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

ISICS Standard:	**Standard #:**	2.12.6
Over the Air Rekeying	Date Adopted:	06/09/2022
	Date Reviewed:	
	Version:	

1. Purpose or Objective

To outline the roles and responsibilities of the ISICS System Administrator (SA) and local subsystem administrators (LSA) with respect to over the air rekeying (OTAR) of subscriber radio units on the Iowa Statewide Interoperable Communications System (ISICS) Platform.

2. Technical Background

- **Capabilities**

  A traffic encryption key (TEK) is used to encode the radio transmission in a manner that prevents unauthorized radios from receiving or transmitting audio. Each TEK is stored within a hexadecimal key identification number (KID) that is associated with a decimal storage location number (SLN). Some manufacturers may refer to a SLN as a common key reference (CKR). See ISICS Standard B.B.B – Encryption Key Storage Location Number and Key ID for more information on assigned SLNs and KIDs.

  Modern APCO Project 25 (P25) subscriber radios on ISICS may have the ability to be provisioned and have their encryption material managed and/or updated remotely with OTAR that takes place over the common air interface (CAI). This is accomplished via a key management facility (KMF) if the subscriber radio is equipped with those associated features. The use of a KMF can save the time of service technicians that would be keying and rekeying ISICS subscriber radios and limit potential down time of equipment.

  When a P25 subscriber radio attempts to update its installed TEKs via OTAR, it must communicate with the KMF using a unique key encryption key (UKEK) that is assigned to it via the KMF or a trusted technician via key fill device (KFD) in addition to a unique

radio subscriber ID (RSI). When the subscriber radio communicates with the KMF over the air, the UKEK prevents unauthorized persons from intercepting and deciphering the updated TEK through the CAI.

- **Constraints**
    - In the past, updating TEKs in radios was time consuming and necessitated downtime of equipment and in some cases removal of personnel from the field. This was due to subscriber radios needing to be provisioned by a trusted technician using a KFD. During this provisioning, all associated encryption material is input into the subscriber radio.

      Even with OTAR, subscriber radios must still be provisioned by a KFD upon programming to input a provisioning key encryption key (PKEK) that may be used for provisioning by the KMF. Upon first affiliation with the KMF, the PKEK installed in the subscriber radio is updated to a UKEK.
    - Proper coordination must be conducted to ensure that roles and responsibilities are clear and well understood to prevent mishandling or incorrect rekeying of subscriber units utilizing OTAR. If processes are not followed, subscriber radios may not receive the correct TEKs which can prevent successful transmission of audio to operators during critical and/or sensitive operations.
    - If a subscriber radio is not active when the KMF sends notice to subscriber radios that new key material is available, that radio may miss the update. Agencies can circumvent this potential failure by ensuring that a 'Rekey' button is available on the radio menu, and that end-users are trained in the use and operation of the 'Rekey' button.
    - In addition, expectations of functionality need to be established among the ISICS SA and LSAs to define roles and establish processes for encryption key management. See ISICS Standard 2.12.3 – Encryption Key Security for additional information.
    - Capabilities of the KMF will change regularly with new features. These new features need to be evaluated and possibly incorporated into policy, standards and/or procedures to ensure effective use of equipment.

3. Operational Context

Agencies that have investigated encrypted radio traffic should take every reasonable measure to define their operational adversaries for each aspect of their operational picture before deployment. As an example, agencies may find that the update cadence of encrypted talkgroups utilized by a specialized drug enforcement task force is different than a standard operational talkgroup.

4. Recommended Protocol/Standard

The ISICS SA and LSAs are responsible for coordinating the use of SLNs and KIDs across the ISICS Platform. Certain SLNs and KIDs are reserved for the regional and statewide interoperable talkgroups and have been registered with the National Law Enforcement Communications Center.

Assignment of the KMF RSI for each subscriber radio is outlined in the ISICS Programming Guide and is considered non-public information under Iowa Code 22.7(50).

The preferred method for subscriber radios is that UKEKs shall be assigned and entered into a radio upon programming and provisioning with a KFD. Those UKEKs shall be coordinated with the ISICS SA for entry into the KMF. In certain instances, a PKEK can be used for mass provisioning of subscriber units. Upon first affiliation with the KMF, the PKEK shall be updated to a UKEK.

The ISICS SA is responsible for global settings within the KMF. Global settings are defined as settings that will cause changes in subscriber radios across multiple agency jurisdictions. This includes but is not limited to:

- Changing primary active key to secondary inactive within the KMF software interface. Updating this setting will affect all subscriber radios utilizing the ISICS KMF and should not be done unless absolutely necessary.
- Updating TEKs associated with the interoperable talkgroups defined in ISICS Standard 1.5.0 – ISICS Regional and Statewide Interoperability Talkgroups and listed in the ISICS interoperable fleetmap. This includes key material and update cadence.

