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

ISICS Standard:	**Standard #:**	2.12.2
Subscriber Security with Advanced System Keys	Date Adopted:	06/12/2018
	Date Reviewed:	
	Version:	V2

1. Purpose or Objective

The purpose of this standard is to ensure radio subscriber security with the utilization of radio system keys and describe proper management of radio system keys. Radio system keys have definable security options used for programming subscriber radios.

Individual manufacturers of radios have different system key capabilities in managing radio security.

2. Technical Background

- **Capabilities**

  The advanced system key (ASK) adds security to radio programming and may include programming options such as, who can program the radio, radio and talkgroup ID limitations, system ID limitations, key expiration dates, and limitations on replication of the key.

  Some brands of radio can also be password protected, which prohibits anyone without the password from reading or modifying the radio.

  ASKs are created from the primary/master advanced system key. The primary ASK is only used to create distributed ASKs and is not used to program equipment.

- **Constraints**

  Using an ASK creates an increased hardware cost over the use of a regular system key.

System key can also refer to a file utilized for programming, the ISICS system allows only advanced system keys and programming with hardware (a USB dongle) and does not allow for software system keys.

All ISICS users will have to sign for and incur all costs and liability associated with each ASK.

3. Operational Context

There will be one "Primary" or "Master" advanced system key per vendor which is held by the ISICS system administrator. The ISICS system administrator will develop all advanced system keys (ASKs) from the primary advanced system key with proper provisioning for user specific requirements to allow subscriber programming. The system administrator will track all created keys in a secure location. System key security is required to protect the integrity of the ISICS system.

There are many different names for advanced system keys. They may also be referenced as ASK, distribution keys, child keys, and daughter keys among other names. They all refer to a USB stick that contains programming permissions to access the ISICS platform.

All ASKs generated by the system administrator will have an expiration date set to assist in system security and integrity and of tracking distributed keys.

- Key expiration dates for system partners/subsystem administrators = 3 years
- Key expiration dates for trusted technicians and third-party service shops = 2 years
- Key expiration for an unlimited system key will be set to six months and will not be available to third-party service shops
    - Shorter expiration dates can be programed into the distributed ASK at the recipient agency request.

System partners and trusted technicians must consent to the following:

- Background checks through the Iowa Department of Public Safety.
- Follow all ISICS standards, policies, and procedures.
- Only program radio equipment you have written consent to program.
- Properly program all radios and other devices to ensure there is no degradation or loss of use of access by any user.
- Programming equipment per ISICSB Standard 1.7.0- minimum programming standards.

Password protection features, which add a layer of security to the radio programming are at the discretion of the individual agencies who manage those radios.

Any attempt to duplicate, elevate, or otherwise alter an ASK without consent of the ISICB may result in revocation of any/all ASKs by the ISICS system administrator.

Any attempt to add an unauthorized radio on the system with a programmed ASK without the consent of the ISICSB may result in revocation of any/all ASKs by the ISICS system administrator.

Agencies having an ASK can lend their key to third-party shops for radio programming, but the agency is responsible for any programming actions performed with the key.

4. Recommended Protocol/Standard

Any agency needing an ASK created from the primary system key will purchase their own dongle and provide it to the ISICS system administrator for programming.

The ISICS system administrator will program keys with the limited ID range needed by the recipient agency for their operational needs. Ranges can be added or changed as needed by having the ASK reprogrammed by the system administrator.

5. Recommended Procedure

The ISICS system administrator holds the primary advanced system key for each vendor. It is also the distribution point for system partner agencies and third-party service shops. The system administrator will create advanced system keys from the primary advanced system key and distribute to those agencies meeting the required criteria and having the required agreements in place to be on ISICS. Agencies provide their own programmable dongle to be programmed.

All Advanced System Keys programmed will be documented and logged.

ASKs will be programmed by the system administrator with the ID range limited to that designated to the recipient agency as required for their operational needs. ASKs that need an authorized change to the ID range will be provided back to the system administrator who can make those changes to the programming.

6. Management

The ISICS system administrator or designee is responsible for the distribution of the ASKs.

Subsystem administrators who have received an ASK are responsible for the management of the key for their respective agencies.

System partners and third-party service shops are responsible for providing keys to the system administrator for updated expiration dates.

ISICSB reserves the right to revoke the ability to possess a key if the agency's possession affects the integrity and/or security of ISICS.

Password protection of radios is entirely under an individual agency's management and discretion.