ALMR INSIDER

Volume 10, Issue 2 April 15, 2016

ALMR Help Desk

In Anchorage:
334-2567

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

E-mail:
almr-helpdesk@inuitservices.com

Inside this issue:

The Importance of Public Safety Grade P25 for ALMR

The Project 25 (P25) user community has identified a broad set of features and services important to public safety communications. The suite of 25 standards defines the functional and operational aspects of these features and services. There are too many to list here, but this includes several types of voice calls, IP and common air interface data bearer services, control signaling services, mobility management services and location services. It also includes voice and data encryption, security services such as authentication and also key management. Most services are available in both trunking and conventional operating modes.

In addition to meeting national and international government spectrum regulations, the suite of P25 standards defines additional performance requirements important for public safety communications. This includes coverage performance modeling and verification methods, receiver and transmitter performance measurement methods and specifications for both frequency division multiple access (FDMA) and time division multiple access (TDMA) air interfaces. Additionally, it includes voice service access and throughput delay specifications and measurement methods for radios, base stations and trunking systems. P25 also defines a rigorous vocoder intelligibility and background noise performance evaluation process that has resulted in approval of interoperable full-rate and half-rate digital vocoders.

As stated previously, the public safety community has identified requirements for a wide variety of interoperable, standards-based communication services, configurations and capabilities with well-defined performance interoperability, and testing specifications. This is the essence of the P25 suite of standards, as it relates to "public safety grade" communications systems.

- A public safety grade communications standard, first and foremost, provides a set of features, capabilities and services required by the diverse group of public safety users.
- The P25 User Needs Sub-Committee (UNS) has defined those required features and the Project 25 suite of standards supports those features.
- Manufacturers take the features and specifications defined by the P25 standard and implement them in reliable software, hosted on rugged hardware platforms that are exhaustively tested to meet the performance and interoperability specifications prescribed by the P25 suite of standards.
- These software and hardware platforms are then combined and implemented as a P25 system in a highly-reliable, highly-resilient manner, with redundant elements, backup power, etc. These systems are designed to cover a specified geographic area with extra margin for coverage reliability. Equipment that is built to the P25 standards and has been tested to P25 standard tests and is installed, operated and maintained to the maximum extent practical, creates an interoperable public safety grade communications system.
- Multi-vendor solutions enabling interoperability between devices, public safety individuals and groups, fleets and teams that can be can be linked across local, regional, state and national networks exist, thereby offering public safety agencies competition and options for cost-effective sourcing.
- Public safety practitioners have been doing this with the P25 suite of standards for close to 30 years and there are over 700 P25 systems in operation, including the Alaska Land Mobile Radio (ALMR) Communications System, providing public safety grade, life-saving communications for day-to-day operations, as well as emergency situations.

(Article by Mr. Del Smith, Operations Manger, with excerpts from PTIG Whitepaper, "Is Project 25 Public Safety Grade?" March 2016)

New ALMR Subscriber Radio Vendor Approved

As of March 2, three models of Icom Inc. subscribers were tested and approved for use on the Alaska Land Mobile Radio (ALMR) Communications System, using the established ALMR Acceptance Test Procedure (ATP) standards. The subscribers are the IC-F9011S portable radio, the IC-F9511T mobile radio (5, 25 and 50 watt models) and the IC-F9511HT mobile radio (110 watt model).

Icom specification sheets and test results can be found at www.alaskalandmobileradio.org/radios.htm.

As with any vendor radio purchase, agencies should always request the use of demo radios to ensure they will meet the agency's needs and expectations prior to expending acquisition funds.

The ALMR Operations Management Office (OMO) will be glad to address any questions or concerns your may have regarding Icom, or any approved vendor radios.

Additionally, a Unication P25 trunking-capable, G5 multiband pager, VHF and 700-800MHz, is going to be made available to ALMR for testing. When it arrives, the OMO will contact agencies to determine interest in participating in testing

(Article by Mr. Rich Leber, ALMR Technical Advisor)

Tech Corner: Passwords, Logins and Security

The ALMR User Council has developed system login and security procedures to ensure the ALMR System remains secure from unwanted intrusions and possible compromising of our ability to provide critical communications capabilities to our member agencies. Given the digital environment that exists today, it is also important to employ some of the policies and procedures we use to protect ALMR in our personal lives.

