UNII Software Security Description

FCC ID: ACJ9TGWL22B

SOFTWARE SECURITY DESCRIPTION		
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.	**The driver software is downloaded from website of Panasonic by OTA. It is digitally signed by proprietary key.**
	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?	**There are no the radio frequency parameters that are modified by any software/firmware without hardware changes. Because all radio frequency parameters of the mounted radio module when programmed into the module's internal non-volatile memory (NVM) at the module manufacture's factory. The same is true of module's firmware. These cannot be changed except module manufacture's factory. Therefore, it will not exceed the authorized parameters.**
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.	**The driver software is digitally signed by proprietary key. When the user installs it, it is verified by system. The user can install verified driver software only. The module's firmware cannot be changed except module manufacture's factory.**
	4. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	**The proprietary public key encryption is used of legitimate driver software.**
	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	**The device will be able as master only ISM band. For DFS, non-DFS bands the device will**

	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?	**only listen for a master device. These parameters are fixed at the factory. And the end user cannot access to change master and client in each band.**
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.	**Third-parties do not have the capability to operate a US sold device on any other regulatory domain, frequencies and all RF parameters.**
	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 module's hardware platform and firmware are proprietary of module manufacture. The software tool chain including all firmware is not available to third-parties. Therefore, third-parties cannot use "flashing" and load non-US versions of the firmware or installation of third-party firmware on the device.** **RF parameters are verifies using the software tool chain by the manufacturer.**
	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.	**This module cannot modify the firmware and all RF parameters according to General Description #2 and Third-Party Access Control #2 except module manufacture.**

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.	**The UI is accessible by anyone using the device.**
	a) What parameters are viewable and configurable by different parties?	**Nothing to operate RF parameters**
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	**Nothing to operate RF parameters**
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	
	c) What parameters are accessible or modifiable by the end-user?	**Nothing to operate RF parameters**
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	
	d) Is the country code factory set? Can it be changed in the UI?	**The county code is factory set. It cannot change 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.?	
	e) What are the default parameters when the device is restarted?	**Even if the device is restarted, the default parameters are not changed.**
	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.**

	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 will be able as master only ISM band. For DFS, non-DFS bands, the device will only listen for a master device. These parameters are fixed at the factory. And the end user cannot access to change master and client in each band.**
	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 Section15.407(a))	**The device will be able as master only ISM band. For DFS, non-DFS bands, the device will only listen for a master device. These parameters are fixed at the factory. And the end user cannot access to change master and client in each band. The device is embedded special antennas, they do not configure by user.**