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. A: There is only one way to download firmware: =>Put RF Module on unique jig to update firmware by download software.
	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? A: There is no software provided by the manufacturer that can modify critical radio transmitter parameters.
	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. A: 1. Firmware are encrypted with integrity check to ensure the validity of its content. 2. Without passing the firmware integrity check, no upgrade will be performed.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. A: Firmware are encrypted with integrity check to ensure the validity of its content.
	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? A: It can only be used as a Client.
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. A: The operation frequency and RF parameter only can be change by unique jig so no any third parties can 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. 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. A: It is no third-party software or firmware can 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. A: Not applicable.

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. There are no RF parameters can be modified. And there are no different levels of access are permitted for professional installers, system integrators or end-users
a. What parameters are viewable and configurable by different parties? There are no RF parameters are viewable and configurable.
b. What parameters are accessible or modifiable by the professional installer or system integrators? There are no RF parameters can be modified 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? There are no RF parameters can be modified.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? This device is not a professionally installed device.
c. What parameters are accessible or modifiable by the end-user? There are no RF parameters can be modified by the end-user.
(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? There are no RF parameters can be modified.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? The firmware is compiled as binary file and cannot change the RF parameter through this binary file. It is read-only without the change to change the setting.
d. Is the country code factory set? Can it be changed in the UI? Yes, the country code is factory set, 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.? Since it can not be changed in the UI, So there are no this controls.
e. What are the default parameters when the device is restarted? The device will record the last user's operation and use this as the default parameter when the device is restarted. These default RF parameters are the parameters of the authorization scope.
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. It can not be configured in bridge or 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? The operation band and RF parameter of module are fixed can't be change by external DSP, MCU or UI.
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)) Do not set point-to-point or point-to-multipoint mode.

Printed name: Aly Han
Title: Senior Project Manager
Signature of applicant: