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.	The user can download the software on website, and devices’ upgrade management system . But both two upgrade methods only can upgrade the operating system and built-in application software, the radio frequency parameter will not changed.
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?	The radio frequency parameter store in non-volatile memory(EPROM), and it can not be modified by end user except our professional service engineer used special tools and drivers.
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.	The devices radio frequencies was controlled by the radio frequency parameter which store in non-volatile memory(EPROM). If the radio frequency parameter missing the radio frequencies will not working anymore. And the radio frequency parameter need special tools and drivers to re-fleshed.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The user cannot download software/firmware, because the software upgrade is not support for the end user, and the radio frequency parameter was produced by special software after calibrated, and the radio frequency parameter packed encrypt used Message Digest Algorithm MD5 method.
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	The devices was design as a client without radar detection function.

	operation?	
Software Security description – Third-Party Access Control		
1	Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.	there is no body can re-flash the radio frequency parameter except our professional service engineer used special tools and drivers. RF concerned parameters are stored and encrypted in EPROM, third-part developers could not change the parameters ,even if third-part violently changed the RF parameters uncorrectly, the RF module won't work .
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.	The radio frequency parameter is not easily be re-fresh by the third parties, it must be re-fresh by a special tools and drivers, what more our devices upgrade software will compare the new parameter, if it's not correct the upgrade process will be automatically forced.
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 devices is a end product not a modular devices, and it's function can not working as a modular devices.
Software Security description – USER CONFIGURATION GUID		
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.	The UI for the service engineer need used a special tools, drivers and password. there is no need a professional installer for our devices.
	What parameters are viewable and configurable by different parties?	There is no need a professional installer for our devices.
	What parameters are accessible or	The end user can not accessible

	modifiable to the professional installer? Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? What controls exist that the user cannot operate the device outside its authorization in the U.S.?	or modifiable any radio frequency parameters. RF concerned parameters are stored and encrypted in EPROM, third-part developers could not change the parameters .
	What configuration options are available to the end-user? Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The end user can not accessible or modifiable any radio frequency parameters. RF concerned parameters are stored and encrypted in EPROM, third-part developers could not change the parameters .
	Is the country code factory set? Can it be changed in the UI? If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Yes, there is country code in software, and it is set by factory, and the end user cannot change it.
	What are the default parameters when the device is restarted?	When restarted, the device will resume on/off state and try to reconnect to pair devices remembered and connected before.
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, this devices cannot 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?	This device was designed only as a client without radar detection function. For the end user cannot configure this device in the end user 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	No, it cannot be configured as an AP in DFS band.

	controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. See Section 15.407(a).	