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. 1. The device firmware is encrypted & signed at a secure station in development center and it is uploaded to an internet server that we control. 2. The device downloads the new firmware information and host server URL information from a private internet server. The downloaded information is already signed and it is verified by the device before using it. 3. The device downloads the firmware from the host server using URL. 4. The device decrypts the firmware & verifies the signature before flashing the firmware. Any modification in firmware by middle man can be caught and that firmware will be discarded by the device before installation 5. The device also verifies the signature every time before booting the device.
	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? 1.Users do not have control over the radio parameters, and never directly enter radio parameters other than standard network connection information such as SSID entry, Password and WPS setup. 2. RF parameters can be modified via firmware download but will always retain compliance with original certification. 3. The firmware download will follow the FCC permissive change procedure or new ID application process, should such changes become necessary.
	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. 1. The device firmware is encrypted and signed by unique-perproduct key 2. The device decrypts the firmware & verifies the signature before flashing the firmware. Any modification in firmware by middle man can be caught and that firmware will be discarded by the device before installation
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. 1. The device firmware is encrypted using AES-128 key 2. The device firmware is signed by unique-per-product public/private RSA key chain 3. The signature is verified in CPU using its OTP available RSA-2048 bit key, before booting the firmware.
	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? 1. The device enforces compliance via the signed software 2. The maximum output power is restricted by setting limits based on our FCC test results 3. The device supports either (Wi-Fi Access Point) master or (Wi-Fi station) client modes. It can't act as both master and client at same time. 4. No Wi-Fi parameters can be configured by end-user / installer. 5. The maximum output power is the same regardless of whether it functions as a master or a client. 6. Device doesn't support ad-hoc, Wi-Fi direct modes ….

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. 1. At the time of device boot-up the country code is set to US and it can't be modified by user or by router published data 2. The device does not allow third-party access to SW parameters or configurations including operation outside the Scope of FCC authorization.
	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. 1. The device doesn't allow third-party firmware to be downloaded/flashed 2. The device firmware must be signed by unique-per-product key 3. The firmware signature is verified by CPU using public/private (RSA) key chain before booting the firmware. 4. In every boot stage, the signature of the next stage boot code / firmware is verified. 5. No unsigned code may be executed by the CPU, even including scripting languages like JavaScript.
	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.[7] 1. Not applicable as the device doesn't have Wi-Fi certified transmitter module, instead it is embedded on main PCB. 2. The host driver is part of the device firmware which is encrypted and signed. Hence, it can't be modified by outsider.

III. SOFTWARE CONFIGURATION DESCRIPTION GUIDE

SOFTWARE CONFIGURATION DESCRIPTION	
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. Only the End user configuration is permitted. 1. The radio parameters are not accessible through a UI to any operating party. 2. End users are only able to enter a UI that allows connection to an established AP network and WPS configuration.
	a) What parameters are viewable and configurable by different parties?[9] None that affects compliance
	b) What parameters are accessible or modifiable by the professional installer or system integrators? None that affects compliance
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Not applicable as these types of settings are not accessible to any operating party.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? The device does not allow third-party access to software /firmware parameters or configurations including operation outside the scope of FCC authorization.
	c) What parameters are accessible or modifiable to by the end-user? None that affects compliance
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? Not applicable
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? The device does not allow third-party access to software / firmware parameters or configurations including operation outside the scope of FCC authorization.
	d) Is the country code factory set? Can it be changed in the UI? The country code is hardcoded into the device firmware 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.? Hide this part in firmware, it can not be changed in the user interface.

	e) What are the default parameters when the device is restarted? 1. Network/Wi-Fi Configured device would be acting in Wi-Fi-station (client) mode after device is restarted 2. All Wi-Fi parameters are subjected to connected Wi-Fi Access Point (Home router) 3. Network un-configured device (at factory reset condition) would be acting as Wi-Fi Access Point in 2.4 GHz band.
	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 bridge or mesh mode so can't the radio 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? 1. The device enforces compliance via the signed software 2. The maximum output power is restricted by setting limits based on our FCC test results 3. The device supports either (Wi-Fi Access Point) master or (Wi-Fi station) client mode. It can’t act as both master and client at same time. 4. No Wi-Fi parameters can be configured by end-user /installer. 5. The maximum output power is the same regardless of whether it functions as a master or a client. 6. Device doesn’t support ad-hoc, Wi-Fi direct modes
	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)) 1. The device can’t be configured as different types of access points. 2. No support for external antenna is provided in the device.