Transcript: Introduction to Encryption

Welcome to this Alaska Land Mobile Radio training presentation, an introduction to encryption.

The ALMR system is an APCO project 25 compliance system. This provides for a broad set of standards that ensure the system is sufficient and works well for public safety and other uses. As a part of these standards and the use of more advanced technology, ALMR has a number of features that can be utilized by its members.

Among those is the ability to encrypt radio traffic. ALMR radio traffic uses digital technology. In other words, your voice, when you use your radio, is not transmitted in the clear like an analog signal, but is more like a digital stream, such as how a voice over IP phone would work.

Because ALMR uses digital technology, we're able to utilize the radio spectrum more efficiently and also able to utilize advanced subscriber units or radios to enable advanced features. Encryption is one tool that is available. However, there are important considerations before you utilize encryption on the ALMR system. This training will provide a brief overview of those considerations.

Simply put, encryption enables secure communications between radios. This ensures that unauthorized radios cannot hear the traffic being exchanged. This also prevents any members of the public or other parties that may be scanning the ALMR system to receive the radio traffic being sent. It is a misconception that the Alomar system cannot be scanned. Keep in mind that it is significantly more difficult to scan digital technology and requires much more advanced and expensive equipment, but it is possible for the public to scan radios. Some agencies have connections to their radios to Internet services and other broadcast mediums, which allow for the use of cell phones and other things for monitoring. These connections also impact security and allow others to receive the radio traffic.

Encryption utilizes a key encryption key that is loaded on each radio that essentially decrypts the traffic. It can be used by agencies on the ALMR system, and encryption may be something that initially sounds like a positive and useful step, but there are several

important management considerations to think about before utilizing encryption in your daily work.

Some considerations for encryption began with the additional hardware and software that is required. Loading encryption keys requires the agency to possess a key loader, which is a physical device that loads the system keys or encryption keys onto the radio. These units do come with additional cost and depending on the geographic area, agencies may wish to purchase more than one to allow for efficient use and programming of radios. Where that service takes place. Additionally, radios generally by default do not come with the encryption capability enabled. Most P25 radios have the ability to use encryption, but that feature must be activated or purchased when you purchase the radio. This can increase the per unit cost to the agency.

When encryption keys are loaded into radios, control of the radio units themselves become even more essential. If a radio is lost or stolen with encryption keys that can create a vulnerability and cause the encryption keys to be compromised.

When initially loading encryption keys, this must be done on the radio. There is over the air re keying and other changes that can take place without having the radio. However, the proper encryption keys must be loaded on the unit physically by hand before this can occur on the system.

To have communications with other agencies in encrypted mode, you would be required to share your encryption key with other agencies. Any time an encryption key is shared, that key is now on radios that are not in your control and security can be impacted depending on the security needs for your particular agency. This may be something to carefully consider before going with an encrypted mode of contact.

Because the encryption keys need to be shared with other agencies. These can cause barriers to interoperability if agencies do not wish to share their encryption keys. Then the users must either switch to a non encrypted mode or move to another talk group that's interoperable or is shared using the talk group sharing agreement. These can create confusion for users. Between what situations would require encryption and what situations require clear transmission.

If a user, for example, forgets to change to clear when talking with other agencies and transmits encrypted, the radios that do not have that encryption key will simply not hear any of that traffic and generally won't indicate that traffic is taking place. This can be an issue for working together on an incident scene or cause other communications confusion.

Keep in mind that encryption is not appropriate for interoperable situations and they are not permitted on all of our interoperable channels such as the central and north zones. Keep in mind that ALMR encryption is only for ALMR tALK groups. If you are utilizing conventional channels as part of your communications plan, or using conventional channels as part of the Almar interoperability zone. Encryption does not function on those channels.

Encryption does cause an increased load to the Alomar system. If you are considering using encryption, contact the ALMR helpdesk for specific advice and assistance. If you have further questions, contact the Amar help desk or ALMR operations Management Office for assistance.