ALMR INSIDER

Volume 20, Issue 4 October 15, 2026

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:

Alaska APCO Chapter	2
Nationwide Test of the Emergency Alert System	2
FIPS 140-3 level 3 Encryption	2
Drones are a Security Challenge for Critical Infrastructure	3
New Document Specialist	4
New Email	4

APCO and MTUG 2026 Conferences

From August 2nd to August 7th, I attended three conferences and seminars back to back. The week started with the Genesis Users Forum (GUF), followed by the Association of Public Safety Communications Officials (APCO) and the Motorola Trunked User Group (MTUG). The APCO and MTUG associations have many members in Alaska and I attend these events to advocate for our interests.

The GUF opened with introductions of participants and it was a great networking event, being able to talk with my peers and share information. Alaska Land Mobile Radio (ALMR) uses Genesis to maintain the system and pull the monthly metric reports for the User Council meetings. It also monitors all the ALMR towers and the current usage.

Some of the updates to Genesis will assist the ALMR team in maintaining the system and subscriber inventory. The ALMR team can edit talkgroups for activities on specific towers. With the newest map enhancements, ALMR can add in all of the bi-directional antennas (BDA's) and with new report features, ALMR can run zero radio usage reports to identify radio that have not been on the system for several years.

APCO began the next day and I met with Alaskan members to see what seminars they were attending. We attended the opening session and the keynote speaker before we dispersed for our training sessions.

APCO held 132 individual sessions with 11 professional development tracks over the four days.

As the Operations Manager for ALMR, it is my responsibility to approve and test radios to ensure they will work on the system. When the exhibit hall opened I made my rounds to meet with multiple radio and equipment vendors to see their latest products, schedule acceptance testing for the ALMR system and to gather brochures. I was able to set up testing for three radios from two different manufacturers.

Some of the seminars I attended were regarding interoperability and how it can help LMR systems and agencies. Another seminar I attended was a about the FCC regulatory updates regarding federal agencies which was beneficial since there are a large number of federal agencies on ALMR. This led me to begin asking about the latest security requirements under the Federal Information Processing Standards (FIPS) 140-3 level 3. This requires that any radio that has a federal frequency must comply with FIPS140-3, level 3 by September 21, 2026.

ALMR is a Motorola system which is why it is important people from Alaska attend MTUG. This gives us a platform to listen to what is new from the engineers, voice complaints, and meet with other Motorola product users and attend the national MTUG meeting.

Some of the sessions I attended included the latest on the APX Next XE models, which are designed to be used by fire departments and are National Fire Protection Association compliant.

I also learned that there are new antennas being developed that are an improvement over the current omnidirectional antennas. The new antenna technology is compatible with Anchorage's AWARN 700/800 MHz system and could be beneficial for their upgrade.

After the sessions, I received all of the brochures, handouts, and power point slides of the presentations and forwarded them other ALMR team members so that they could learn about the latest products and innovations pertaining to ALMR.

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

Alaska APCO Chapter

Stacey Day, the 9-1-1 Public Safety Supervisor with the Kenai Police Department, attended the 2026 APCO International Conference & Expo in San Antonio, Texas. As president of the Alaska APCO/NENA Joint Chapter and Alaska's representative on APCO's Executive Council, Day values the opportunity to attend Executive Council and chapter president meetings, connect with leaders from other states, and bring ideas home to Alaska.

"Leadership training and conversations with other chapters help us grow our chapter and better serve dispatch centers across Alaska," Day said. "Every time I attend a public safety conference, I come back excited about our profession and with a renewed sense of purpose."

Day purchased recordings of the APCO conference sessions to share with her dispatchers and earn Continuing Education Credits towards recertification. She encourages agencies and individuals to consider annual APCO and NENA memberships, including group options. Membership can provide free or discounted training, scholarships opportunities and resources that help new dispatchers build their skills while giving experienced dispatchers continued opportunities to grow.

APCO also continues to work on federal occupational reclassification efforts for public safety telecommunicators, reflecting the critical role dispatchers play in emergency response.

"I want dispatchers across Alaska to know there is training designed for the work we do—and that their experience and ideas matter," Day said. She invites dispatchers from every Alaska center to join the chapter's monthly Zoom meetings, consider an open chapter leadership position, and get involved.

