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

| Document Section Title | **Management of System** | **Status**: Committee Date: 6/28/2021 |
|---|---|---|
| State Standard Number | **2.1.0** | |
| Standard Title | **Subscriber Radio Standards** | |
| Date Established | **08/19/19** | **SIEC Approval**: |
| Replaces Document Dated | | |
| Date Revised/Reviewed | **03/15/2021** | Date: 6/28/2021 |

### 1. Purpose or Objective

The purpose of this standard is to:

- Set minimum technical and performance standards for subscriber radios allowed to operate on the North Dakota Statewide Interoperable Radio Network (SIRN).
- Provide procedures to measure, test, certify and/or publish a list of subscriber radios that are approved for use on the system

### 2. Technical Background

- **Capabilities**

The SIRN Platform uses digital communications technology specified in the TIA-102 Series Standards, Interim Standards, and Telecommunications Systems Bulletins, commonly known as APCO Project 25 (P25) Standards. Specifically, the SIRN Platform employs P25 Phase 2 Time Division Multiple Access (TDMA). The P25 standards provide capability for full backward migration and limited forward migration along an evolving continuum of technologies and services, assuming the radios operate on a common set of frequencies. P25 standards also permit different vendors of subscriber radios and infrastructure to interoperate while providing value added vendor specific premium features and services.

- **Constraints**

Subscriber radios from vendors using different radio operating software will provide a variety of services, features, functionality, and performance to the users. Some radios will also interact differently with the infrastructure and could potentially exhibit undesirable operations.

It is possible that new, unproven radios and/or software may exhibit performance and functionality characteristics that are destructive to the overall performance, capacity and/or security of the SIRN platform.

This standard does not include paging equipment.

### 3. Operational Context

Compliance to these standards is essential in advancing the SIRN objectives—reliable, standardized, and interoperable operation. SIRN User Agencies may elect to use radios from any P25-certified manufacturer provided that the device complies with this Standard. It is anticipated that radios capable of operation on the system will be available from multiple vendors over the life of the system. Users need the flexibility and knowledge to optimally choose from the radios available in the marketplace that would be operationally desirable and not cause problems for other users on the SIRN Platform.

## 4. Recommended Protocol/ Standard

All subscriber radios meeting the applicable P25 standards that DO NOT exhibit operational, performance, or other characteristics that substantially and negatively impact the system or its users will be approved for use on the system.

Before a new subscriber radio that is not on the vetted subscriber radio list is approved for use on the system, it shall undergo a certification process in which the list of required P25 and SIRN operational features are sent to the manufacturers for verification that the required functionality exists in their subscriber units and is compatible with the SIRN infrastructure. The manufacturers shall provide documentation confirming device functionality and compatibility with a list of required SIRN features. Additionally, at the discretion of the SIEC, a radio may be required to undergo a certification test on SIRN infrastructure as described in this Standard.

A list of approved radios are posted on the SIRN web site.

## 5. Recommended Procedure

**Minimum Device Requirements**

- Only devices certified for P25 Phase 2 operation by the Department of Homeland Security-sponsored Compliance Assessment Program (CAP) certified radios are approved for SIRN access.

- To verify devices have been certified for P25 Phase 2 operation, check the Department of Homeland Security database of radios CAP-tested for P25 Phase 2 trunked operation at the following link: https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment.[1] Select "Project P25 Phase 1/2 Trunked Subscriber Unit" under "Equipment Type;" and select 2017 or later under "CAB Test Req Year."

## CAP Test Documentation (STR and SDOCs)

The filters below can be used to search for P25 CAP Test documentation for equipment tested.

| Supplier | Equipment Type | CAB Test Req Year | Items per page | |
|---|---|---|---|---|
| - Any - ▾ | Project 25 Phase 1/2 Trunked Subscriber Unit ▾ | - Any - ▾ | 25 ▾ | Apply |

- In addition to supporting base P25 Phase 2 operation, a variety of standardized and optional P25

---

[1] Websites and information may be relocated by DHS. Contact the SIRN System Administrator if you experience issues accessing the list of DHS CAP-certified devices.