Everyday on the news, we hear about some business or government agency being hacked, intellectual property being compromised or personal information being stolen. There isn't much we can do to avoid this type of loss, unless you pay cash for everything and live in a cave, but there are steps that we can take to protect our professional and personal information from potential theft.

At one time or another, all of us have come into work and attempted to sign onto our workstation and this dreaded message appears; "Your password has expired." This isn't the way any of us wants to start our day, and when you attempt to change the password, the message appears that you have used that password before and you must come up with a new one. I think this situation could be added as one of life's certainties; "death, taxes and password changes." I know from experience that we all have a multitude of passwords that we must remember to access a myriad of applications. Such is life!

There are good reasons and sound logic for changing passwords on a regular basis and rules that apply to changing them. The Criminal Justice Information System (CJIS), National Law Enforcement Telecommunications System (NLETS), National Crime Information Center (NCIC), Alaska Public Safety Information Network (APSIN) and ALMR systems all require frequent password changes to remain compliant and keep them secure.

According to a January 21, 2014, CBS News article, the three most commonly used passwords are "123456", "Password" and "12345678." Is it any wonder that so many systems and accounts are hacked on an annual basis?

Hackers are smart and have plenty of free time and sophisticated software to help them. Using numbers in place of letters such as "d15patch" may seem secure to you, but I can guarantee that if you have thought of it, so has a hacker. You should use a combination of numbers, capital letters and symbols. Badge or ID numbers should never be used as they are easily obtained by the public. Birthdays should also never be used, as they are easily obtained through social media (Facebook, etc.). Lastly, never use any work-related words and/or codes.

Unfortunately, the easiest way to gain access to a system, such as ALMR, is to pose as a "Trusted" system user/member, which requires the use of the correct login and password. This is just another reason not to share login and password information in a dispatch center.

Technology is continually advancing. CNN Money reports that in a few months, you should be able to verify your identity when shopping online by taking a selfie or scanning your fingerprint. MasterCard will launch these new mobile technologies that make this possible in the United States, Canada and the United Kingdom over the next few months. Specifically, a special mobile app will enable customers to take a photo or scan their fingerprint each time they make an online purchase.

CNN explains: Their face (or fingerprint) will be scanned to prove that they are not hackers or thieves making a purchase. The scan will verify that it's a legitimate selfie, instead of a previously taken photo, by requiring users to blink when they take their own photo.

Such authentication methods will be used regularly worldwide within five years, according to Ajay Bhalla, president of enterprise safety and security at MasterCard. Facial recognition and fingerprint scanning are safer than passwords, he says, because many people use weak passwords.

MasterCard is also exploring other authentication methods, including monitoring a customer's heartbeat as well as iris scans and voice recognition. Hopefully some of these new technologies can and will transition over to our secure systems to eliminate the need for passwords. We can only hope!

(Submitted by Mr. Rich Leber, ALMR Technical Advisor, MasterCard excerpts taken from the February 23, 2016 Money Talk News)

DHS Releases Funding Amounts for Ten Grant Programs

The Department of Homeland Security (DHS) released fiscal year (FY) 2016 notices of funding opportunity for ten (10) DHS preparedness grant programs totaling more than $1.6 billion. The grant programs provide funding to state and local governments, transportation authorities and others to improve the nation's readiness in preventing and responding to terrorist attacks, major disasters and other emergencies.

The FY16 grant guidance will continue to focus on the nation's highest risk areas. Grant recipients are encouraged to use grant funding to maintain and sustain current critical core capabilities through investments in training and exercises, updates to current planning and procedures, and lifecycle replacement of equipment. New capabilities that are built using Homeland Security grant funding must be deployable, if needed, to support regional and national efforts.

The allocations include:

- Emergency Management Performance Grant (EMPG) with more than $350 million to assist state, local, tribal, and territorial governments in enhancing and sustaining all-hazards emergency management capabilities.
- The State Homeland Security Program (SHSP) provides $402 million to support the implementation of risk-driven, capabilities-based state homeland security strategies to address capability targets.
- Operation Stonegarden (OPSG) provides $55 million to enhance cooperation and coordination among local, tribal, territorial, state and federal law enforcement agencies to jointly enhance security along the United States land and water borders.
- Intercity Passenger Rail – Amtrak Program (IPR) provides $10 million to protect critical surface transportation infrastructure from acts of terrorism and increase the resilience of the Amtrak rail system.
- The Port Security Grant Program (PSGP) comprises $100 million to help protect critical port infrastructure from terrorism, enhance maritime domain awareness, improve port-wide maritime security risk management, and maintain or re-establish maritime security mitigation protocols that support port recovery and resiliency capabilities.
- The Transit Security Grant Program (TSGP) provides $87 million to owners and operators of public transit systems to protect critical surface transportation from acts of terrorism and to increase the resilience of public transit infrastructure.
- The Intercity Bus Security Grant Program (IBSGP) includes $3 million to owners and operators of intercity bus systems to protect critical bus surface transportation infrastructure.

