CENTRAL REGION

800 MHz Trunked Regional Public Safety Radio System

Standards, Protocols, Procedures

Document Section:	**3 - Interoperability Standards**	**Status: Approved** **O&O Approval: 8/20/2020**
Sub-Section:	**CM 3.19.0**	
Procedure Title:	**Use of Regional Encrypted Interoperable Talkgroups**	
Date Established:	4/14/2011	**ESB Approval: 9/30/2020**
Replaces Document Dated:	4/14/2011	
Date Revised:	8/20/2020	

1. Purpose or Objective

To establish policy & procedures for use of the CM ESB Encrypted Interoperable talk groups. The Regional Encrypted talkgroups are intended to facilitate encrypted communications between 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 interoperable talkgroups in radios used by agencies that share use of the ARMER radio system. These encrypted talkgroups can be used for a wide range of intercommunication when coordination of activities between personnel of different public safety agencies is needed on an event.

■ Constraints

CM encrypted talkgroups must be programmed with DES/OFB encryption.
CM encrypted talkgroups must be programmed as always encrypted (strapped)
CM 2-5 LE talkgroups cannot be utilized outside of law enforcement purposes.
All radios programmed with CM encrypted talkgroups must use the CM ESB assigned encryption keys.

Operational Context

CM encrypted talkgroups are a region wide resource to facilitate communications between public safety agencies that typically do not communicate with each other on a regular basis.

The CM ESB Region recognizes there is a need for encrypted communications for events that include participation by all branches of public safety. The Region also recognizes the need to designate several encrypted talkgroups as “law enforcement only”.

Patching CM 2-5 LE and CM 6-12E should be limited to other encrypted talkgroups to retain

encrypted communications. It is important to note: Successful communications when patching two encrypted talkgroups is dependent on proper radio programming (assignment of statewide designated 'Patch Key') for all radios involved with the event.

If a situation arises where communications with a clear mode talkgroup is absolutely necessary for officer/citizen safety, these talkgroups may be patched to a clear mode talkgroup **ONLY** with proper announcement by the dispatcher to all parties that **encryption is no longer active**.

3. Recommended Protocol/ Standard

CM-2 LE – CM-5 LE

TG Requirements	**For Whom?**
Required	Dispatch Console, Law enforcement encrypted radios
Highly Recommended	
Recommended	
Optional	
Not Allowed	All others

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

CM-6 E – CM-12 E

TG Requirements	**For Whom?**
Required	Dispatch Console, CM agencies with encryption capable radios
Highly Recommended	
Recommended	
Optional	
Not Allowed	

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

Status Board will be used to manage talkgroup resources.

No CM encrypted talkgroup shall be part of any multi-group.

Logging will be the responsibility of each entity using the talk groups. All CM encrypted talkgroups should be programmed in dispatch consoles.

For any agency adding CM encrypted talkgroups to subscriber radios, it is required that all allowed CM encrypted talkgroups be programmed for each specified discipline in a designated Zone "CE". See examples below for law enforcement and non-law enforcement zones.

Position	**Zone CE (LE radios)**	**Zone CE (non LE radios)**
1	CM-CALL	CM-CALL
2	CM-2 LE	
3	CM-3 LE	
4	CM-4 LE	
5	CM-5 LE	
6	CM-6 E	CM-6 E
7	CM-7 E	CM-7 E
8	CM-8 E	CM-8 E
9	CM-9 E	CM-9 E
10	CM-10 E	CM-10 E
11	CM-11 E	CM-11 E
12	CM-12 E	CM-12 E
13		
14		
15		
16		

5. Recommended Procedure

CM-2 LE thru CM-12 E should only be patched to another strapped encrypted talk group to meet the communications needs of an event. (See Operational Context for exemption.)

The order of usage for **PREPLANNED NON-EMERGENCY** interoperability events should be CM-5, 4, 3, 2 LE and CM-12,11,10, 9, 8, 7, 6 E.

The order of usage for **UNPLANNED EMERGENCY** interoperability events should be CM-2, 3, 4, 5 LE and CM-6, 7, 8, 9,10, 11, 12 E.

The Request and assignment of CM encrypted resources shall be completed through the controlling PSAP. A Dispatch center capable of assigning the resource, shall use the "Status Board" application to identify and assign the appropriate CM encrypted 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 ESB System Administrator will be responsible for managing the CM ESB encryption keys.

The dispatch center managers for agencies on the ARMER system shall ensure that there is a procedure for assigning the CM encrypted talk groups.

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 for CM agencies will be the responsibility of the local system administrator. Requests to allow these talk groups with the encryption key for agencies outside the CM Region will be reviewed and decided by the CM Owners and Operators Committee. This authorization will be supported by the local public safety official responsible for the requesting agency.