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

ISICS Standard:	Standard #:	3.11.0
Talkgroup Site Access and Roaming	Date Adopted:	07/12/2018
	Date Reviewed:	11/14/2024
	Version:	2.0

1. Purpose or Objective

This standard establishes guidelines for system and subscriber unit programming to provide ISICS users with wide area access, as needed, while minimizing roaming and preventing unnecessary system loading for the efficient use of system resources.

2. Technical Background

- **Capabilities**

  Subscriber units must be programmed in a manner that ensures users have access to necessary wide-area communications when required for mission-critical operations. Programming shall be done in accordance with the following guidelines:

  - **Talkgroup Management**: Users shall have access to wide-area talkgroups based on operational need and approved by the System Administrator.
  - **Channel Availability**: Subscriber units should be programmed to minimize simultaneous access to multiple wide-area talkgroups, prioritizing local talkgroups unless wide-area coverage is essential.

- **Constraints**

  Each ISICS repeater site has a limited number of channels able to provide talk paths available to carry radio transmissions. If care is not taken to program talkgroups and radios to be allowed only on certain sites or prefer certain sites, radio traffic could unnecessarily overburden a site preventing some radio messages from being sent.

Subscriber units shall be programmed to minimize roaming onto other regional or state systems unless required by operational needs. The following measures must be implemented:

- **Roaming Restriction**: Roaming shall be restricted to mission-critical instances, such as mutual aid or emergency response outside of the home coverage area.
- **Home System Priority**: Whenever possible, ISICS users should remain connected to the ISICS system to avoid unnecessary strain on foreign systems.
- **Local Site Restrictions**: Local Operational talkgroups should be contained to the local operational geographical area.

With respect to operable talkgroup site access, this standard only applies to state-owned tower sites. Local Sub-System Administrators who desire operable talkgroup access to other local sub-systems need to complete a Memorandum of Agreement between Sub-System Administrators/Owners.

Interoperable talkgroups shall be allowed access to local Sub-Systems.

3. Operational Context

Radio users may not have control over where their public safety responsibilities take them nor do they have the ability to control which repeater sites their radios affiliate. Site affiliation permission must be proactively managed by sound system and radio programming guidelines. Not all scenarios can be defined by standard so system administrators should communally develop and share best practices.

Subscriber units must adhere to the following programming standards:

- **Home Area Programming**: Subscriber units should be programmed with a primary focus on their home region, using local talkgroups and channels by default.
- **Wide-Area Talkgroups**: Access to wide-area talkgroups shall be limited and assigned based on operational necessity, with clear guidelines for activation and use.
- **Roaming Talkgroups**: Roaming talkgroups shall only be activated when necessary, and user agencies must ensure their units have the capability to roam when authorized.
- **Talkgroup Prioritization**: Critical talkgroups (e.g., emergency, command, and mutual aid channels) shall be prioritized in the programming of subscriber units.
- **Idle Time Management / Talkgroup parking**: Subscriber units that are not actively transmitting should minimize channel access to free up resources for other users.
- **System Access Control**: Access to wide-area channels or talkgroups shall be based on predefined operational needs and must be approved by the ISICS network management authority.

4. Recommended Protocol/Standard

Site Access Profiles define talkgroup access to ISICS repeater sites. They serve as the preferred tool for managing repeater site access. The following Site Access Profiles are established:

- In-County/Geopolitical Subdivision Operations: Includes all sites within a county or geopolitical subdivision and may include sites outside of the physical boundaries of the county or geopolitical subdivision but engineered to serve the county or geopolitical subdivision.
- Border (aka Adjacent Site): Includes all sites included in the In-County/Geopolitical Subdivision Operations profile plus one ring of adjacent repeater sites encircling the In-County/Geopolitical Subdivision Operations profile.
- Regional Sites: Includes all sites within a Homeland Security Region plus one ring of sites encircling the Regional Sites profile.
- Statewide Sites: Includes all ISICS sites.
- Custom Sites: Certain entities with atypical geographic boundaries may require a custom Site Access Profile. These profiles must be approved by the impacted site's owner and the Operations Committee.
- Requested Site: Profiles will always broadcast specified radio traffic regardless of site affiliation with the repeater site. Example: A rural county relies on another county's repeater sites for coverage in a border area and car-to-car traffic (utilizing an In-County Operations profile) is not carried through that neighboring county's repeater. Requested Site profiles must be approved and documented by the neighboring site's owner and the Operations Committee.

