SOFTWARE SECURITY INFORMATION

FCC ID: 2AENNE2F
Pursuant to:
FCC Part 15E 15.407(I) and KDB 594280 D02 UNII Device Security v01r03 / IC RSS-247article 6.4(4).

The information within this section is to show compliance against the SW Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03. The information below describes how to maintain the overall security measures and systems so that only:

1. **Authenticated software is loaded and operating on the device.**
2. **The device is not easily modified to operate with RF parameters outside of the authorization.**

SOFTWARE SECURITY DESCRIPTION		
	Requirement	**Answer**
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.	The firmware will be sent to the production line in secure mode, then load to the device via the special tool. After finishing firmware installing, the user can not modify it.
	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 have been confirmed in accordance with FCC regulations, and burned into the device. The unauthorized person can not modify via changing the firmware or other ways.
	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.	The firmware use encrypted IC to encrypt, which is with the special encryption, handshake, authorization and configuration protocols.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Please check the above 1&3 description for details.
	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?	Please refer the testing report. This device is the master, which is compliant with FCC regulation demands.

	Requirement	Answer
Third Party Access Control	1. Explain if any third parties have the capability to operate a U.S./Canada -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./Canada.	This device is not to be allowed to firmware installing and modification permission by the third party, any third party can not modify RF relevant parameters.
	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./Canada. 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.	This device is not to be allowed to firmware installing and modification permission by the third party, any third party can not modify RF relevant parameters.
	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.	Not applicable. This device is a non-independent module.

This section is required for devices which have a "User Interface" (UI) to configure the device in a manner that may impact the operational parameter. The operation description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 D01.

	SOFTWARE CONFIGURATION DESCRIPTION	
	Requirement	**Answer**
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.	UI RF Menu only open for public as below: 1. WIFI ON/OFF 2. Release and display wireless hotspot
	a) What parameters are viewable and configurable by different parties?	None that affect compliance.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	RF parameters "professional installer or system integrators" can not modify.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes, the parameters are limited in some way. UI do not display RF parameters.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S./Canada?	The unauthorized device can not connect tot his device.

	c) What parameters are accessible or modifiable by the end-user?	None, that affect compliance.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Yes, the parameters is limited in some way. UI do not involve in RF parameters.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S./Canada?	The unauthorized device can not modify and connect tot his device.
	d) Is the country code factory set? Can it be changed in the UI?	The country code has already been burned into the device, which can not modify in UI menu.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S./Canada?	Not applicable.
	e) What are the default parameters when the device is restarted?	After restarting the device, the RF parameters are determined by the country code, and will not be changed.
	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
	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?	User can not configure in UI interface.
	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)).	Unable to configure. Antenna is the for fixed one.

Name and surname of applicant (or authorized representative): Peizhi Chen

Date: 2019-01-07

Signature: Peizhi Chen