features are required or recommended to support the critical and interoperable communications mission of the SIRN. Minimum technical standards and options for SIRN operation may vary based on an agency's operational and functional needs. The table below identifies the required and recommended device features categorized as follows. Please refer to the features and functions identified in this table when purchasing radios for your User Agency.

a. **\*Required**: Mandatory for operation on SIRN

b. **\*Strongly Recommended**:

    i. May be mandatory at a future date to accommodate evolving SIRN/P25 standards, OR

    ii. Is a features that enhance local and regional interoperability

| Feature | Notes |
|---|---|
| P25 Phase 2 TDMA | **Required** for All Devices |
| Minimum: 256 modes/channels | **Required** for All Devices |
| AES Encryption | **Required** for all Law Enforcement agencies and any other agencies with access to encrypted talkgroups |
| Multi-key Encryption | **Required** for all Law Enforcement agencies and any other agencies with access to encrypted talkgroups |
| OTAR | **Required** for all Law Enforcement agencies and any other agencies with access to encrypted talkgroups |
| OTAP | **Required** for all agencies and any other agencies with access to encrypted talkgroups |
| Multi-band Operation (VHF + 700/800MHz) | **Strongly Recommended** for agencies with routine mutual aid support from/to Montana and South Dakota |
| Intrinsically Safe Device | **Strongly Recommended** for Fire fighters and HAZMAT personnel |
| Hardware-Based Programming Keys | **Required** support for hardware, electronic dongle programming key |
| GPS | **Required** for all public safety agencies |
| Noise Cancellation | **Strongly Recommended** for Fire fighters |
| 14 Character Front Display | **Strongly Recommended** for all agencies |
| Wi-Fi | **Recommended,** At Agency's Discretion; see applicable policy |
| Bluetooth | At Agency's Discretion |

| Feature | Notes |
|---|---|
| 4 x 3 Key Pad | At Agency's Discretion |
| Group Services | At Agency's Discretion |
| Link Layer Authentication | Not Required |

### New Device Certification Procedures

Vendors must demonstrate new devices (not previously approved for SIRN use) meet the proper CAP certification. Acceptable documentation can include P25 Compliance Assessment Program (CAP) results or other inter-manufacturer interoperability testing results.

Prior to approval for use on SIRN, each new radio model may be subject to further SIRN certification process to determine compliance with the P25 Standards and, more specifically, minimum features required for SIRN operation.

Vendors or manufacturers seeking to sell new products (radios) may be required to provide the SIRN Statewide Administrator with operational radio units from production for the certification test.

A test SIRN-specific codeplug, personality or equivalent would be developed by the manufacturer or manufacturer-approved personnel in conjunction with the radio manufacturer and the requesting agency, to verify features including, but are not limited to:

- Roaming parameters
- Scanning performance
- Site affiliation, registration/de-registration
- Radio Inhibit
- Encryption communications (OTAR, KMF Affiliation, AES)
- Emergency activation and clearing
- Group calls and "announcement" group calls

Real-time system logs (UEM/ATIA data) will be used to validate the device properly registers/affiliates with the system and generally exhibits the required characteristics from the SIRN infrastructure vantage point.

Test documentation and any additional actions taken by the SIRN Technology Committee will be submitted to the SIRN Statewide Interoperable Executive Committee (SIEC) for final action.

If the stipulations are met, the SIRN Technology Committee acts to approve the radio for use on the system. Any potential concerns, limitations or constraints will be documented. If the SIRN Technology Committee has any concerns or questions that would preclude approval, follow-up documentation will be requested.

Note that per SIRN Standard 2.16.0 Subscriber Configuration File or Codeplug Development, all new

device will need to undergo the *New Base Radio Codeplug Development* procedures in which a master SIRN codeplug will be developed, loaded and tested to validate baseline SIRN-wide device features and interoperability programming requirements are met.

## Pre-Production Subscriber Radios

Radios or pre-production radios may be submitted for evaluation by any authorized user. However, devices will not be permitted for regular use on SIRN until CAP-certified and FCC-approved.