Visit the Alaska APCO/NENA Facebook page for chapter updates. The chapter is updating its Facebook page and working on a state chapter website. Public Safety individuals are also welcome to reach out to Day directly with questions or concerns.

Contact Information:
Stacey Day
Alaska APCO/NENA Joint Chapter President
APCO Executive Council Representative for Alaska
sday@kenai.city (907) 335-5257

Nationwide Test of the Emergency Alert System – November 17, 2026

With our risk of tsunami inundation, and the need to rapidly get warnings to the public, Alaska has been a leader in Emergency Alert System (EAS) live-code testing. Alaska tests regularly so that life-safety warnings are transmitted over radio, television, wireline video, and cable to the public to save lives in an emergency.

In fact, given Alaska's EAS test experience, the Federal Emergency Management Agency (FEMA) often requests permission from Alaska broadcasters and the state to come to Alaska first to try their live code tests before going nationwide. This allows FEMA to test their procedures and systems in our state, and correct any errors, before going nationwide.

FEMA testing will occur again in Alaska on October 7, 2026, at 10:20 am, when FEMA will transmit a national test message over Alaska's EAS. Following the Alaska test, FEMA will then send an EAS test message nationwide on November 17, 2026 at 10:20 am. In both cases the message will be brief and clearly identified as a test with the test script stating "this is a test of the Emergency Alert System, issued by the Federal Emergency Management Agency… This is only a test. No action is required by the public".

This testing allows Alaska's emergency officials, broadcasters, and the nation to be sure they can transmit emergency messages to the public. In Alaska, EAS has been used for tsunami warnings, AMBER Alerts, and immediate evacuations for fires or flooding. These alerts in Alaska over EAS are issued through the voluntary participation of Alaska's broadcasters who partner with the state's emergency officials to provide the public with immediate life-safety information.

(Article prepared by Mr. Mark Roberts, SEOC/DMVA)

FIPS 140-3 level 3 Encryption

The Federal Information Processing Standard (FIPS) 140 is a benchmark standard established by the National Institute of Standards and Technology (NIST) to validate the effectiveness of cryptographic modules. For nearly two decades, FIPS 140-2 served as the national baseline for securing sensitive but unclassified data. However, as technology changed and threats evolved, flaws within the framework were highlighted. In response NIST introduced FIPS 140-3 to align with modern global frameworks and address advanced vulnerabilities.

FIPS 140-2 established a baseline for cryptography, but the implementation of FIPS 140-3 moves these requirements into the modern world. By aligning with international ISO standards, introducing defenses against non-invasive side-channel attacks, and tightening the rules around software integrity, FIPS 140-3 ensures that cryptographic modules remain resilient against today's threat landscape. As of the publishing of this article FIPS 140-3 level 3 is required for all Alaska Land Mobile Radios which utilize Department of War and Federal Agency talk groups.

(Article prepared by Mr. David Reed, ALMR ISSM)

Drones are a Security Challenge for Critical Infrastructure.

For many critical infrastructure operators, drones have become indispensable tools used for tasks like transmission line inspections, pipeline surveys and rail corridor monitoring.

However, drones have also introduced new challenges that existing security systems and on-the-ground teams weren't built to address. The same capabilities that make drones operationally valuable also make them effective tools for surveillance and reconnaissance. Bad actors can use them to map facility layouts, monitor security protocols and identify vulnerabilities, often without operators knowing a drone was ever there.

The recent GridEx VIII report highlighted the growing risks drones pose to critical infrastructure and the need for operators to improve their visibility into activity occurring around sensitive facilities. At the same time, the Federal Aviation Administration's proposed section 2209 rule would enable eligible fixed-site facilities in the U.S. to request restrictions on drone operations near sensitive infrastructure.

Every major critical infrastructure sector has invested heavily in perimeter security. Cameras, lighting, motion sensors and access control are mature, well-understood capabilities. However, they were designed to address ground-based threats. While these measures remain essential, they provide little visibility into activity occurring above a facility.

A consumer-grade drone can operate at several hundred feet above ground and reach a top speed of 47 miles per hour. From two miles outside a facility's perimeter, a drone can cross into restricted airspace, complete a reconnaissance mission, and exit in under three minutes, all without a security team even knowing it was there.

