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. Answered: We do not release the firmware on our website for downloading. Our direct host manufacturer (OEM) can request the firmware from us and it will be made available via secure server. End-user can request the firmware from our technical support
	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? Answered: Radio frequency parameters are limited by US regulatory domain and country code to limit frequency and transmit power levels. These limits are stored in non-volatile memory by the module manufacturer at the time of production. They will not exceed the authorized values.
	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. Answered: Firmware will be authentication via md5 or sha1 when device boot up. And also, device firmware partition can not be changed by end-user.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. Answered: Self-developed 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? Answered: The device ensures the compliance by checking the configured parameter and operation values according to the regulatory domain and country code in each band. The device configured as a client without radar detection capability
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. Answered: No, third parties don't have the capability to access and change radio parameters. US sold products are factory configured to US.

	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. Answered: Module RF paramters ard store in non-volatile flash, third-party software can not access and changes any paramters
	2. 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. Answered: Module RF paramters ard store in non-volatile flash, third-party software can not access and changes any paramters

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.

a. What parameters are viewable and configurable by different parties?
ALL supported parameters in WebUI. E.g: Device IP

b. What parameters are accessible or modifiable 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?
     Do not support professional installer.
     (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
     Do not support professional installer.

c. What parameters are accessible or modifiable by the end-user?
     (1) Are the parameters in some way limited, so that the installers will not enter parameters exceed those authorized?
     No

     (2) What controls exist that the user cannot operate the device outside its authorization in t U.S.?
     The country code and regulatory domain control do limit all the parameters set
d. Is the country code factory set? Can it 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.?
There is no user configuration GUI.

e. What are the default parameters when the device is restarted?

The country code is factory set and is never changed by UI.
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. Not supported
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? Not supported
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)) Not supported