-service training as new technology and methods are available.

Recognizing the importance of cybersecurity and the impacts on LMR systems will help mitigate potential cyber risks and improve LMR system resiliency.

(Article prepared by Mr. Paul Fussey, ALMR Operations Manager, with excerpts taken from the CISA "*Cyber risks to land mobile radio" publication 2022*)

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

Considering Encryption for your Organization

Federal agencies are required by law/policy to use encrypted communications at all times. State, local, tribal, and territorial public safety agencies are strongly encouraged to also adopt advanced encryption standard (AES) encryption. All agencies must first identify what information it needs to protect. Agencies should review their jurisdictional legal requirements, operational environment, standard operating procedures, and communication vulnerabilities.

Encryption can apply to so many parts of a communications ecosystem that an agency's first impulse might be "let's encrypt everything," but in practical terms blanket encryption can work against an agency. Blanket encryption should not interfere with interoperability between agencies. If an agency chooses to generate its own encryption keys and fails to coordinate with neighbors and partners, interoperability can be compromised, preventing disciplines from coordinating their efforts.

AES256 is the only algorithm that complies with the P25 standards and its use is strongly recommended. As in all areas of management, record-keeping for an encryption system is essential. System administrators must keep accurate, up-to-date records of who in their organizations have encrypted radios and what keys and talk groups are assigned to those radios.

The ALMR team can help organizations with their encryption concerns and questions. ALMR policy and procedures requires the reporting of lost or stolen radios as soon as possible to protect the encryption keys.

(Article prepared by Mr. Paul Fussey, with excerpts taken from CISA article "*Encryption in P25 Public Safety Land Mobile Radio Systems*")

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

2024 ALMR End-of-Year Statistics

Member Agencies: 165 agreements

Subscribers: 32,677
(TDMA and non-TDMA)

*Group and Individual Calls: 17,714,270

*Push to Talks: 28,797,345

*Busies/Percentage rate of calls: 7,232 (0.0004%)

(*Totals are cumulative)