SOFTWARE SECURITY INFORMATION

FCC ID: IR5RS13 **IC : ______________________**

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.	Ans: Software/Firmware will be controlled by MilDef Crete Inc.'s management system. Only MilDef Crete Inc. approval FW will be available to end user. End user can't load non- signed FW to this board.
	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?	Ans: They are fixed before shipping out. After factory, it's locked so user can't change it. End user is not capable to make RF changes by software/firmware update.
	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.	Ans: Any software that is loaded on the device is verified to ensure that its cryptographic signature matches MilDef Crete Inc. public-private keypair. Only if the signature matches is the software loaded onto the device.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Ans: The verification protocols are based on standard Public Key encryption.
	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?	Ans: This device cannot be configured as a master and client.

	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.	Ans: It's not allowed since country code option cannot be modified by end user.
	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.	Ans: The device information is built in the firmware. When the firmware upgrade is performed, CPE checks if the device information between old and new firmware is equal. If device information is not equal, the firmware upgrade cannot be performed.
	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.	Ans: The RF parameters is put in read-only partition of EUT's flash and is only installed by the factory.

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.	
	a) What parameters are viewable and configurable by different parties?	Ans: Authorized channel, bandwidth, and modulation.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	Ans: This is not professional install device.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Ans: This is not professional install or system integrate device.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S./Canada?	Ans: This is not professional install or system integrate device.

	c) What parameters are accessible or modifiable by the end-user?	Ans: Authorized channel, bandwidth, modulation.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Ans: Yes
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S./Canada?	Ans: The RF parameters in Flash is Read-Only and is obtained by the factory.
	d) Is the country code factory set? Can it be changed in the UI?	Ans: Country code is set at the factory as a parameter. No. It can't 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./Canada?	Ans: It can't be changed.
	e) What are the default parameters when the device is restarted?	Ans: Factory default is DEMO country that has commonly allowed channels and transmit power limit in all regulatory domains
	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.	Ans: 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?	Ans: This device cannot be configured as a master and client.
	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)).	Ans: ☐ Yes ☒ No This device cannot be configured as different types of access points and use different types of antennas.

Name and surname of applicant (or authorized representative): Willie Liang

Date: 2019-07-31 **Signature:** Willie