MPSCS | Advisory
MICHIGAN'S PUBLIC SAFETY COMMUNICATIONS SYSTEM | RADIO PROGRAMMING & TEMPLATE DESIGN UNIT

Minimum Subscriber Radio Encryption Recommendations

Encryption algorithms in use today on MPSCS

- ARC4 *(ADP)*
- DES-OFB *(Hardware-based only)*
- AES256 *(Hardware-based only)*

__Note__: Software-based encryption is not supported for DES-OFB and AES256 algorithms on MPSCS, even-though some manufacturers may offer this as an option. It is recommended that only hardware-based encryption options be considered when selecting subscriber radio equipment.

As of 2022, __ARC4 (ADP)__ is __NO LONGER INCLUDED BY DEFAULT__ when ordering new subscriber radio equipment and cannot be purchased separately when utilizing any DHS grant-based funding, without also including the AES256 option as the primary encryption algorithm. When purchasing subscriber radio equipment, it is imperative that you ensure your vendor is requesting ARC4 (ADP) alongside of the additional DES-OFB and AES256 formats to ensure your radio equipment maintains interoperability across MPSCS.

Multikey Option

This option allows for several encryption keys to be loaded into a single radio and is necessary for interoperability across MPSCS when encryption is required.

Example, with this option, the following encryption keys can be loaded into a radio:

MPSCS ADP *(**CKR 169**)* = used on numerous talkgroups throughout MPSCS
MPSCS DES *(**CKR 152**)* = used on statewide I-Event & J-Event talkgroups
MPSCS SYSWIDE *(**CKR 796**)* = future AES256 systemwide Patch/Failsoft/Private Call
MPSCS LAW AES *(**CKR 1667**)* = AES256 Statewide Law Enforcement Common
MPSCS FE AES *(**CKR 1668**)* = AES256 Statewide Fire and EMS Common
MPSCS COM AES *(**CKR 1669**)* = AES256 Statewide All Agency Common

OTAR with Multikey Option **Enhanced Security Upgrade Option**

This option replaces the standard Multikey option noted above and allows for "*Over-the-Air Rekeying*" exchange of encryption keys. This is an enhanced security option, which allows for frequent encryption key changes and "*one time provisioning"* of subscriber radios, which allows for dynamic field updates without physically touching the subscriber radio to address security concerns. This option is ideal for covert operations and tactical units to ensure high levels of security.

__Note__: without one of these two options, a radio can only contain a single encryption key, which does not support encrypted interoperability across MPSCS and further complicates interoperability with your neighboring agencies!

Example minimum subscriber radio specifications:

Motorola Solutions, Inc.

APX models *(all models *EXCEPT APX 900, APX 1000, APX 1500, APX 4000, and APX N30)*

Minimum recommended options:

- H38/G51 SMARTZONE Systems Operation
- Q806/G806 ASTRO Digital Operation
- Q173/G173 SMARTZONE OMNILINK Multizone Operation
- Q361/G361 ASTRO 25 9600 Baud Trunking Systems Operation
- QA00569/GA00244 700/800 MHz
- QA00580/ GA00580 TDMA Operation *(recommended for all new radio purchases)*
- **Q667/G193 Advanced Digital Privacy Software**
- **Q15 ADP, AES256, DES-OFB Encryption**
- **H869/W969 Multikey**

**APX 900, APX 1000, APX 1500, APX 4000, and APX N30 models are incompatible for MPSCS encryption interoperability standards and therefore are not recommended for any public safety users.*

JVCKenwood / EF Johnson

Viking VPx000/VMx000 *(all models EXCEPT VP5430)*

Minimum recommended options:

- 8322000002 P25 Conventional
- 8322000005 P25 Phase 1 Trunking
- 8322000006 P25 Phase 2 TDMA *(recommended for all new radio purchases)*
- **8323000004 DES-OFB and AES256 *(includes Multikey)***
- **8323000005 ARC4 Encryption**

Viking VP5430 model

Minimum recommended options:

- 8322000002 P25 Conventional
- 8322000005 P25 Phase 1 Trunking
- 8322000006 P25 Phase 2 TDMA *(recommended for all new radio purchases)*
- **KWD-AE30K Encryption Hardware Module**
- **8323000004 DES-OFB and AES256 *(includes Multikey)***
- **8323000005 ARC4 Encryption**

Kenwood NX/TK series *(includes all models)*

Minimum recommended options:

- KWD-5100CV P25 Conventional
- KWD-5101TR P25 Phase 1 Trunking
- KWD-5102TR P25 Phase 2 TDMA *(recommended for all new radio purchases)*
- **KWD-AE31K Encryption Hardware Module DES-OFB & AES256 *(includes Multikey)***
- **KWD-5107EE ARC4 Encryption**

**KWD-5006DE DES 4 Key option is not supported on MPSCS*

***Due to ARC4 encryption limitations, Kenwood NX/TK series models not recommended for any public safety users within the region 2 / Wayne County area.*

L3Harris

XL series *(includes all models *EXCEPT XL-45P and XL-150P)*

Minimum recommended options:

- YRXL-PKGPT P25 Phase 1 Trunking
- YRXL-PL4F P25 Phase 2 TDMA Trunking *(recommended for all new radio purchases)*
- YRXL-PL9F P25 Conventional Fallback *(required for Motorola Failsoft support)*
- **YRXL-PKG8F DES-OFB & AES256 Encryption *(includes Multikey)***
- **YRXL-PL8Y ARC4 Encryption Lite**

Tait Communications

TP/TM series *(includes all models *EXCEPT TP9100 and TM9100)*

Minimum recommended options:

- TPAS050 P25 Common Air Interface
- TPAS055 P25 Phase 1 Trunking
- TPAS091 P25 Phase 2 TDMA *(recommended for all new radio purchases)*
- **TPAS057 DES Encryption**
- **TPAS058 AES Encryption**
- **TPAS102 ARC4 Encryption**

*** TPAS053 Single DES Encryption and TPAS109 Single Privacy Key features are not supported by MPSCS*

BK Technologies

BKR-9000 series *(includes all models)*

Minimum recommended options:

- BKR0579 P25 Phase 1 Trunking
- BKR0593 P25 Phase 2 Trunking *(recommended for all new radio purchases)*
- **BKR0574 AES256 Encryption *(includes ARC4, DES-OFB, and Multikey)***

**BK Technologies radios are incompatible for MPSCS encryption interoperability standards within region 2 / Wayne County area due ARC4 encryption limitations; therefore, these radios are not recommended for any public safety users in that geographical area.*

If there are any questions concerning this advisory notice or you would like assistance reviewing a quote to ensure conformance to the minimum recommended specifications, please contact the MPSCS Radio Programming Unit.

Phone: 517-333-2720
Email: MPSCS-RPU@michigan.gov