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

Standard Name:	**Subscriber Security**		Date Created:		March 3, 2017	
Standard Policy #	**1.1.0**	**Section Title: Governance**	**Interoperability Guidelines**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**06/08/2017**	Reviewed:	**06/08/2017**

1. Purpose or Objective

The objective of this standard is to provide the proper guidance for "Radio System Keys" in order to ensure radio subscriber security is protected. By utilizing "Radio System Keys," the radios are able to be programed with the appropriate security options. To properly account for and represent the various system key capabilities available by different manufactures, each capability will be discussed in its own section.

2. Technical Background

- **Capabilities**

  The Iowa Statewide Interoperable Communications System Board (ISICSB) wants to ensure that the highest level of security is incorporated into the Iowa Statewide Interoperable Communications System (ISICS) in order to protect the integrity of its users and ISICS as a whole. Both System and Advance System Keys assist in accomplishing this task. Advanced System Keys allow for the following protections: restricting who is given access to program the radios and restricting radio and talkgroup IDs. Advanced system keys allow the user to determine how long the key will be operable. Advanced System Keys offer an extra layer of security for users as these keys are unable to be replicated.

Security options also vary by the radio brand the system user selects to access ISICS. For example, the radio might include an option to password protect the radio. This will allow the agency to prevent any modifications to be made to the radio settings without inputting the password.

- **Constraints**

  The Advanced System Key is determined by the vendor radio, and is configurable to allow enhanced security. The radio user will need to provide a configurable system key (child key, daughter key, slave key, distribution key, etc.) to be configured by the ISICS System Administrator (System Administrator) or the System Administrator's Designee (Administrator Designee) who is selected from a list of individuals approved by ISICSB.

  All ISICS users will have to sign for and will incur all the costs and liabilities associated with each key; absolving ISICSB and its representatives of any liabilities and/or costs associated with its use or impact from use of the key.

3. Operational Context

As mentioned earlier, the Advanced System Key is being utilized to increase security in the programming of the radios as well as protecting the integrity of ISICS. Please refer to Sections four and five of this standard for greater information regarding the management of the keys.

4. Recommended Protocol/ Standard

Do not program a radio you are not responsible for without written consent. Please note, if a key is programmed and distributed as "software and hardware," then the keys will be logged and tracked. The System Administrator will track all keys. The information will be stored on state secure servers internal to State of Iowa.

- **System Key Administration**

  There will be one Master System Key per vendor in the possession of the System Administrator. The System Administrator will develop all system keys (child key, daughter key, slave key, distribution key, etc.) with proper provisioning for user specific requirements to allow subscriber programming. ISICSB reserves the right to amend this policy at their sole discretion in order to increase the security and protect the integrity of the system.

All keys generated by the System Administrator will have an expiration date set, which will assist in increasing security and tracking the keys distributed to system users. 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.

- **Liability for the Misuse of the System Keys**

  Each agency must designate a governmental employee as representative and a governmental employee as alternate who will be responsible for obtaining and securing the system key(s). While not mandated, ISICS encourages agency users to create their own agency policy to ensure compliance. Both representatives will be required to sign for the key(s) and will agree to the following:

  1. The agency representative and agency alternate absolve ISICSB and ISICS representatives of all liability involving the loss or misuse of the system key(s) they signed for and took possession of for their agency.
  2. The agency representative and agency alternate will be personally and professionally liable for the misuse and/or loss of system keys while in their possession. The agency representative will not be liable for the loss or misuse of a system key while in the possession of the agency alternate or vice versus unless the agency user's policy assigns such liability. If this is the case, then ISICSB will follow the most stringent policy in determining liability and the ability for individual users to have future access to the system.
  3. All system users are mandatory reporters of misuse of ISICS. Failure to do so could result in the individual and/or agency who has knowledge of the misuse being permanently removed from the system. The agency representative and agency alternate agree to provide this requirement to all agency users.
  4. If the misuse and/or loss of a system key is discovered by the agency representative and/or agency alternate, then the violation must be reported orally to the System Administrator within 48 hours of obtaining this knowledge. This will allow for a cursory investigation by the individual agency user to ensure the information is accurate. ISICSB stresses the importance of reporting the misuse or loss of a system key if the agency cannot determine the credibility of the information received as a failure to report could result in the loss of the key or access to ISICS. The oral notification must be followed up with a written explanation to be submitted to the System Administrator within 48 hours of providing the oral notification. The System Administrator will forward the information to the Standards Coordinator within 24 hours of receiving the written notice. To protect the integrity and the security of the system, access to the system keys will be immediately suspended until the issue is resolved.

Please review the standard "Response to Non-Compliance" for additional information.

5. The misuse and/or loss of a system key could result in the agency representative's and agency alternate's access to ISICS being permanently revoked.

5. Recommended Procedure for System Keys

The ISICS System Administrator and his or her designee (System Designee) will be the keepers of the Master Advanced System Keys. The System Administrator and System Designee will distribute the provided key back to the entity for subscriber programming. The entities who receive the keys are responsible for documenting all keys that have been programmed. This information will be placed into a tracking spreadsheet. The System Administrator may contact the person responsible for the keys for auditing purposes.

- **Radios that are Capable of the Advanced System Key feature**

  Agencies will need to purchase a key reader and key buttons. The agency will be responsible to bring the blank key buttons to the System Administrator or System Designee to be programmed.

Key Expiration Dates

- System Partners: Two Years
- Trusted Technician: Three Years

System Partners and trusted technicians must consent to the following:

(1) Yearly Iowa Department of Public Safety Background checks, and

(2) Misuse of their position could result in access to ISCIS being revoked. Examples include but are not limited to the following: violation of one of the standards, his or her actions directly causes a failure to the system, accessing group and/or systems within ISICS he or she was not granted access, or failing to properly program in anyway a radio, other device which causes any misuse, degradation or loss of use of access of any user.

Programmed Key Range Usage

To ensure programed key are not misused, a range limit will be set for each ID based on the range the agency will need to conduct business. If a greater use is demonstrated, then the range will be able to be modified by reprogramming the key.

Time restrictions are mandatory restrictions by ISICSB.

Assumptions: In drafting this standard, the Standards Working Group assumes there will be individuals qualified to serve as the ISICS System Administrator (System Administrator) and the System Administrator's Designee (Administrator Designee), and these individuals will be able to successfully carry out their required duties.

Liabilities: The manner in which the standard is drafted, keeps a majority of the liability with the individual agency users and the individuals employed by ISICS to carry out the required duties. All liability cannot be discharged from the system as there are legal doctrines recognized by Iowa Code, such as the doctrine of respondent superior.

Cost: The cost of the standard is unknown. Some costs could include filling the position of ISICS System Administrator (System Administrator) and System Administrator's Designee (search, background checks, possible salary, etc.).