## Problems with Previously Approved Radios

*New problem with previously approved radio*

If a previously approved subscriber radio type begins to exhibit characteristics that are harmful to the operation of other users on the system, users will be notified and will be required to coordinate with the manufacturer and provide documentation when the problem is solved. If the harmful effects are detrimental to SIRN operation, the device-in-question will be deactivated from SIRN access until resolution.

Any applicable certification tests may need to be repeated to validate that proper functionality has been restored.

If a problem is due to the use of a new feature in the radio, that feature will not be allowed to be used until satisfactorily repaired and tested by the manufacturer for proper operation.

If the manufacturer introduces a firmware update to resolve the problem, the SIRN Statewide System Administrator may require the device to undergo certification tests prior to approval for SIRN use.

## Approval of second-hand and/or used radio equipment

Any purchase of second-hand or used radio equipment may require an inspection and software flash by the vendor to ensure that it is in proper working order. The purchasing agency is responsible for ensuring the radio is coming from a reputable vendor and in good working order.

The SIRN Technology Committee may require the device to undergo certification tests prior to approval for SIRN use.

## 6. Management

The Statewide System Administrator is responsible for managing this procedure, including maintaining all certification records, managing radio equipment manufacturer-initiated submittals, and coordinating activities of the SIRN Technology Committee.

**Appendix A**

List of device Certification Testing

Note: The following test will be executed only as required by the SIEC for new or for vendors permitted to test pre-production radios. Only a subset of the certification test may also be applied.

- Radio Programming Software
    - Programming Software Load
    - Read Configuration from Radio
    - Radio Version
    - Software Protection
    - System Keys (Master/Slave)
    - Edit Radio Configuration
    - Save Radio Configuration to Disk
    - Load Radio Configuration from Disk
    - Write Configuration to Radio
    - Clone Radio
    - Test of a radio with No System Access Privileges

- Technical Specification Testing
    - Radio RF specifications
    - Environmental Testing
    - Battery

- Radio Registration / Affiliation Testing
    - Radio Registration with System
    - Radio De-Registration with System
    - Radio Affiliation Display / Updates Talkgroup
    - Radio Affiliation Display / Updates Multigroup
    - Radio indication when account disabled in UCS
    - Access permissions/denials based on Radio ID PCRF

- Radio Roaming Tests
    - CC list  (Takes approximately 2 ½ - 5 minutes for initial finding of control channel after programming radio with no control channels)
    - Fast Start/CC scanning at critical or typical site profile (CC list)
    - Adjacent control channel
    - Multizone Operation

- o Site Access Control for Talkgroup & Radio User
- o Site Avoidance
- o Site Preference & Roaming
- Trunking Tests
  - o Talkgroup Call (Wait and Interrupt)
  - o Smart PTT
  - o Busy Tone and Callback
  - o Continuous Assignment Updating
  - o Initiate a Multigroup Call
  - o Receive a Multigroup Call
  - o Emergency Alarm/Call w/Ruthless and Top of Queue
  - o Emergency Alarm/Call with Tactical Operation
  - o Emergency Alarm/Call with Talkgroup Revert
  - o Emergency Alarm ID Display
  - o Failsoft Recovery to Site Trunking
- Encryption Operations
  - o KMF Communications
  - o Secure Talkgroup Operation
  - o Multi-select operation
  - o OTAR Key and Rekey
- Radio Control Manager (RCM) Tests
  - o Emergency Alarm Display
  - o Dynamic Regrouping
  - o Selective Radio Inhibit
  - o Radio Check
- Features Testing
  - o Non-Priority Scan
  - o Priority Scan
  - o User Editable Scan List
  - o Rx Only Radio
  - o Secure / Encryption Operation
  - o Subscriber to Landline Telephone Interconnect
  - o Subscriber to Landline

- o Telephone Interconnect, Overdial Mode
- o Landline to Subscriber Telephone Interconnect
- o Call Alert
- o Private Call
- o Conventional 800 MHz Resources
- o Direct Talk-Around in Digital clear mode
- o Direct Talk-Around in Digital encrypted mode
- System Failure Mode Testing
  - o Site Trunking Talkgroup Call