The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Security.

The information below describes how we 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

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.	End-user can not update the software/firmware
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?	Yes, channel can be modified which must be in the FCC band range.
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.	Digital signature. The device will verify the digital signature before upgrading.
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Verifies the digital signature before upgrading.
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 module can be configured as a client only. Verifies each mode to ensure the module for compliance in the FCC band range.
3rd 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.	We have a digital signature verification mechanism.

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.	No, it is impossible. We do not provide the interface to load device for third parties. Loading new drivers must upgrade software /firmware. The device will verify the digital signature of new software /firmware.
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 regulatory domain and frequencies are factory set. We do not provide the interface for third parties.
SOFTWARE CONFIGURATION DESCRIPTION (The user is not permit to change the parameters through the UI)	
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.	End user
a. What parameters are viewable and configurable by different parties?	Channel, regulatory domain
b. What parameters are accessible or modifiable by the professional installer or system integrators?	Does not provide
(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The regulatory domain, band and frequencies are factory set and cannot be changed.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Only supports the channels specified by U.S.
c. What parameters are accessible or modifiable by the end-user?	Channel.
(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	The regulatory domain, band and frequencies are factory set and canont be changed.

(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	Only supports the channels specified by U.S.
d. Is the country code factory set? Can it be changed in the UI?	factory set and cannot 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.?	The regulatory domain, band and frequencies are factory set and cannot be changed.
e. What are the default parameters when the device is restarted?	regulatory domain, band and frequencies
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 support bridge 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 device acts as 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))	In any mode, using the same antenna, and factory configuration does not allow replacement

Best Regards

Bin Lin
Product Design Engineer