Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

ISICS Standard:	**Standard #:**	2.12.4
Defining and Encryption Key Compromise	Date Adopted:	06/09/2022
	Date Reviewed:	
	Version:	

1. Purpose or Objective

To outline and define the conditions and resolution of a potential or confirmed traffic encryption key (TEK) compromise on the Iowa Statewide Interoperable Communications System (ISICS) Platform.

2. Technical Background

- **Capabilities**

  A TEK is used to encode the radio transmission in a manner that prevents scanners and unauthorized radios from receiving and/or transmitting audio.

  The ISICS Platform brings certain capabilities to mitigate some effects of a suspected or confirmed compromise such as inhibiting a radio and over-the-air-rekeying (OTAR).

- **Constraints**

  ISICS Standard 2.12.3 – Encryption Key Security outlines security practices for TEKs for additional information. However, it does not define a compromise.

  Updating of TEKs can be time and labor intensive and come with significant cost depending on the capabilities of each agency.

3. Operational Context

A compromised TEK may allow unauthorized persons to monitor sensitive communications during an event that could jeopardize the mission and safety of personnel.

Proper definition of a key compromise is essential to ensuring that secure communications are available for sensitive missions while limiting impacts on agencies if a TEK needs to be updated.

4. Recommended Protocol/Standard

Local System Administrators (LSA) and end radio users are responsible for maintaining control of their equipment that stores any TEKs or other sensitive ISICS information. Any loss or suspected compromise must be reported immediately along with supporting evidence.

The ISICS System Administrator (SA) will monitor the ISICS secure interoperable talkgroups for any possible compromise.

If any verified compromise is noted, the ISICS SA will take appropriate action.

5. Recommended Procedure

ISICS LSAs and end radio users are responsible for maintaining control of their equipment that stores any TEKs or other sensitive ISICS information. This includes terminal subscriber radios and key fill devices (KFD) which may also referred to as a key variable loader (KVL). Any subscriber radio with TEKs stored in it must be noted in each LSA's inventory in addition to any KFDs.

If a suspected lost radio is noted, the LSA must report it to the ISICS SA immediately along with any evidence of compromised communication. The report must also include the subscriber unit ID (SU ID).

If a KFD is suspected to be lost, it must be reported immediately to the ISICS SA as this is considered a major security breech.

If the ISICS SA notes any SU IDs that are not on an inventory provided by the LSA that affiliate to an encrypted interoperable talkgroup, the ISICS SA will report it to the LSA.

In addition, any disposals of subscriber radio equipment shall be consistent with ISICS Standard 2.13.1 – Subscriber Radio Disposal. It is also recommended that the radio's crypto module be zeroized before a radio is sent in for maintenance if possible.

Coordination between the ISICS SA and LSA will dictate the appropriate course of action.

6. Management

The ISICS SA and LSAs will be responsible for ensuring that all subscriber radios and KFDs are noted and maintained on applicable inventory(-ies). The ISICS SA and LSAs shall also coordinate with the Operations and Technology Committees to ensure this standard is reviewed as deemed necessary for accuracy, efficacy and completeness.