Policy 17-09 **June 8, 2017**

Voice Encryption

I. PURPOSE

This document sets forth the policies on Voice Encryption for radios and talk groups on the St. Louis Area Trunked Emergency Radio (SLATER) system as provided by the St Louis County Emergency Communications Commission (ECC).

II. GENERAL

Voice and data transmissions on public safety radio systems are much more prevalent today and are increasingly used to transmit sensitive data on first responder activities, as well as Personally Identifiable Information (PII).

The ECC owns and operates the SLATER system, a digital Project 25 trunked radio system licensed by the Federal Communications Commission (FCC) that provides county and regional interoperable radio coverage for public safety agencies within St. Louis County.

III. DEFINITIONS

Advanced Digital Privacy (ADP): Proprietary encryption protocol.

Advanced Encryption Standard (AES): The Federal Information Processing Standards approved for cryptographic algorithm that can be used to protect electronic data. Advanced Encryption Standard algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Emergency Communications Network: St. Louis County staff employees of the ECC.

Encryption: The conversion of data into a form called cipher text that cannot be understood by unauthorized entities.

Key Material: A parameter used in conjunction with a cryptographic algorithm that is used to perform a cryptographic transformation.

Operations Committee: A committee established by the ECC to advise the Commission on setting minimum standards for all users tied to the SLATER system and to provide a mechanism to establish protocols for its use and resolve issues that may arise regarding use or design. (As described in Section 10.3 of the ECC By-Laws adopted February 8, 2010.)

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity; such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual.

Rebroadcast: To broadcast radio transmissions which are being simultaneously received from another source.

Streaming: A method of transmitting data over a computer network as a steady, continuous flow, allowing playback to proceed while subsequent data is being received from another source.

User Group: Six (6) individual groups of representatives from the specific disciplines on the SLATER system appointed by the ECC to provide broad based input in the development of standards, protocols, training and use of the system. (As described in Section 10.3 of the ECC By-Laws adopted February 8, 2010.)

IV. POLICY

The protocols authorized by this policy to be used for encryption are Advanced Digital Privacy (ADP); which is used for the encryption of general use talkgroups (i.e. dispatch, tactical, support, etc.), and Advanced Encryption Standard – 256 bit (AES-256); which is used for talkgroups requiring elevated secure communications (i.e. Intelligence Units, Special Operations, etc.).

A. The ECC has authorized the encryption of public safety voice transmissions for radios and consoles on the SLATER system. This encryption will help manage the risk to public safety personnel, the public by abetting criminal activity from intercepting first responder communications, the protection of sensitive information and PII.

B. Except as otherwise specifically provided herein, all User Agencies of the SLATER system operating on encrypted talk groups of the SLATER system are forbidden

from disclosing, directing, rebroadcasting or streaming encrypted radio transmissions or any of their contents and/or manipulation of equipment on the SLATER system.

C. It shall not be a violation of this policy for any investigative or law enforcement officer or emergency medical services provider to disclose contents of encrypted radio transmissions to another investigative or law enforcement officer or medical services provider to the extent that such disclosure is appropriate to the official duties of the officer or medical services provider making or receiving the disclosure.

D. The ECC owns the key material used for the encryption of radio transmissions and is responsible for the protection and maintenance of all keys. For security protection ECN staff will not release encryption key information to any agency, individual or vendor without authorization from the Radio Systems Manager.
If it has been determined the key material has been compromised to the detriment of its intended purpose, the ECC is authorized to issue the reprogramming of radios to update the key material.

E. Use of encryption on interoperable talkgroups is prohibited unless authorized by the ECC Operations Committee and proper communication plans are established.

F. The tampering, alteration, and distribution of encryption program settings and key material is strictly prohibited.

V. PROCEDURE

A. Encryption Application and Monitoring

1. Applications (ECC Form #17-XX) requesting talkgroup encryption must be submitted through the appropriate User Group (i.e. fire, police) for preliminary approval prior to submission to the ECC Operations Committee.

2. The Radio Services Manager is responsible for the installation, maintenance and upgrade of the encryption keys and encryption programming.

3. As part of daily operations the Radio Services Unit shall monitor the SLATER system to assure operational efficiency. During monitoring the Radio Services Unit shall assure the encryption feature installed on various talk groups has not been compromised by internal programming error or intentional rebroadcasting or streaming.

B. SLATER System Users

Public Safety agencies operating their own communication center on a specifically assigned talk group(s) for their agency and/or contract agencies are responsible for monitoring and reporting any anomalies, rebroadcasting or streaming of encrypted voice radio transmissions to the Radio Services Manager immediately upon discovery.

C. Reporting

1. The Radio Services Manager will report monthly to the ECC on the status of the violations to this policy as part of the Radio Services Unit report.

2. Upon discovery of tampering, rebroadcast, or streaming of an encrypted talk group, the Radio Services Manager will report the preliminary findings to the Director of the Emergency Communications Network (ECN). The Director, or his designee, shall notify the ECC members in writing of the incident, any findings into the source of the encryption rebroadcast or streaming, and a recommended course of action. Initially notification to the ECC members will be via email. A formal report on the discovery and detailed actions of the ECN staff will be provided at the next regular ECC monthly meeting.

D. Investigation

1. Internal investigations shall be conducted by ECN staff with the assistance of contractor vendors and/or consultants, if needed. The St. Louis County Counselor's Office will be notified of the investigation, steps taken during the course of the investigation and, if necessary, provide legal advice throughout the course of the investigation.

2. If warranted, staff will notify the FCC of possible federal violations and request the assistance of the FCC to further the investigation.

3. ECN staff will work cooperatively with local, state and federal law enforcement investigators to investigate the incident and pursue criminal prosecution if appropriate.

E. Remediation

At the direction of the ECC, several forms of remediation shall be employed to resolve the encryption violation.

1. A formal notification from the ECC Chairman advising the agency chief executive officer (i.e. mayor, city administrator, district board of directors, chief) of the source radio unit of the violation and directing the "cease and desist" of the rebroadcast or streaming in lieu of radio unit shut-off/inhibited. The formal notification will further advise if the rebroadcast or streaming continues 24 hours after notice, the radio unit will be inhibited.

2. ECN staff shall work with the County Counselor's office to determine and pursue appropriate legal action.

3. If the source of the rebroadcast or streaming continues following formal notification, the ECN Director has the authority to direct the Radio Services Unit to inhibit the identified source radio unit based on the risk to public safety personnel, sensitive operational plans and/or PII.

VI. MEMORANDUM of UNDERSTANDING

This policy is covered under the MOU signed previously by each public safety user and outside agency user on the SLATER system.

Approved by the Emergency Communications Commission on June 8, 2017

Captain Steve Sack
Director,
Emergency Communications Network

William Karabas
Chairman,
Emergency Communications Commission