The FAA's Remote ID framework requires drones to broadcast identifying and location information, functioning much like a digital license plate for aircraft operating in low-altitude airspace. Remote ID is an important step toward greater visibility and accountability for drone operators and supporting the safe integration of drones into commercial applications. However, it falls well short of providing the comprehensive visibility critical infrastructure operators need.

Remote ID works when drone operators choose to comply and broadcast their information. Only about 20% of drone flights today are Remote ID compliant, and a bad actor targeting critical infrastructure will simply choose not to broadcast information announcing their presence.

Organizations need visibility into drone activity, whether operators choose to comply or not. Passive radio frequency, or RF, detection is one example of a technology that makes this possible. Rather than waiting for a drone to announce itself, RF-based systems identify the communication link between a drone and its controller from the moment of takeoff — regardless of whether Remote ID is enabled — allowing operators to identify drone activity that would otherwise go unseen.

As drone activity continues to rise and new rules, like Section 2209, bring new regulatory attention to airspace security, effective security must assume the threat won't cooperate and plan accordingly.

When a drone appears over a refinery, substation or other sensitive facility, critical infrastructure operators should have a clear process for assessing the activity, documenting what occurred and sharing actionable information with the appropriate authorities. While the authority to investigate or mitigate unauthorized drones often resides with local law enforcement, state agencies or federal partners, critical infrastructure operators play a critical role in providing the information those organizations need to respond effectively.

That means building relationships before an incident occurs. Organizations should establish response procedures, identify points of contact with law enforcement and government partners, and ensure drone activity can be documented and shared quickly with supporting evidence.

Effective airspace security depends on a shared operating picture. When critical infrastructure operators, local law enforcement, state agencies and federal authorities are working from the same understanding of drone activity, they can make faster decisions, coordinate more effectively, identify patterns across facilities and respond with greater confidence.

Recent industry exercises, guidelines and regulatory developments make one thing clear: Airspace is now part of the security perimeter, and critical infrastructure operators can no longer afford to leave it unmonitored or unmanaged.

Section 2209 is more than a regulatory proposal. It is a recognition that drone activity has fundamentally changed the security landscape for critical infrastructure. Organizations can no longer define their security perimeter solely by fences, gates and cameras. The airspace above their facilities has become an operational security concern that demands the same level of visibility, awareness and planning.

The organizations best positioned for this new environment will be the ones that can understand what is happening in the airspace around them, share that understanding with the right partners and respond accordingly.

(This article was prepared using excerpts and information from Melissa Swisher's article, "Drones Are the Next Big Security Challenge for Critical Infrastructure," published by *Utility Dive* on August 26, 2026. The source was used to provide background and context regarding the growing security challenges posed by drones to critical infrastructure. (Swisher, 2026).

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

New Document Specialist

Elizabeth Serrano is a third-generation Alaskan and currently works as the Document Specialist supporting Alaska Land Mobile Radio (ALMR) through Wostmann & Associates, Inc. Before joining ALMR, she worked for the Alaska Center for Resource Families, where she supported foster, adoptive, and guardianship families across the state.

Her work there included coordinating trainings and resources, developing community partnerships, and helping connect families with services and opportunities throughout Alaska.

Community involvement has been a regular part of Elizabeth's life as well. She served on the board of the Chugach Education Corporation from May 2022 to May 2026 and on the statewide Resource Family Advisory Board from January 2024 to July 2026. She also volunteers with Alaska Junior Theater, and the Salvation Army of Alaska. Most recently, she added flag football coach to the list and currently coaches her son's team through Club Sports Alaska.

Outside of work and volunteering, Elizabeth is the mother of a 12-year -old son and has more interests than she has free time to fit them into. She paints, sews, crafts, works on DIY projects around her home, and is almost always learning how to make, repair, or try something new. She is especially interested in ancient history and collects ancient coins,

Elizabeth is curious by nature and enjoys figuring things out, whether that means learning a new skill, researching an obscure subject, solving a practical problem, or taking on a project she has never attempted before. One of the ideas she tries to live by is that "everything is figureoutable."

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

New Email

The Operations Management Office has a new email that it will be using to send out meeting invites and membership agreements. The new email is linked to everyone in the office and is as follows ALMR-OMO@wostmann.com.

We ask everyone to add this email to your approved list so important information from us does not end up in your spam or junk files.