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

ISICS Standard:	**Standard #:**	3.6.0
Radio Site Access Permission – Subsystem Roaming	Date Adopted:	04/12/2018
	Date Reviewed:	10/09/2025
	Version:	2.0

1. Purpose or Objective

The purpose of this standard is to guide radio site access permissions and subsystem roaming. The network infrastructure and subscriber units are configured to permit managed access to sites throughout various parts of the system. This managed site access provides the ability for users to achieve wide area coverage where necessary for mission-critical operations, enhanced in-building portable coverage, and a degree of system level backup in the event of certain types of major network failures. Roaming for non-essential operations is subject to being restricted, to maintain an acceptable grade of service for mission-critical operations.

2. Technical Background

Infrastructure programming settings that control site access for talkgroups / multigroups

There are settings in the system infrastructure to control the "Site Access Denial Type" parameter, which controls how site access is handled for radio users of the system. Radio users and talkgroups have independent access lists programmed into the system infrastructure. These lists control which sites the radio and/or the talkgroup can access. The level of access depends on the "Site Access Denial Type" setting. Options for this setting are:

- Individual Only: The radio is rejected if the individual radio user ID does not have access to the system.
- Talkgroup Only: The radio is rejected if the current, selected talkgroup ID does not have access to the site, regardless of radio user site access settings.

- Both: The radio is rejected only if BOTH the talkgroup ID AND the Radio User ID do not have access to the system.
- Either: The radio is rejected if EITHER the talkgroup ID OR the Radio User ID do not have access to the site.

Infrastructure programming settings that control site access for Interconnect / Private Call

The site access privileges for private and interconnect calls are based on the site access settings for the radio user and not based on the system "Site Access Denial Type" settings. They are independent of talkgroup site access settings.

Radio programming settings that control site access:

The subscriber radios contain "Site Preference" selections for radio programming. Radios can be programmed with multiple unique personalities, which will allow unique Site Preference Selections for each talkgroup in the radio.

- Least Preferred: The site will be avoided unless it is the only usable site for operation.
- No Preference: The site is given no preference. If the site is not listed here, the radio automatically assigns it no preference.
- *Preferred: The site will be used over all non-preferred sites with similar signal strength.
- *Always Preferred: The site will be used over all non-preferred sites with similar signal strength, even if the site loses communication with the Zone Controller and enters site trunking.

*Note: Always Preferred and Preferred are operationally identical if the radio sites have communication with the system and are operating in wide area mode.

- **Constraints**

  Using the "both" site access denial setting to facilitate unique, individual needs will allow those individuals full access to all their talkgroups at sites they have "Radio User" permission for.

  Using the "either" site access denial setting to facilitate unique individual needs may block those individuals from site access, even in emergency conditions.

3. Operational Context

Normally, only regional and statewide interoperability talkgroups will be permitted access at ALL sites.

Talkgroups would generally be permitted access at all those sites necessary to support the "normal day-to-day" operations of the users of that talkgroup.

If it is necessary that a talkgroup have redundancy protection in the event of a site failure, the attempt shall be made to use an adjacent or overlapping non-owned site for the

talkgroup's protection. Factors determining the best protection site include coverage of the site or function of the talkgroups per site.

Custom talkgroup site access configuration profiles can be created for consistency with this standard.

Dispatchers would be able to use the regional and statewide interoperability talkgroups or other "common," "roaming," or "pool" talkgroups as described in Infrastructure Configurations (below) for patching to their local area talkgroup to facilitate temporary wide area access.

4. Recommended Protocol/Standard

Subscriber Unit Configuration:

In subscriber radio programming, the radio would normally be enabled for all sites of the system, and the operational site access would be managed at the system level.

The subsystem administrator will program the radio's site preference tables to maintain roaming at an acceptable level, while minimizing impact to other sites.

Radios with no site preference tables, or with all sites set to the default "No Preference," will generally not be allowed on the system, because they will indiscriminately roam among all sites where the selected talkgroup is allowed.

Infrastructure Configuration:

Radio user profiles would generally not have special site access permissions granted. Site access for wide area operations will primarily be managed at the talkgroup level. subsystem administrator's may accomplish this by designating site access throughout the system to a limited number of special wide area talkgroups. These special talkgroups would not be main dispatch or tactical talkgroups with high volumes of radio traffic but may be regional and statewide interoperability talkgroups or Wide Area, "roaming," "common," or "pool" talkgroups. The "Site Access Denial Type" for the system is at a site if both talkgroup privileges are denied at the site. The use of "Critical User" and Critical Site" in the system is generally discouraged and must be authorized by the ISICS System Administrator.

5. Recommended Procedure

The defined standard would be implemented and maintained by the appropriate system and subsystem administrator(s).

6. Management

The system and subsystem administrator are responsible for oversight and ensuring that this standard is followed.