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

Document Section	**2 – Management of System**	**Status**: SIEC Sub Committee Approval Date: 5/24/2022
State Standard Number	**2.6.0**	
Standard Title	**Network Management**	
Date Established	2/22/2021	**SIEC Approval**: 5/24/2022
Replaces Document Dated	11/29/2021	
Date Revised/Reviewed	5/24/2022	

1. Purpose or Objective

The purpose of this Standard is to define the responsibilities for Network Management.

2. Technical Background

- **Capabilities**

The SIRN architecture is primarily anchored on an internet protocol (IP) based network. The network is composed of, but not limited to, switches; routers; servers; local area networks; and wide area links connecting sites together, consisting of microwave and fiber optic equipment. Network management for these network elements is provided through various industry standard management and diagnostic tools.

- **Constraints**

The system network is complex, and unusual problems may be difficult to identify and resolve. The system documentation will have to be kept up-to-date to maintain its value in supporting the system network.

The network must also be protected from other agency data networks to protect its security and functionality. Connections to another data networks shall be through an appropriately designed and maintained firewall.

3. Operational Context

A robust and standardized network architecture management, security and maintenance plan is vital for the integrity of SIRN.

4. Recommended Protocol/ Standard

Network Configuration Database Integrity

SIRN is composed of thousands of network switches, routers and interfaces provisioned and optimized over time through manual and automatic IP- and MPLS-based configurations. Per the *SIRN Standard 2.5.0 Database Management*, network configuration databases, directories and architectural documentation must be regularly archived.

Network Security and Updates

All NDIT-operated and locally-operated network components and interfaces shall at all times be kept secure and provide high availability service through:

- Strict adherence to the SIRN *Standard 2.18.0 General IT Security* on issues related to firewall configuration, routine security posture monitoring, link encryption, and proper technical staff training
- Regular antivirus updates of all networked elements including dispatch subsystems through active vendor licensing contracts covering security elements

Transport/Backhaul Links

Network connectivity provided by public, private and commercial ethernet carriers or other transport media architecture shall deliver high availability to meet the mission critical requirements of SIRN. The Statewide System Administrator shall evaluate link availability and reliability trends on a regular basis to determine overall performance and areas for improvement. See *SIRN Standard 4.5.0 Preventative Maintenance* for complete procedures on periodic network maintenance activities.

Other Standards

Several other defined standards for maintenance, documentation, notification, changes, security, and training also pertain to the network portion of the system.

5. Recommended Procedure

The methods for performing detailed network operations are defined in the technical resource manuals and training for the system. The technical resource manuals contain configuration information related to critical infrastructure and is therefore exempt from mandatory public disclosure pursuant to North Dakota Century Code (N.D.C.C.) § 44-04-18.4(7) and N.D.C.C. § 44-04-24.

Details on procedures not otherwise defined are at the discretion of the SIEC and will be recommended by the SIEC Subcommittee who will define the flow and input of information by other committees.

6. Management

Local Administrators or their designees are responsible for managing and maintaining their agency's data attributes. The Statewide System Administrator or designee shall be responsible for the statewide portion of the network.