ISICS LSAs, if a KMF control interface is purchased via the Customer Enterprise Network (CEN), will have access to:

- Update TEKs on their operable talkgroups
- Update TEKs on their local interoperable talkgroups
- Overwriting/replacing TEKs listed in the primary active key and inactive key for a local operable or interoperable talkgroup via CKR/SLN Refresh.

Before any changes are conducted with encrypted talkgroups, it is vital to notify affected agencies to ensure operations can continue without interruption and to minimize the potential for failure.

There may be situations that would necessitate a short-notice or emergency update where encryption material has been compromised. An example of this is a lost key fill device which is a major security breech as defined in ISICS Standard 2.12.4 - Defining an Encryption Key Compromise.

Proper notification shall be given for any encryption key updates to agencies affected. The ISICS SA shall notify all LSAs and other stakeholders of an impending key update of the regional and statewide interoperable talkgroups in accordance with ISICS Standard 4.8.0 – Notification for System Outages and Changes. In addition, notification 90, 60, 30, 15, 10, 5, 4, 3, 2 and 1 day(s) prior to any planned update. Once the update is pushed out, the authorized users are responsible for updating the key material and notifying their LSAs that the update has been completed. The LSAs shall then notify the ISICS SA that the update has been completed.

Other notification methods used shall include but not be limited to:

- Iowa Law Enforcement Information Network (LEIN) bulletins;

- ISICSB Committee and Subcommittee meetings;
- Association meetings such as Iowa State Sheriff's and Deputies Association, Iowa Firefighter's Association, Iowa Emergency Management Association, Iowa EMS Association, etc.

LSAs are required to notify their local agency users and other agencies they have shared their TEKs with to ensure they prepare to receive those updates. Contact with the affected agencies by the LSAs is recommended to be done at 90, 60, 30, 15, 10, 5, 4, 3, 2 and 1 day(s) prior to any planned update. An example of this would be a specialized shared talkgroup that is intended to be operated in an encrypted configuration.

In the event of a compromise, the ISICS SA and LSA shall coordinate or meet daily to ensure that necessary updates are completed as expeditiously and completely as possible. Local agency users shall work with their LSAs to ensure the updated key material is applied as quickly as possible.

In order to increase the probability of OTAR success on end-user subscriber radios, trusted technicians should ensure that any agency utilizing OTAR has a 'Rekey' menu option available to end users if it is available. A 'Rekey' button will force the radio to attempt to communicate with the KMF and request updates to all TEKs that are currently in that subscriber radio. If this option is not available to the end users, they may miss an OTAR update and have to use other methods to get updated encryption material.

5. Recommended Procedure

A. Pre-update:

Upon notice from the ISICS SA and/or LSAs that an update to encryption key material is expected, LSAs and end users should verify at the beginning of their first shift after notification of an update has been received in order to ensure that the subscriber radio has the most current version of the key material in order to appropriately plan for the update. This can be accomplished by the review of the OTAR data logs from the KMF by the ISICS SA and LSAs. If there are noted failures by subscriber radio IDs, the LSAs shall contact those users to encourage them to utilize the menu 'Rekey' button if enabled on the subscriber unit.

If an end-user has a question whether their radio subscriber has the latest key material, that user can utilize the 'Rekey' option to ensure the encryption material in the subscriber radio is current.

Proper notification shall be given for any encryption key updates to agencies affected as stated in Section 4 of this standard.

B. Updated TEK Deployments:

There are two primary methods for updating TEKs and/or active TEKs in end user subscriber radios—rollover and SLN/CKR Refresh.

Rollover is a global setting utilizes a changeover from an active KID/TEK in a radio to the inactive KID/TEK. This is a global setting that will affect every radio under an

agency profile and should only be done with proper coordination with all LSAs under that profile and the ISICS SA.

CKR/SLN Refresh is a process that will update KID/TEK pairings in the KMF and end user subscriber units that have the CKR/SLN entered into the subscriber unit. CKR/SLN Refresh is the preferred method for agencies that wish to update encryption material at a more frequent cadence since agencies can choose to update a specific TEK without affecting other TEKs and subscriber radios.

In the event of a compromise, the ISICS SA and LSAs shall coordinate or meet daily to ensure that necessary updates are completed as expeditiously and completely as possible. Local agency users shall work with their LSAs to ensure the updated key material is applied as quickly as possible following methods outlined above. In this instance, a Rollover may be the preferred method depending on the severity of the compromise.

C. Post-Update Verification:

During a TEK update cycle, the ISICS SA and LSAs shall run daily reports on the KMF to verify which subscriber units have successfully completed the update. Notification shall be sent to agencies notifying them of which radios have yet to complete the update so the update can be completed.

6. Management

The ISICS SA and LSAs will be responsible for ensuring that all radios are keyed and updated at appropriate intervals. The ISICS SA and LSAs shall also coordinate with the Operations and Technology Committees to ensure this standard is reviewed for accuracy, efficacy and completeness.