Statewide Interoperability Radio Network (SIRN)
Standards, Protocols, Procedures

Document Section	**2 – Management of System**	**Status**: SIEC Subcommittee Approval Date: 1/31/2022
State Standard Number	**2.5.0**	
Standard Title	**SIRN Database Management**	
Date Established	**2/22/2021**	**SIEC Approval**: 1/31/2022
Replaces Document Dated	**N/A**	
Date Revised/Reviewed	**1/31/2022**	

1. Purpose or Objective

The purpose of this standard is to define the responsibilities for managing, archiving, updating and safeguarding the numerous system provisioning and configuration databases required for SIRN operation.

2. Technical Background

- **Capabilities**

SIRN uses a suite of central databases, software, applications and other system records that define its operational characteristics including:

- Network Configuration data
  - System and subsystem equipment configuration parameters
  - Subsystem equipment software and configuration
  - Transport network routing profiles
  - Client workstation software and configuration
  - Infrastructure databases
  - Disaster recovery plans
  - System and as-built documentation
  - Maintenance logs
  - Historical system usage and other performance data
  - FCC and other regulatory approval documentation
  - Equipment manuals
- Administrative Profiles
  - Security group structures
  - Login user accounts and privileges
- User Subsystems Profiles
  - Subscriber radios and radio configuration files
  - Profiles for radio users, talkgroups and multi-groups
  - Console software and configuration

These SIRN databases contain the operational personality of the entire system; loss or corruption of this information could severely compromise the performance of SIRN. In addition, the databases and their management can be distributed among the agencies/staff responsible for the various aspects of the data in the database. Because of this critical function, the data must be properly managed, updated and archived in case of data loss or corruption.

3. Operational Context

SIRN databases contain essential information developed and optimized over time; the integrity and security of these operational parameters are essential for normal operations and operational continuity. In order to meet these objectives, this Standard defines processes for:

- Managing updates to the databases
- Proper and regular archiving of the databases
- Regulating personnel access to the databases

SIRN technical staff need up-to-date system configuration information to perform their required maintenance and support duties.

4. Recommended Protocol/ Standard

This will be an ongoing task in the operation and management of the system.

Archiving Protocols and Backup Locations
The Statewide System Administrator is responsible for routinely archiving and securely storing the SIRN configuration databases as defined in this Standard.

All system data must be maintained in electronic format.

The Statewide System Administrator, at least twice per month, will back up all system databases via automated scripts. In the event that substantial changes to a particular database are implemented, a backup should be created immediately.

Archived copies will be created and kept at on-site, off-site or cloud-hosted locations including at a location managed by the primary vendor, Motorola Solutions, Inc., and the primary operator, NDIT.

Multiple revisions will be dated and kept in a rotating stock so a restore would be possible from an earlier backup if the need arises.

System Restore
Database restores will only be done by the Statewide System Administrator and only in the event of one of the following:

- System software reloading and version changes
- System database corruption, or
- As defined in any SIEC-approved continuity of operations (ConOps) plans

Database restores may also be performed where there is a need, in a non-critical condition, as determined by the Statewide System Administrator if there is a reasonable consensus from the appropriate Subsystem Administrators and Local User Administrators.

Database Access Rights
Preserving the integrity of these critical network databases requires closely-controlled access rights. In general, only the SIRN Statewide System Administrator or a designee shall have *write* access to any of the system management suite of databases and applications. Some exceptions to radio device and console related databases may apply.

View/Read only access may be granted to NDIT or vendor staff (Statewide Administrator designees), Subsystem Administrators and PSAP Managers as approved by the SIEC. In such cases, the system databases will be partitioned to provision access to only the database elements for which the Administrator is approved or is responsible for managing. See *SIRN Standard 2.11.0 SIRN - System Management Login Accounts* for further details on SIRN database access and login account assignments.

In general, outside of the approved self-maintained functions, all other requests for and changes to SIRN databases and functions including user profile updates, talkgroup attribute changes and historical user audit records must be directed to the SIRN Statewide System Administrator.

Console and Radio Configuration Files
Individual agencies will be responsible for maintaining and archiving their own radio codeplug data or console configuration profiles as defined by the agency's internal procedures. Mobile and portable radio fleet information includes such details as radio manufacturer, model, firmware, and flashcode.

Subsystem Administrators, PSAP Managers and Local Administrators, as applicable, are responsible for creating any local infrastructure database, subscriber database, console configuration profiles and shared resource backups and storing them at a secure facility.

The Statewide Administrators will retain a consolidated database on console and radio information and conduct a regular audit of Local Administrators' data.

5. Recommended Procedure

Equipment Configuration Records Keeping
All system information and documentation detailed in the Technical Background Capabilities section of this Standard shall be kept up-to-date and made available to pertinent Administrators or the SIEC.

Local Administrators and PSAP Managers are responsible for maintaining accurate records for self-maintained subsystems.

It is the responsibility of SIRN Administrators to obtain accurate system as-built documentation from vendors and contracted staff that make changes to or provide additive products to the SIRN.

Any changes or alterations that come to the knowledge of a Local System Administrator will be immediately forwarded to the Statewide System Administrator for entry into the records.

6. Management

The Statewide System Administrator is responsible for managing and archiving the SIRN databases.