Software Security Description – KDB 594280 D02v01r03 Section II	
General Description	1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate. Software/firmware will be obtained, downloaded and validated by the factory first, it's a whole system binary image, no single upgrade package for device's RF. The RF parameters will be write into the protected read-only partition by factory, and the partition can only be written once, any upgrade from system software will not affect RF parameters.
	2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics? The RF parameters cannot be modified by software. All these parameters will not exceed the authorized parameters. The firmware has been complied as binary file. It couldn't change the setting RF parameter through this binary file. It is read-only without change.
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification. RF-related firmware is build-in the system image, based on the official release version, the RF module can only work on the firmware provided by the manufacture, users have no way to change it, unless re-flash the whole system image, and the system image based on our hardware for verification, other images can not be flashed to the device.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. No encryption methods used and no need, because users have no way to update it.
	5. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation? This device can only be used as a slave device and cannot be configured as a master device.
Third-Party Access Control	1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S. No any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.
	2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality. The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this

	partition. 3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside the grant of authorization. There are no RF parameters that can be modified. All rparameters are programmed in OTP memory at thefactory and cannot be modified or overridden by third parties. The module is not controlled by driver sofwareon the host and cannot override critical RF parametersstored in module OTP memory.

Software Configuration Description – KDB 594280 D02v01r03 Section III
USER CONFIGURATION GUIDE

1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.

a. What parameters are viewable and configurable by different parties?

Authorized channel, bandwidth, and modulation.

b. What parameters are accessible or modifiable by the professional installer or system integrators?

(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

This is not professional install device. All applications installed can only visit their own process data space and the system public API, can not access or modify any parameters or resources of other application or the system resources

(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

Default mode is always FCC compliant. Other country modes cannot be activated without receiving three independent country codes from different APs, otherwise remains in FCC default mode (always FCC compliant)

c. What parameters are accessible or modifiable by the end-user?

(1) Are the parameters in some way limited, so that the installers will not enter parameters exceed those authorized?

This is not professional install device. All applications installed can only visit their own process data and the system public API, can not access or modify any parameters or resources of other applicatic the system resources

(3) What controls exist that the user cannot operate the device outside its authorization in U.S.?

Default mode is always FCC compliant. Other country modes cannot be activated without receiving independent country codes from different APs, otherwise remains in FCC default mode (always FCC compliant)

d. Is the country code factory set? Can it be changed in the UI?

(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

Programmed for default mode which is always FCC compliant. Always set for default for all start-ups, reset or other host or network events.

e. What are the default parameters when the device is restarted?

Always FCC compliant.

2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02. No, this device cannot be configured in both bridge and mesh mode.
3. For a device that can be configured as a master and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance? No.
4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a)) This device cannot be configured as different types of access points.

Name: Chao Chen **Date:May, 21, 2025**

Title: EMC&PE

Signature of applicant: