COMMUNICATIONS GUIDELINE NUMBER 18-01

Land Mobile Radio Encryption

Effective: Immediately
Date issued: 9/12/2018
Valid: Until revoked or superseded
Revision: **1** (Updated Contact Information)

SUMMARY:
This document is intended to provide guidance to public safety entities considering encryption. This document does NOT require the use of encryption by any agency, but rather it sets forth a process to follow if an agency *chooses* to utilize encryption.

DESCRIPTION:
If an agency chooses to implement encryption in their land mobile radio system, this guideline outlines best practices to follow to permit interoperable encrypted communications. Utilizing encryption in a digital radio system has additional parameters required beyond clear voice communications. Failure to coordinate these parameters can inhibit the ability to share encryption when desired, and could even result in loss of communications if keys are inadvertently overwritten. Each agency considering encryption should carefully weigh the increased security of the communication against the impacts on administration and interoperability.

DEFINITIONS:
Advanced Encryption Standard (AES) – Generally recognized as the strongest widely available Land Mobile Radio encryption available to State/local public safety. Project 25 (P25) supports the AES-256 bit encryption type. This is the State recommended format for general use, and is the required format for interoperable encryption.

Common Key Reference (CKR): A decimal value between 1 and 4095 that is utilized by the radio and programming software to locate the encryption key within memory. Also known as the Storage Location Number (SLN).

Key ID (KID): The unique identifier for the actual over the air encryption key. This is a hex value between 0000 and ffff and is transmitted in the P25 data stream. This is the identifier that the radio utilizes to locate the proper internal key for the transmission.

Storage Location Number (SLN): A decimal value between 1 and 4095 that is utilized by the radio and programming software to locate the encryption key within memory. Also known as the Common Key Reference (CKR).

JUSTIFICATION:
Conflicting or uncoordinated encryption keys can hamper operability and/or interoperability. For example, if two neighboring agencies both program their systems and radios with a CKR/SLN and KID of 1, it would not be possible to share encryption keys with the neighboring agency. The act of sharing would cause the home agency's key to be overwritten. Whereas with unique, coordinated keys, agencies can share without concern for inadvertent overwrite.

PROCESS:
Once an agency has decided to implement P25 digital encryption, and to ensure a non-conflicting assignment, they shall contact the National Law Enforcement Communications Center (NLECC) to obtain a unique CKR/SLN and KID.

The point of contact at NLECC is:

National Law Enforcement Communications Center (NLECC)
U.S. Department of Homeland Security, Customs and Border Protection
Office: 407-975-1966
NLECC-WSOC@cbp.dhs.gov

The NLECC will maintain a database of assigned CKR/KIDs in an effort to prevent overlap among public safety agencies.

Agencies that are already utilizing AES-256 encryption should also contact the NLECC and determine if their existing CKR/KID is unassigned. If it is unassigned, the NLECC can mark it as "in use" to prevent duplicate assignment. If there is already a conflict, the agency should evaluate a change at the next reasonable opportunity.

It must be noted that this process only applies to the CKR/SLN and KID. The actual encryption key string (the unique values that secure the communication) are left entirely to the agency to select. Only the agency will know those parameters and have access to the secured communication, unless they chose to share their encryption. No part of this guideline's process reveals your secured communications or key strings to NLECC or DHSES.

TECHNICAL PARAMETERS:
- Public safety agencies who choose to implement encryption should implement the AES-256 type encryption to ensure multivendor compatibility and information security. Deployments of older or proprietary encryption types/algorithms should be avoided. Agencies receiving grant funds must ensure compliance with relevant grant requirements.
- Agencies purchasing radios capable of encryption are strongly encouraged to procure radios with support for multiple encryption keys (sometimes known as "multikey").
- Encryption is not permitted on VHF, UHF, and 800 MHz national interoperability channels.
- CKR/SLN 1 through 20 (decimal) are reserved for nationwide interoperability, as managed by NLECC. No agency in New York State shall utilize CKR/SLN 1 through 20 for any other purpose. Existing non-conforming uses should migrate away from these nationwide reserved identifiers as soon as practical.
- Agencies that choose to utilize encryption are strongly recommended to utilize a radio programming mode where the encryption is fixed on or off per channel, commonly known as "strapped encryption". Permitting user selectable encryption on a particular channel can lead to possible inadvertent leakage of secure information due to the incorrect mode/knob setting being selected by the user.