Connecticut Interoperable Communications Executive Committee

ADOPTED TECHNICAL STANDARD

SUBJECT: **INTEROPERABLE ENCRYPTION**

ISSUE/REVISION DATE: Adopted February 16, 2016

PURPOSE: The purpose of this Standard is to provide a mechanism for interoperable encrypted communications among local, state, and federal government agencies. This Standard does not require the use of encryption by any agency.

DISCUSSION: The use of encryption among public safety agencies is growing as the use of digital radio systems is increasing and the cost of encryption is decreasing. The use of encryption adds a layer of complexity to the ability to interoperate but doesn't preclude the ability to interoperate between properly equipped local, state, and federal agencies. Proper preplanning, communications, and preplanning is required to achieve interoperability. This Standard does not require the use of encryption by any agency nor does this Standard dictate when encryption is to be used. This Standard simply enables the ability to interoperate in an encrypted manner should the ability be desired.

REFERENCE:

- Federal Partnership for Interoperable Communications *FPIC Guidelines or Encryption in Land Mobile Radio Systems*
- National Law Enforcement Communications Center – DHS/CBP
- Region 19 806 MHz NPSPAC Regional Plan
- FCC Rules and Regulations 90CFR553 - Encryption

DEFINITIONS:

ADVANCED ENCRYPTION STANDARD (AES) – A Federally approved interoperable encryption standard adopted and mandated by the Federal Government using a 256 bit key.

COMMON KEY REFERENCE (CKR) – A common method to refer to an encryption key. In an OTAR system, each CKR contains two TEK's (one active/one inactive). This is a decimal value between 1 and 4095. This is also known as a "SLN."

CRYPTO PERIOD – The period of time that a Traffic Encryption Key is active.

DATA ENCRYPTION STANDARD (DES) – An encryption standard using a 56 bit key that was previously approved by the Federal government. This standard is no longer certified by the Federal government but is still in widespread use.

KEY ID (KID)/"SELECTABLE ADP KEY ID" – Provides a unique address to identify a Traffic Encryption Key. This is expressed as a hexadecimal value between 0000 and ffff. The KID, along with an algorithm identification value is sent as part of the P25 data stream. It is from this information that the radio understands what key to use to decrypt information sent.

KEY MANAGEMENT FACILITY (KMF) – A powerful secure computer that serves as an application server and key material storage facility. The KMF can create, store, and manage keys.

RADIO SET ID (RSI) – A unique identifier for each unit in an OTAR system.

OVER THE AIR REKEYING (OTAR) – Message either to or from the KMF to provide encryption information to a radio, such as a request for an encryption key, keyset changeover, etc.

PROPRIETARY ENCRYPTION – An encryption algorithm that is not adopted as a standard.

RADIO SET ID (RSI) – A unique identifier for each unit in an OTAR system.

STORAGE LOCATION NUMBER (SLN): A common method to refer to an encryption key. In an OTAR system, each SLN contains two TEK's (one active/one inactive). This is decimel value between 1 and 4095. This is also known as a "CKR."

STATE LEVEL INTEROPERABILITY KEY – An encryption key provided by the Department of Homeland Security, Wireless Secure Operations Center for the purposes of interoperability.

TRAFFIC ENCRYPTION KEY (TEK) – The unique hexadecimal key used to encrypt and decrypt voice and data traffic. The length of the TEK depends on the algorithm used.

1.0 Accepted Standard(s)

1.1 The Connecticut standard for encryption is the 256 bit Advanced Encryption Standard (AES).

1.2 Legacy Data Encryption Standard (DES) users will continue to be supported for legacy users only however users are encouraged to transition to AES as is practical.

1.3 Proprietary encryption standards will not be supported for the purposes of interoperability.

2.0 Storage Location Number/Key ID Assignment Coordination

2.1 To avoid future conflict, it is a best practice to coordinate the assignment of Storage Location Number(SLN) and Key Identification (KID) assignments.

2.1.1 Duplicate SLN and/or KID assignments can impede interoperability

2.1.2 Conflicting SLN and/or KID assignments can impede the ability to rekey a radio via OTAR

2.2 Agencies wishing to participate in an interoperability key system should coordinate SLN and KID assignments.

2.2.1 Contact the DESPP CTS Unit at (860) 685-8280 to request SLN and KID assignments

2.2.1.1 Information required includes: Number of SLN/KID's requested and algorithm used

2.2.1.2 Agencies using proprietary encryption algorithms are encouraged to also coordinate SLN and/or KID assignments to avoid potential future conflict.

3.0 Interoperability Keys

3.1 The Federally issued State Level Interoperability Keys are designated as the common keys for interoperability between local, state, and federal agencies.

3.1.1 The designated Federal Interoperability Keys will be the only encryption key permitted to be used on the 700 MHz interoperability channels.

3.2 The State will designate a separate, common statewide AES encryption key for interoperability between local and state agencies.

3.2.1 Local or state agencies may use this common statewide interoperability key for day-to-day operations if so desired.

3.2.2 The crypto period for the Statewide AES key will be essentially static to accommodate system without access to the State OTAR system.

3.2.2.1 Any compromise of the Statewide AES key will result in a key change.

3.2.2.2 Users of the Statewide AES key will be notified of the availability of the new key.

3.3 Agencies requesting access to the Federal State Level Interoperability Key and/ or the Statewide AES key will need to make arrangements with the DESPP CTS Unit to obtain these keys.

3.3.1 Inventory information on all radios loaded with either of these interoperability keys needs to be forwarded to the DESPP CTS Unit.

3.3.1.1 Information required includes: Manufacturer, model of radio, serial number, RSI and/or OTAR ID, and point of contact.

3.3.1.2 Users of the State Key Management Facility (KMF) must use the adopted State P25 ID Schema.

3.3.2 Any compromise of any radio loaded with either Interoperability key needs to be reported as soon as possible to the DESPP Network Control Center (NCC) at 860-685-8008 for notification to the CTS Unit.

4.0 Subscriber Unit Recommendations

4.1 All encryption should be mode slaved to avoid confusion regarding transmitting clear versus encrypted transmissions.

4.1.1 Consideration should be given to having user selectable keys for use on common interoperable resources.

4.2 All radios employing encryption must have a readily accessible control that permits the radio user to disable encryption while using the 700 MHz interoperability channels.

4.3 Training regarding the use of encryption is highly recommended prior to the deployment of encryption with periodic retraining to be conducted thereafter.

RECCOMENDED FOR ADOPTION:

3/17/16
Chairman, Connecticut Interoperable Communications Executive Committee
Date

William J Hackett
3/18/16
Statewide Interoperability Coordinator
Date

APPROVED:

22MAR16
Deputy Commissioner
Division of Emergency Services and Homeland Security
Department of Emergency Services and Public Protection
Date