

CENTRAL REGION
800 MHz Trunked Regional Public Safety Radio System
Standards, Protocols, Procedures

Document Section:	3 - Interoperability Standards	Status: Complete O&O Approval 4/14/2011
Sub-Section:	CM 3.19.0	
Procedure Title:	Use of Regional 800 MHz Encrypted Common Pool Talk Groups – CM ENC's	
Date Established:		RRB Approval:
Replaces Document Dated:		
Date Revised:	4/14/2011	

1. Purpose or Objective

To establish policy & procedures for use of the CM RRB 800 MHz Encrypted common pool talk groups. The Regional Encrypted talkgroups are intended to facilitate encrypted communications between law enforcement agencies that typically do not communicate with each other on a regular basis/daily basis.

2. Technical Background

■ **Capabilities**

It is possible to have access to one or more encrypted common pool talk groups in radios used by agencies that share use of the 800 MHz radio system. These encrypted talk groups can be used for a wide range of intercommunication when coordination of activities between personnel of different Law Enforcement related agencies is needed on an event.

■ **Constraints**

CM ENC talkgroups must be programmed with DES/OFB encryption.
 CM ENC talkgroups must be programmed as always encrypted (strapped)
 CM ENC talkgroups cannot be utilized outside of law enforcement purposes.
 All radios programmed with CM ENCs must use the CM RRB assigned encryption keys.

Operational Context

The Encrypted common pool encrypted talk groups are a system wide resource to facilitate communications between law enforcement related agencies that typically do not communicate with each other on a regular basis.

3. Recommended Protocol/ Standard

CM ENC 1-6 TALK GROUPS

TG Requirements	For Whom?
Highly Recommended	All law enforcement agencies
Recommended	
Optional	
Not Allowed	All others

Cross Patch Standard	YES / NO	To Talk Group
Soft Patch	YES	Other strapped Encrypted talkgroups
Hard Patch	No	

The "Status Board" application will be used to manage the pool talk group resource.

None of the CM ENC 1-6 talk groups shall be part of any multi-group.

Logging of CM ENC 1-6 will be the responsibility of each entity using the talk groups. CM ENC 1-6 should be programmed in dispatch consoles.

It is highly recommended that entity radio users program a sufficient quantity of CM ENC talk groups into their subscriber radios to meet their interagency encrypted communications needs.

5. Recommended Procedure

CM ENC 1-6 may only be patched to another strapped encrypted talk group to meet the communications needs of an event.

The order of usage of CM ENC 1-6 for **PREPLANNED NON-EMERGENCY** interoperability events should be CM ENC 6, 5, 4, 3, 2, 1.

The order of usage of CM ENC 1-6 for **UNPLANNED EMERGENCY** interoperability events should be CM ENC 1, 2, 3, 4, 5, 6.

The Request and assignment of CM ENC resources shall be completed through the controlling PSAP. An appropriate 800 MHz dispatch center capable of assigning the resource, shall use the "Status Board" application to identify and assign the appropriate CM ENC resource as "in use".

The controlling PSAP will be responsible for the reassignment of the resource as "available" at the conclusion of use.

6. Management

The CM RRB System Administrator will be responsible for managing the CM RRB encryption keys.

The dispatch center managers for agencies on the CM RRB 800 MHz radio sub-system shall insure that there is a procedure for assigning the CM ENC talk groups.

The MnDOT System Administrator shall be responsible for the Status Board application.

PSAP personnel shall receive initial and continuing training on the use of this procedure.

Responsibility for monitoring performance, and modification, of this procedure shall be a function of the agencies using this resource.

Eligibility to allow these talk groups with the encryption key will be the responsibility of the local system administrator. This authorization will be supported by the local law enforcement official responsible for the requesting agency.