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

Document Section	**Management of the System**	**Status**: SIEC Sub Committee Date: 08/31/2020
State Standard Number	**2.2.0**	
Standard Title	**Law Enforcement/Criminal Justice Information (CJI) Encryption**	
Date Established	**09/28/2020**	**SIEC Approval**: 09/28/2020
Replaces Document Dated	**NA**	
Date Revised/Reviewed	**NA**	

1. Purpose or Objective

The purpose of this standard is to establish policy and procedures for the encryption of Criminal Justice Information (CJI) on the SIRN network.

2. Technical Background

- **Capabilities**

Encryption is used in end user equipment where secure voice communications are required. This includes, but may not be limited to, subscriber radios and devices, dispatch consoles and radio voice logging equipment.

- **Constraints**

If a radio or other SIRN device, including dispatch consoles, utilizes encryption while transmitting all other devices on that talk group, must have the correct Traffic Encryption Key (TEK) and Key ID (KID) installed in order to hear the transmission. Any device that does that does not have the appropriate TEK and KID will not have the ability to decrypt and hear the encrypted voice traffic.

3. Operational Context

The FBI CJIS Security Policy requires that all CJI be encrypted during transmission.

The North Dakota Office of Attorney General - Bureau of Criminal Investigation published a memo (Dated January 3rd, 2020) that requires all CJI communicated over a radio system be encrypted per FBI CJIS Security Policy.

NLETS is the portal through which all states, including North Dakota, transmit driver's license, registration, and other CJI information. NLETS and all member agencies that have a connection to the FBI's CJIS network are required to adhere to the CJIS Security Policy. For these member agencies, NLETS shall adopt the CJIS Security Policy as the policy governing the NLETS connection.

The SIEC reviewed and agreed with the BCI memo and federal guidelines on encryption of CJI over LMR on 01/14/2020. This would require that all LE CJI radio traffic be encrypted on the SIRN network.

4. Recommended Protocol/ Standard

All CJI related information will only be transmitted through the SIRN system on encrypted talk groups.

5. Recommended Procedure

All CJI related information will only be transmitted through the SIRN system on encrypted talk groups.

6. Management

The System Administrator will develop a naming convention that clearly distinguishes encrypted talk groups from non-encrypted talk groups.

Fleet mapping will ensure interoperability between disciplines by developing interoperable talk groups for use by multiple disciplines during emergencies, ensuring that law enforcement can maintain communications with agencies not possessing encrypted devices.