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

Standard Name:	**Security "System Keys"**		Date Created:		**05-08-2018**	
Standard Policy #	**2.12.2**	Section Title**:**	**Management of System**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**06-12-2018**	Reviewed:	**06-12-2018**

1. Purpose or Objective

The purpose of this standard is to establish policy and procedures for radio subscriber security; in particular, management of the "Radio System Keys," which are used for programming subscriber radios with definable security options.

Individual manufacturers of radios have different System Key capabilities in managing radio security, so this standard is split into sections based on System Key capability.

2. Technical Background

Capabilities

The System Key adds security to radio programming and may be programmable with options, such as who can program the radio, Radio ID limitations, System ID limitations, and how long a system key will last before expiring. An Advanced System Key (ASK) also has the capability of not being replicated, unlike a regular System Key.

Some brands of radio also have the security option of being password protected, which prohibits anyone from reading or modifying the radio without the password.

Constraints

If an Advanced System Key is used, there is an increased hardware cost. The key itself is a purchasable hardware button, requiring a reader adapter for the computer.

There are many different names for Advanced System Keys. They may also be referenced as Child Keys, Daughter Keys Among others. They all refer to a USB stick that contains programming permissions to access the ISICS Platform.

3. Operational Context

The purpose of a System Key is to increase security around the programming of subscriber radios. Details for the management of the keys are defined under sections 4 and 5 of this State Standard.

If a radio is capable of password protections, this also adds a layer of security to the radio programming. Whether or not this feature is used is up to individual agencies managing the radios.

4. Recommended Protocol/ Standard

If a radio is under the responsibility of another administrator, do **NOT** program the radio without the permission of the administrator that is responsible for that radio.

All keys programmed and distributed will be logged and tracked.

Subsection for radios that are capable of the Advanced System Key feature
Agencies having an Advanced System Key can lend their key to third-party shops for radio programming, but the agency is responsible for any programming actions performed with the key.

Programmed keys can be updated in all parameters, with the exception of the time expiration.

5. Recommended Procedure

ISICSB holds the Master Advanced System Key. It is also the distribution point for system partner agencies and third-party service shops, with criteria that the receiving agency has met the requirements of any applicable standards and has the needed agreements in place to be on the system.

All Advanced System Keys programmed will be documented and logged.

Subsection for radios that are capable of the Advanced System Key Feature
Any agency needing an Advanced System Key will have to purchase their own I-Button Dongle and bring the blank key buttons to Statewide System Administrator for programming.

Key expiration will be set to two years for third-party service shops and three years for system partners.

Key expiration for an unlimited System Key will be set to six months and will not be available to third-party shops.

Programmed keys will be ID range limited to the range(s) needed by the recipient agency for their business needs; ranges can be added or changed as needed by having the key reprogrammed.

A tighter time restriction or other restrictions can be programmed into the distributed keys at the recipient agency's discretion.
Any attempt to duplicate, elevate or otherwise alter an Advanced System Key without consent of the ISICSB may result in revocation of any System Keys by the State System Administrator. The entity may appeal this decision to the ISICSB.

An attempt to add an unauthorized radio to the system with an already programmed Advanced System Key without consent of the ISICSB may result in revocation of any System Keys by the State System Administrator. The entity may appeal this decision to the ISICSB.

6. Management

Statewide System Administrator or designee is responsible for the distribution of the System Keys and Advanced System Keys.

Subsystem Administrators who have received a System Key or Advanced System Key are responsible for the management of the key for their respective agency.

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