SOFTWARE SECURITY INFORMATION

FCC ID: W23-WMXWAVE2AS _ **IC : ______________________**

Pursuant to:
FCC Part 15E 15.407(I) and KDB 594280 D02 UNII Device Security v01r03 / IC RSS-247 issue 2 article 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.	There will be no firmware release on the manufacturer's website, and the security level defined by the system that have 2 differenet level, 1. Manager: Can modify general parameters 2. User: Can only be used
	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 firmware limits the RF power so that it does not exceed the authorized RF characteristics
	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.	There are administrators and normal users in the system. Normal users cannot change any settings or configurations. The administrator can change the settings and configurations, but they cannot change the RF parameters. Because the RF parameters keep on one-time-programming (OTP) flash memory, it cannot be changed.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The system used SSL security protection firmware.
	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?	The firmware have limit the RF config by master and client, so that can ensures compliance for each mode.

	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.	The system runs on the local network, so no any third party can operate this device
	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.	The system can not support third-party software or firmware installation.
	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.	The module is controlled by the module's firmware, and the firmware cannot be changed or modified.

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 v02r01

SOFTWARE CONFIGURATION DESCRIPTION		
	Requirement	Answer
ER 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.	Can't be configured via UI.
	a) What parameters are viewable and configurable by different parties?	Administrator can viewable and configurable. The normal user can not viewable and configurable.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	network setting, SSID, security, and security password...

	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Parameters are set through fixed options, so installers can only set fixed options.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S./Canada?	The params values only support U.S. authorization.
	c) What parameters are accessible or modifiable by the end-user?	network setting, SSID, security, and security password
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Parameters are set through fixed options, so installers can only set fixed options.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S./Canada?	The params values only support U.S. authorization
	d) Is the country code factory set? Can it be changed in the UI?	That can not be changed.
	(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?	The country can't be changed
	e) What are the default parameters when the device is restarted?	Is restarted all parameters based on the radio calibration done in factory.
	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.	Only Master 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?	Just provides wireless link, and it can't work alone without installing at system platform. The system platform decides to be configured as master or client mode.
	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)).	The antenna is fixed and shipped together

Name and surname of applicant (or authorized representative): Jeff Shu

Date: 2022-01-19

Signature: ______________________