Document Section	**Management of System**	**Status**: Committee
		Date: 6/28/2021
State Standard Number	**2.16.0**	
Standard Title	Subscriber Configuration File Codeplug Management	
Date Established	**03/15/2021**	**SIEC Approval**: 6/28/2021
Replaces Document Dated	**00/00/00**	
Date Revised/Reviewed	**00/00/00**	

1. Purpose or Objective

The purpose of this standard is to establish policy and procedure for developing and maintaining the integrity of subscriber radio configuration files (commonly known as codeplugs). This standard outlines the process for the initial development, continued updates, storage, distribution, and quality control of SIRN radio codeplugs.

2. Technical Background

- **Capabilities**

Each subscriber device is loaded with a *unique radio configuration file* (or codeplug) consisting of network access parameters, subscriber performance variables, end user data and agency-specific talkgroups and features. Codeplug files include detailed parameters that establish radio characteristics per SIRN standards and in accordance to the individual agencies' operational needs.

- **Capabilities**

Codeplugs contain hundreds of user-definable parameters populated manually and automatically that control the behavior and performance of the radio. SIRN will support thousands of devices, each with their unique configuration files developed by dozens of technicians. Errors can easily be introduced during codeplug development that adversely affect not only the individual user device but the SIRN infrastructure. Therefore, a robust process for the creation, development, distribution and quality assurance of device configuration files ("codeplugs") is essential for the integrity of SIRN.

3. Operational Context

Codeplugs contain sensitive data in the form of dozens of system and device parameters that will be obtained from the SIRN Systemwide Administrator. In order to ensure the integrity of the data and subsequently the radio's performance, an established process for handling system data is essential. In addition, a single codeplug may be loaded into hundreds of devices; therefore, close inspection and vetting of codeplugs at interim stages of development is crucial in reducing the likelihood of error propagation.

4. Recommended Protocol/ Standard

Each device model approved for SIRN will have a "base" radio codeplug file or template developed in conjunction with the manufacturer. The SIRN Systemwide Administrator will maintain a database of base radio templates for all unique device models on SIRN. Base radio templates consist of key parameters to

help facilitate the development of customized agency-specific codeplugs including:

- minimum network parameters for SIRN access by device,
- talkgroup information for systemwide interoperable resources, and
- other essential codeplug profiles such as user interface configuration.

Codeplug developers/technicians are not permitted to develop codeplugs "from scratch" for new agencies or new radio models. Rather, technicians must request an approved base codeplug file from the SIRN Administrator for the device-at-hand for further customization. This step is intended to limit the introduction of errors to device parameters that have already been thoroughly tested and are readily available. If a base codeplug file does not exist for that specific model, the following procedures for New Codeplug Development shall be followed.

New device models for which a certified base radio template is not yet available must undergo the steps outlined in this standard.

5. <u>Recommended Procedure</u>

General Codeplug Development Standards
All agency or service shop personnel shall execute the *System Key Authorization* agreement to obtain System Keys and other network data to configure devices or develop codeplug files. (See SIRN Standard 2.14.0 Subscriber Programming System Key).

Personnel providing codeplug development services must meet the minimum training requirements established in SIRN Standard 4.4.0 Technical Staff and Maintenance Providers Minimum Requirements. The SIRN Administrator shall maintain a database of all government agency and commercial service shop personnel approved for developing codeplugs for SIRN devices.

SIRN Systemwide Administrator will maintain base codeplug files or templates for all approved radio models on SIRN. This is intended to assist agencies in providing a thoroughly vetted codeplug base that can be further customized to suit the agency's operational needs.

Customizing Codeplugs for Previously Approved Devices

Agencies seeking to develop or customize new codeplugs for already-approved SIRN devices must contact the SIRN Administrator to obtain ("check out") a base radio template for that device, and must not develop codeplug files "from scratch."

Changes to the base template may be made by the requesting agency provided that the final codeplug adheres to all SIRN fleetmap standards and as authorized by the *System Key Authorization*.

Any pre-existing bugs identified in the base radio template must be reported to the SIRN Administrator to update the base template on record.

New Base Radio Codeplug Development

All new devices models must first meet all applicable requirements stated in the SIRN Standard 2.1.0 Subscriber Radios Standards for SIRN access approval.

A base radio template, as described below, will be developed by the requesting agency or programming personnel for review and approval by the SIRN Systemwide Administrator. The initial base radio template is designed to accurately cover all generic system and statewide interoperable features. At minimum, the base radio codeplug file includes:
- Subscriber-wide settings
- SIRN control channels
- Recommended user interface settings (for buttons, switches, and knobs)
- Fleetmap/Radio Layout structure as required by the SIRN Fleetmap Standards
- All SIRN-wide, statewide and regional interoperable talkgroups and conventional channels
- Correct talkgroups IDs and aliases specific to the requesting agency
- Correct talkgroups IDs and aliases specific to the requesting agency's interoperable partners

The SIRN Administrator will furnish codeplug development personnel with system information covering the parameters listed above. Codeplug development requires substantial sensitive system data to be provided to the programmer or developer. Misuse of the data will cause revocation of programming rights or other repercussions per the *System Key Authorization* agreement.

SIRN Administrator and support staff will additionally provide guidance to the development team to ensure the codeplug adheres to all applicable SIRN standards and includes the proper system data and subscribers for the requesting agency.

Due to the complexity of initial codeplug file development, the requesting agency or programming personnel must make technical and engineering resources from the *device manufacturer* available to ensure the integrity of the initial base radio template.

The draft base template will be subject to the *SIRN System Codeplug Test Procedures* to ensure all SIRN-wide and SIRN-specific features and configurations are correct. The SIRN Systemwide Administrator will make the Test Procedure document available.

Upon approval, the base template will be stored by the SIRN Administrator to support other agencies seeking to customize codeplugs for that specific model.

Programming personnel are then permitted to use as a base template and further customize the approved base radio template to meet other local agencies' needs provided that the final version(s) adheres to SIRN standards.

6. Management

The System Administrator will maintain records of all base radio codeplug files provisioned for entities consistent with current records retention policies.