To learn more or apply, visit http://www.grants.gov.

(Article submitted by Mr. Rich Leber, ALMR Technical Advisor with excerpts extracted from Mission Critical Communications Transmission Weekly News, February 24, 2016)

Radio Frequency Technician Shortage

On a recent nightly news program, they talked about a shortage of skilled trades individuals and the fact that parents nowadays are steering their children to college for that four year degree. That has left a void in skilled trade positions like electricians, plumbers, welders and masons, all of which are compensated quite well.

We can also add radio frequency (RF) technicians to that list. In the August 2015 Mission Critical Communications magazine, there was an article on this shortage and the problems public safety organizations are having finding, hiring and retaining qualified personnel to fill open positions in the RF field.

The armed forces and vocational schools were the major source for RF technicians in the past, but with the evolution of radio technology in the 1970s and 80s, requirements have changed. The use of radios in business and the need for a FCC Class 2 license drove the demand for RF curricula into the vocational schools. This was also a time when participation in high school ham radio clubs peaked student interest in radio careers.

In the past, service in the military offered young people the opportunity to receive radio communications training. Large numbers of recruits took advantage of these opportunities and have since served as mentors for the current generation of RF technicians. Professional technicians of this era are a dying breed (myself included). Replacing the current field of technicians with individuals of the same caliber of knowledge and experience is nearly impossible. Even hiring individuals for entry-level positions is becoming more difficult, if not impossible.

Employers are now hiring personnel with little or no experience in the radio field and providing training to meet their institutional requirements and needs.

The problem of hiring/replacing retiring RF technicians is also not limited to the government sector. In most commercial radio shops around the (continued on page 4)

RF Technician Shortage (continued)

country most of the staff are in their 50s and 60s and are on track to retire in the near future. Additionally, most of these technicians got into the radio business through training they received while in the military. These days the military doesn't train component level troubleshooting; if it isn't functioning, they simply replace the board.

The vocational schools offering RF technical training have declined over the past two decades, as young people became more interest in information technology (IT) fields. Little do they know that that is the way that radio communications field has gone.

IT technicians and RF technicians are not interchangeable. The culture of the two disciplines is different. IT technicians specialize in the flow of information and tend to focus in a single area, such as server or computer support. RF technicians have to be competent in multiple disciplines to configure, maintain, troubleshoot and repair interoperable communications components and systems.

There are also technology solutions that alleviate some of the RF technician shortage issues by making it easier to identify problem radios over the air, test equipment that troubleshoots and aligns radios, and radio equipment that requires fewer adjustments/ tweaks. All of these solutions require less time by the technicians, but they are not cheap! Even with these time saving solutions, technician must be available to utilize the equipment and decipher any test results.

Bottom line: If you have a good RF technician, appreciate him/her and thank them once in a while.

(Article by Rich Leber: ALMR Technical Advisor with excerpts from the August 2015 Mission Critical Communications magazine)

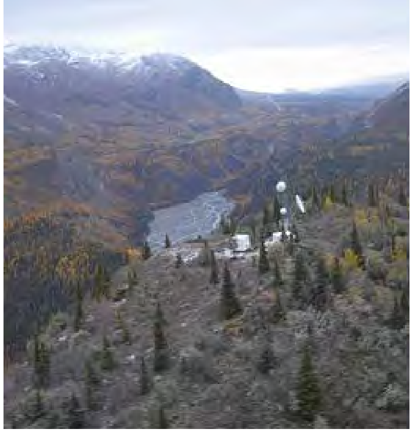
Help Desk In Anchorage Bowl: 334-2567

Toll Free within Alaska: 888-334-2567

Fax: 907-269-6797

Email: almr-helpdesk@inuitservices.com

Website: http://www.alaskalandmobileradio.org



Lions Head, ALMR Site 54

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

ALASKA MUNICIPAL LEAGUE