Encryption Work Group Update March 2025

Chris Kuhl

CJIS or LEIN Information Via Radio

Michigan State Police, LEIN Field Services has decided on the following criteria for agencies that would be used in upcoming audits pertaining to CJIS information over radio and the need to have that voice traffic secure.

CJIS Requirements

1. The requirement has been in place at the Federal level since 2011, secure voice traffic is now scrutinized on Federal audits.
2. This requirement has not been well circulated or communicated to agencies, MSP CJIS understands hardware costs/changes and planning time frames are critical for successful implementation.
    - ➢Any LEIN audits conducted after **10/01/2026** will look at this area, agencies should be able to show they are working towards compliance on this topic.
    - ➢CJIS information is defined as information obtained from LEIN, AFIS, ALIAS, SNAP, NCIC, NICS, and NDex.

CJIS Requirements Cont.

3. The encryption requirement is FIPS 140-3 or FIPS validated (AES), in either case a minimum 128-bit key is required.

- For the MPSCS network AES256 is the only algorithm that meets/exceeds this requirement.

4. The other component LEIN audits will look at is access to CJIS information over the radio. Only authorized agencies/users are allowed access to CJIS information. Typically, only law agencies are permitted to receive protected criminal justice information.

County/Agency Updates

Wexford Co- New non primary talkgroups-

- 83FOPS4 (Fire Operations) MPSCS ADP CKR169
- 83LEIN2 (83LEIN remains clear) MPSCS AES CKR1667

Barry CO- Barry Co is moving the direction of AES encryption, the request was made to TDU in early May 2024, both AES with common MPSCS CKR's-

- 08P911E

Updates Cont.

Allegan Co- Allegan is moving towards primary dispatching on an ADP talkgroup that was created, strapped with MPSCS ADP CKR-

- 03LAWE- currently they are using an existing talkgroup called 03ALTAC which exists in all radios in Allegan including MSP and DNR.
- Final implementation is dependent on reprogramming completion as they are using this opportunity to incorporate other changes from surrounding counties.

Updates Cont.

VanBuren CO- Van Buren is moving towards AES encryption for day-to-day operations leaving the 80P911 in the clear is it currently is. The new talkgroups are “strapped” with common MPSCS AES Key.

- 80DRUGE
- 80LAWE
- 80LEINE
- MSP already has these added and they are VBCO consoles. (this MSP dist radios are AES capable). Full countywide implementation will be dependent on when upgrades are received, and programming completed.

Updates Cont.

City of Romulus (Wayne County) encryption migration – COMPLETED

- Talkgroups “82RPD1” and “82RPD2” are selectable using CKR 162 “Wayne ADP” to support interoperability within Region 2. This change was necessary to resolve a key conflict. Expected transition for these talkgroups to AES is late 2026.
- Romulus has begun to receive the first round of radio replacements with all encryption algorithms for interoperability with Detroit Metropolitan Airport Authority, SEMI UASI, and other MPSCS resources.
- Life Cycle radio replacement will continue into 2026

Updates Cont.

Western Upper Peninsula Encryption Migration Project

- Houghton, Keweenaw, Gogebic, Baraga, and Ontonagon resolved 20 older CKRS not coordinated with NLECC as of July 2024
- These counties are in the process of onboarding subscriber radios into OTAR; which has accelerated this process.
- Once the final migration is completed, we expect additional CKRs to be shut down, resolving several other CKR conflicts related to Federal partnerships.
- Baraga will take slightly longer which could extend the life of this project.

Updates Cont.

Benzie County- Benzie County CD is moving towards AES256
10P911/10F911 remain unencrypted to maintained interoperability with all neighboring agencies

- New 10PTAC talkgroup to be created using AES CKR 1667 “MPSCS LAW AES” for secure law enforcement communications other than dispatch related traffic – secondary talkgroup
- New 10LEIN talkgroup to be created using AES CKR 1667 MPSCS LAW AES for secure law enforcement LEIN communications
- New 10FTAC talkgroup to be created using AES CKR 1668 MPSCS FE AES for secure Fire and EMS communications other than dispatch related traffic – secondary talkgroup
- All encrypted radios will be onboarded for OTAR operation and managed by MPSCS Key Maintenance Facility (KMF), currently Benzie CD is working with MPSCS on a few test radios and enrollment of those in the KMF/OTAR server.

CKR Update-(1/1/2025)

Approximately 137 total encryption keys in use on MPSCS

- 74 AES256 encryption keys in use; this includes all local, state and federal partners.
- 50 DES/OFB encryption keys in use, 4 CKR conflicts remain but two are currently being resolved.
- 13 ADP/ARC4 keys in use with only two conflicts remaining (down from 4).

StateWide AES Encryption CKR’s

- **CKR 1667 (MPSCS LAW)** = authorized for any law enforcement agency and can only be loaded into law enforcement radios for agencies that operate as a law/public-safety agency. Using this CKR is recommended for primary law enforcement dispatch talkgroups to support common law enforcement interoperability initiatives.
- **CKR 1668 (MPSCS FD/EMS)** = authorized for any fire, EMS, and law enforcement agency.
- **CKR 1669 (MPSCS COM)** = authorized for all agencies/any discipline for inter-agency interoperability.

Talkgroup Changes

MPSCS does not allow new encrypted talkgroups to be selectable.

- Talkgroups will always be secure or clear
- I Event and J Event remain selectable, to many radios contain these, impossible to change
- L Event is only for radios with AES and is always secure or “strapped.”
- **L Event was originally rolled out with CKR 212, that has changed to a non-conflicting CKR, if you have CKR212 you must submit for re-programming by 12/13/2025.**

ADP/DES CKR's

- Effective January 2023 MPSCS will no longer create new/unique CKR assignments for DES and ADP (ARC4) algorithms.
- This is not "retroactive", any existing CKR's can continue to be used.
- DES & ADP are still supported but the agency must use the MPSCS statewide CKR's for those algorithms.
- If the agency has a unique key(s) they should be maintained by your agency.

New Talkgroups with DES/ADP

- Currently the Encryption Work Group is considering a position to no longer deploy new talkgroups with DES or ADP encryption.

- Key points-
  - Only for public safety, (Law, Fire, Public Safety, EMS, OEM) users
  - Organizations like public works and transportation could still utilize lower forms.
  - Is not retroactive, you can continue to use existing talkgroups with ADP or DES encryption.
  - As of 01/2023 Federal Agencies can no longer obtain ARC4/ADP and DES Encryption on radios

Network Connected Consoles

MPSCS Console Inventory & Key Verification

- Todd Velderman has initiated an effort to visit all PSAP's with network connected consoles.
  - The purpose is to inventory and record console information
  - Verify Cryptor's have all necessary encryption keys
  - Set the default system wide patch key

Last but not least…….

None of this would be possible without the hardwork of the Radio Programming Unit (RPU) and Template Design Unit (TDU)

Special thanks to Todd Velderman and Jerry Dubzak who are at the forefront of this effort.