SOFTWARE SECURITY INFORMATION

FCC ID: 2AEUPBHARG07 **IC : 20271-BHARG071**

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.	OTA is using firmwares downloaded from Ring's website only. Images are downloaded via HTTPS. The device has the secure boot option enabled preventing from running any other firmwares not signed by Ring's certificates.
	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?	As the WLAN boarddata file is included into the WLAN firmware theoretically firmware update can change a bunch of RF settings, for example power tables. The firmware itself can only exclude several channels from being used by setting an appropriate country code.
	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.	1. OTA is using HTTPS protocol with domain name validation during TLS handshake. This allows downloading the data only from real Ring's website. 2. Secure boot feature: each firmware binary (including WLAN) is signed using one of the 4 certificates, hash value of which is pre-programmed into OTP during production. Each of these binaries are verified before executing them, if at least one of them fail - the device rolls back to the factory-programmed image (which is also signed).
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	WLAN firmware is not encrypted, it is only signed to protect it from modification (see previous item).
	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?	Work as client only.

	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.	Our device only can be uploaded by Ring's firmware, which follows FCC specifications. The third-party cannot change it.
	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 device does not permit running any standalone third-party firmware. On the other hand the firmware uses third-party code, but the only third-party code related to RF is the Qualcomm SDK which is, I suppose, certified.
	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.	Our device doesn't provide modular application.

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
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.	All basic configurations are viewable by the end user. No parameters are available for professional installers.
	a) What parameters are viewable and configurable by different parties?	Except RF parameters, all basic device configuration can be setup by the user. The only related parameter set by the user is the country code affecting the allowed band set and power tables.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	None

	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Not applicable
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S./Canada?	None
	c) What parameters are accessible or modifiable by the end-user?	WLAN related: SSID, password, IP configuration, country code (implicitly done by the APP based on location).
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	WLAN related: SSID, password, IP configuration, country code (implicitly done by the mobile app based on location).
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S./Canada?	None
	d) Is the country code factory set? Can it be changed in the UI?	If the device is not configured, the country code is set to US. Yes, it can be changed via 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?	Device operates according to the country code provided by the mobile app.
	e) What are the default parameters when the device is restarted?	County code is preserved through system restart.
	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?	Work as client only.
	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 device can only work with built-in antennas, it doesn't support any other external antennas. Compliance when working with internal antennas is tested during manufacturing.

Name and surname of applicant (or authorized representative): _Carro Hsieh/ Engineer, Ring

Carro hsieh

Date: March 10, 2021 **Signature:**