SOFTWARE SECURITY DESCRIPTION

An applicant must describe the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device; and
2. The device is not easily modified to operate with RF parameters outside of the authorization.

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements. While the Commission did not adopt any specific standards, it is suggested that the manufacturers may consider applying existing industry standards. Also, this guide is not intended to be exhaustive and may be modified in the future. There may be follow-up questions based on the responses provide by the applicant for authorization

The device comply with KDB 594280 D01 and D02v01r03

SOFTWARE SECURITY DESCRIPTION	
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. Reply: 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.
	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? Reply: 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. Reply: The firmware is installed on each single module during manufacturing process. The correct firmware is verified and installed by the module manufacturer. In addition, the firmware binary is encrypted using open SSL encryption and the firmware updates can only be stored in non-volatile memory when the firmware is authenticated. The encryption key is known by the module manufacturer only.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. Reply: The process to flash a new firmware is using a secret key to decrypt the firmware, only correct decrypted firmware is stored in non-volatile memory (see #3).
	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? Reply: The device ensures the compliance by checking the configured parameter and operation values according to the regulatory domain and country code in each band.
Third-Party Access Control	1. Explain if any third parties have the capability to operate a U.S.-solddevice on any other regulatory domain, frequencies, or in any manner thatmay allow the device to operate in violation of the device's authorization ifactivated in the U.S. Reply: No, third parties don't have the capability to access and change radio parameters. US sold modules 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 permitintegration of such functions while ensuring that the RF parameters of thedevice cannot be operated outside its

	authorization for operation in theU.S. In the description include what controls and/or agreements are inplace with providers of third-party functionality to ensure the devices'underlying RF parameters are unchanged and how the manufacturer verifies the functionality. Reply: N/A
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization. Reply: N/A

SOFTWARE CONFIGURATION DESCRIPTION GUIDE

In addition to the general security consideration, for devices which have "User Interfaces" (UI) to configure the device in a manner that may impact the operational parameter, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE	
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. Reply: There is no user configuration GUI.
	a) What parameters are viewable and configurable by different parties? Reply: There is no user configuration GUI.
	b) What parameters are accessible or modifiable tothe professional installer? Reply: This device is not subject to professional installation
	i. Are the parameters in some way limited, so thatthe installers will not enter parameters that exceed those authorized? Reply: N/A
	ii. What controls exist that the user cannot operatethe device outside its authorization in the U.S.? Reply: N/A
	c) What parameters are accessible or modifiable by the end-user? Reply: The end user is not able to configure any parameters related to the devices radio
	Are the parameters in some way limited, so thatthe installers will not enter parameters that exceed those authorized? Reply: The parameters can only be changed remotely within the limits of country code US.
	i. What controls exist that the user cannot operatethe device outside its authorization in the U.S.? Reply: The country code and regulatory domain control do limit all the parameters set
	d) Is the country code factory set? Can it be changedin the UI? Reply: The country code is factory set and is never changed by UI.
	i. If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Reply: The country code is factory set and is never changed by UI
	e) What are the default parameters when the deviceis restarted? Reply: At each boot up the country code and the antenna gain are read from the non-volatile memory, those values are configured during production.

	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. Reply: 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? Reply: Not supported
	4. For a device that can be configured as different typesof 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)) Reply: The device does not support these modes/features.