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

Standard Name:	**System Security Groups**		Date Created:		**05-08-2018**	
Standard Policy #	**2.12.1**	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 define a security structure using security groups for overall system security and management of the system.

Security groups are used to protect the system by managing the administrative access to the various objects in Provisioning Manager (PM) – "infrastructure, talkgroups, subscribers, etc."

2. Technical Background

Capabilities

All objects in the User Configuration Server can be independently assigned to specific security groups. User login accounts are independently assigned various levels of rights to the security groups, such as "insert, edit, delete, etc."

Proper planning and implementation of the security groups will allow managing access rights to what users need to control and view. This protects the overall system security and simplifies management of the system.

Constraints

Once a security group is created, it cannot be deleted, only renamed. Planning for a security group structure needs to be completed before the security groups are created.

Proper planning of system security groups is vital for safe and reliable operation of the system in support of all users and is necessary for efficient management.

The security group name field is limited to a specific length.

3. Operational Context

Security groups will be created to allow administering agencies to access and protect objects in the User Configuration Server.

Every agency with authority to create User ID's, talkgroups ID's, etc., will have a minimum of one security group containing the objects they are responsible for. Additional security groups can be created if there is a need to segregate objects into groups requiring different access privileges to different login users.

4. Recommended Protocol/ Standard

The "shared" security group is intended for objects that need to be controlled by multiple agencies, and this provides a container for these objects without compromising individual agency security.

One example of a shared security group is as follows:

- **SHARED-R/W** – To be used for objects in Provisioning Manager as needed.

The "system" security group is used for master site objects, shared profiles, and statewide interoperability talkgroups. All system login users will have "read" rights to the "system" security group. Each agency will have full rights to their own group.

The RF Site Security Groups contain RF Tower Site objects.

Visibility for RF Site Security Groups will be set as needed.

The "user" security groups are for containing subscriber objects, such as "radios, radio users, login user accounts, profiles, storm plans, talkgroups, etc." Each agency's local administrative representative will have full rights to their own group.

Objects created by login user accounts within the "user" security groups will place the object into the same security group by default.

5. Recommended Procedure

Future updates and changes will be managed by the Statewide System Administrator.

6. Management

The Statewide System Administrator is responsible for the security group structure on the system.

The Statewide System Administrator and Subsystem Administrator are responsible for the usage of the security groups as defined in this standard.