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

SOFTWARE SECURITY DESCRIPTION	
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed. Re: The software updates are given to customer via official WEB page.
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters? Re: All the parameter limitations are hard-coded into special permanent memory space to not exceed the authorized limits. Professional installer has no access to change radio parameter limits.
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification. Re: To protect software copywriting or modifications every device has a license which is bonded to a MAC address. Any software modification will end up with a voided license which in turn will prohibit further product usage.
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details. Re: All manufactured product have unique MAC address, unique license and a special product limitation parameters
	5. Describe, if any, encryption methods used. Re: "openssl_sign()" method is used to sign the software license.
	6. 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? Re: Since the software can work in both modes (Master and Client) software was developed to update limitations, during configuration, instantly to meet compliance in any operating mode. Only authorized operating bands are allowed to configure by the professional installer.
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented? Re: All the manufactured products do not support any third party firmware upgrade. Our Company do not cooperate or do not support any thirdparty development company or organization (e.g. OpenWRT).
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded. Re:It is impossible. All the manufactured products do not support any third party firmware upgrade. Our Company do not cooperate or do not support any thirdparty development company or organization (e.g. OpenWRT)
	3. 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. Re: It is impossible for the third party to develop a software manufactured devices.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device? Re: The product Radio Frequency (RF) calibration information is written in non-standard way, thus making impossible for the third party to develop a software manufactured devices.
	5. For modular devices, describe how authentication is achieved when used with different hosts. Re: Products, which are certified as modular transmitters, are used only

	with original software as well. This way protecting illegal device configuration or use.

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. To whom is the UI accessible? (Professional installer, end user, other.) Re: Professional installer
	a) What parameters are viewable to the professional installer/end-user? Re: Below parameters can only be viewable to the professional: - Operating frequency - Channel width (e.g. 20MHz, 40MHz) - Modulation and coding rate - Spacial streams number - Transmit power - Guard interval between transmitted symbols
	b) What parameters are accessible or modifiable to the professional installer? Re: The professional installer may change below listed parameters: Below parameters limit all follow FCC rule and professional installer can't set those parameters over limit. This also means they will be inalterable parameters once beyond FCC limit. - Operating frequency - Channel width (e.g. 20MHz, 40MHz) - Modulation and coding rate - Spacial streams number - Transmit power - Guard interval between transmitted symbols
	i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Re: Yes
	ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.? Radio driver has special code part where allowed frequency, TX power, EIRP are defined. Those values are hardcoded, compiled and cannot be changed. This also means they will be inalterable parameters once beyond FCC limit.
	c) What configuration options are available to the end-user? Nothing can be configuration by the end-user, because they cannot access the configuration UI.
	i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Re: YES
	ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.? Radio driver has special code part where allowed frequency, TX power, EIRP are defined. Those values are hardcoded, compiled and cannot be changed outside its authorization in the U.S.
	d) Is the country code factory set? Can it be changed in the UI? US country code is hardcoded in the driver and cannot be changed in the UI.
	i. If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Radio driver has special code part where allowed frequency, TX power, EIRP are defined. Those values are hardcoded, compiled and can only be changed within its authorization in the U.S.
	e) What are the default parameters when the device is restarted? Frequency: 5745 MHz Channel size: 40 MHz

	Tx power: varies from 1 to 25 depending on antenna Data rate: auto
	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. Product is defined to work in bridge mode only.
	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? Re: Adjusted UI parameters will make sure, professional installer will comply with the regulation requirements.
	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)) Re: Since the device can work in multiple modes with multiple antennas (e.g. connectorized product version), the software requires to enter the antenna gain parameter to adjust UI parameters. Adjusted UI parameters will make sure, professional installer will comply with the regulation requirements.