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

Document Section	2 – Management	Status:
State Standard Number	**2.19.0**	SIEC Sub Committee Approval
Standard Title	**SIRN Application Integration and Interfaces**	Date: 2/28/2022
Date Established	3/15/2021	**SIEC Approval**:
Replaces Document Dated	3/15/2021	
Date Revised/Reviewed	2/28/2022	Date: 2/28/2022

1. Purpose or Objective

The purpose of this document is to define technical standards and procedures for interfacing third-party applications and systems with SIRN.

2. Technical Background

- **Capabilities**

The SIRN platform, like other LMR systems, will be interfaced with a variety of third-party applications that interact with or leverage the radio system technology and data to enhance other public safety services. These applications include public safety solutions such as logging recorders, computer aided dispatch (CAD) systems, mapping applications, fire station alerting systems, push-to-talk applications, or solutions geared toward operators such as network monitoring/management solutions and enterprise backhaul networks.

Integration of third-party applications typically requires direct connectivity to the SIRN using standards-based Application Programming Interfaces (APIs), legacy command and control RS 232 links or over the air audio/data gateways.

- **Constraints**

Network and application interfaces to the SIRN provide third-party applications access to the SIRN core application. Third-party access to the network, if poorly designed and provisioned, can compromise the security and performance of the SIRN or cause the third-party application to malfunction.

3. Operational Context

Various public safety applications rely on radio network data or metadata to deliver essential capabilities to public safety practitioners and technologists. To ensure these third-party solutions function properly in a mutually secure and synchronized manner, a thorough process for requesting, evaluating, designing, approving, installing, and maintaining the solutions (specifically the interfaces) is essential.

4. Recommended Protocol/ Standard

All third-party applications interfaced with SIRN must:
- Be covered by the application vendor's full maintenance, support and licensing agreements
- Adhere to NDIT security policies for on-premises and cloud-based solutions
- Maintain the most up-to-date end point security software
- Employ specific firewalls and network ports as approved by NDIT
- Be evaluated for network traffic/latency impact on the SIRN Core
- Be assessed annually by NDIT for its security posture

If multiple agencies require APIs to the same third party solution, the State may elect to offer a centralized multi-tenant solution.

See SIRN Standard 2.18.0 System and IT Network Security for additional details that apply to all SIRN networked subsystems and solutions.

5. Recommended Procedure

General Standards
All SIRN interfaced applications must have demonstrable and justifiable benefits to the public safety community.

Requests for connecting systems and applications to the SIRN have to undergo NDIT architectural review and be approved by the SIRN Statewide System Administrator or the SIEC.

The SIEC will closely review and approve requests for application integration with SIRN, notably, for those applications which have previously not been integrated with Motorola Astro 25 systems.

Local agencies seeking to implement a SIRN interfaced application shall provide a comprehensive plan and design for SIEC consideration. The Statewide Administrator, with the support of the Motorola technical team, will conduct a technical feasibility/architectural review to advise the SIEC. During this process, all product vendors must provide technical expertise to support the integration feasibility and design analysis.

Application interfaces typically require software development for customization and optimization. Therefore, where multiple applications exist, preference will be given for applications/solutions previously vetted and integrated with Motorola networks and API libraries.

All third-party application implementation costs (including NDIT staff and SIRN vendor resources and APIs) will be borne by the requesting agency.

Local agency assumes full responsibility for the proper operation of the application including its interfaces with SIRN.

Interfaces causing adverse effects on SIRN will be taken offline until the issue is resolved by the user agency.

6. Management

The Statewide System Administrator is responsible for managing the implementation and operations of application interfaces.