Software Security Description – KDB 594280 D02v01r01 Section II	
General Description	
1. Describe how any software/firmware update will be obtained, downloaded, and installed.	Only one firmware will be upgrade.
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?	No (WiFi channel area code ID is only set in factory, instead of firmware)
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	1. No authentication protocol is used. 2. There is checksum information in firmware upgrade bin file and flash ROM.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	1. only checksum information is used. 2. There is checksum information in firmware upgrade bin file and flash ROM.
5. Describe, if any, encryption methods used.	No encryption methods is used.
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?	The device is configured as client.
Third-Party Access Control	
1. How are unauthorized software/firmware changes prevented?	There is checksum information in firmware upgrade bin file and flash ROM.
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.	It is impossible to load device drivers that can modify the RF parameters, country code, and other parameters. There is no telnet feature and console port.
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.	None. There is no telnet feature and console port.
4. What prevents third parties from loading non-US versions of the software/firmware on the device?	No method is used. The RF parmeters are not included in firmware. So it is not necessary to prevent third partied from loading non-US firmware version.
5. For modular devices, describe how authentication is achieved when used with different hosts.	This is not modular devices.

Company Officer: Richard Mullen

Telephone Number: 201-348-7758

Email: Richard.Mullen@us.panasonic.com