Deviations from these Site Access Profiles must be approved in writing by the site owner(s). Ownership is defined as who owns the physical site and who purchased RF channels found on that site. In the case of state-owned sites, Operations Committee will review the deviation and recommend action to ISICSB for final approval.

The following Site Preference procedures are established to define individual radio access to ISICS repeater sites.

- Generally, talkgroup personalities should not have special site access permissions as site access should primarily be managed by talkgroup properties as established in the system.
- Generally, talkgroup personalities should be set to prefer the home infrastructure of the radio owner over that of non-home infrastructure.
- Generally, talkgroups with wide area access (e.g. statewide) should be set not to prefer one repeater site over another.

Deviations from these Site Preferences must be approved in writing by the impacted site owner(s). Ownership is defined as who owns the physical site and who purchase RF

channels found on that site. In the case of state-owned sites, Operations Committee will review the deviation and recommend action to ISICSB for final approval.

The following is a Prohibited Action:
- Selecting a talkgroup (by choosing it as the transmit channel on a radio) for which one has no reasonable need to monitor (as defined by the impacted system administrator) is known as "parking on a talkgroup" and is prohibited. This does not prohibit one from including a talkgroup in a scan list while the radio is legitimately affiliated to another talkgroup.

Exceptions to any item in this standard should be decided on a case-by-case basis by either the Operations Committee or the Technology Committee and are subject to the ISICSB approval.

Emergency exceptions to this standard or emergency resolutions of site access issues may be temporarily authorized by agreement between a Subsystem Administrator and the Chair of ISICSB or the Chair of the Operations Committee (if the ISICSB Vice Chair is not available). Temporary authorization may exist until the next meeting of the Operations Committee or sixty days, no longer.

Paging devices, operating on the ISICS 7/800 MHz band, must be programmed to prevent unnecessary system loading. This includes limiting paging traffic and prioritizing critical alerts:

- **Talkgroup and Paging Prioritization**: Critical talkgroups and paging notifications on the 7/800 MHz band shall be prioritized in the programming of subscriber units and paging devices. (i.e. preferences to home tower sites for subscriber units)
- **Idle Time Management**: Paging devices that are not actively receiving alerts should minimize system access to conserve bandwidth and reduce system strain.
- **System Access Control**: Access to paging groups, particularly on the 7/800 MHz band, must be regulated and based on predefined operational needs approved by the ISICS System Administrators.

5. Subscriber Unit and Paging Device Programming Guidelines

Subscriber units and paging devices operating on the 7/800 MHz band must adhere to the following programming standards:

- **Home Area Programming**: Paging devices should be programmed to primarily receive alerts within their home region and avoid unnecessary traffic from other regions unless part of a specific operational group.
- **Wide-Area Paging Groups**: Access to wide-area paging groups should be limited to users who require statewide or regional notifications, with clear guidelines for use and deactivation when not needed.

- **Roaming and Paging Alerts**: Roaming paging alerts on the 7/800 MHz band shall only be enabled when necessary for mission-critical communication. Users must ensure that their devices have the capability to receive alerts outside their home area when authorized.

The preferred method of paging across ISICS is tones on a single talkgroup, this talkgroup is for receive only, 2-way voice transmission should be directed to a separate operational talkgroup.

Any agency wishing to page across ISICS will work directly with ISICS System Administrators on specific details.

6. Recommended Procedure

Subsystem Administrators are responsible for ensuring that radios and infrastructure under their control comply with this standard.

7. Management

ISICS administrators can monitor system loading and roaming activity. If unnecessary system strain is detected, programming adjustments will be required:

- **Usage Audits**: Agencies may be required to periodically review and update their programming to ensure compliance with ISICS standards.
- **Alerting**: System administrators may issue alerts if excessive roaming or system loading occurs, instructing agencies to take corrective action.

The Statewide System Administrator is expected to manage and enforce this standard. Conflicts should be handled through ISICS Standard 7.1.0 - Standards Compliance Evaluation / Non-Compliance Procedures.