# SOFTWARE SECURITY INFORMATION

FCC ID: **VTV-RFWKD**

| SOFTWARE SECURITY DESCRIPTION | | |
|---|---|---|
| General Description | 1. Describe how any software/firmware update will be obtained, downloaded, and installed. | Method1:<br>The firmware upgrade must via an engineering tool. The tool will initiate FTP client connecting operation and enable firmware update mode. Once the mode is enabled, the module will check the firmware version in the ftp site and update automatically.<br>Method2:<br>Update the firmware via USB port on the engineering tool. The tool will check the firmware version, enable the updating mode, and install it. |
| | 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 is no access to modify frequency parameter but only band changes. |
| | 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. | This is an 802.11 a/b/g/n module. The firmware on the device does not support writing to non-volatile storage areas containing firmware, except through the use of our firmware's upgrade functions. The firmware upgrade functions only allow programming of firmware that has been provided by TSC. |
| | 4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details. | See #3. |
| | 5. Describe, if any, encryption methods used. | No. |
| | 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? | Only support Wi-Fi client mode. |

| | | |
|---|---|---|
| Third Party Access Control | **1.** How are unauthorized software/firmware changes prevented? | Only official firmware functions can write to non-volatile storage. This means that code and/or instructions provided by a third party may not modify non-volatile storage. Furthermore, firmware features that modify non-volatile storage are designed to access very specific locations on the storage device. The only means of writing to the firmware area of the storage device is the firmware upgrade feature. The firmware upgrade feature will only write firmware to the storage device, if that firmware has been provided by TSC. |
| | **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. | There is no practical means for a third party to employ alternative device drivers on the device. |
| | **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. | There is no access method release to any parties. When US locked devices reach other countries, they must be returned for replacement with non US locked devices. There is no way to alter or unlock them. |
| | **4.** What prevents third parties from loading non-US versions of the software/firmware on the device? | There is only one firmware without regulatory modification method provided. All US sold devices are locked to the US FCC rules of this certification, and will never operate in a manner that violates the certification. The country lock is stored in non-volatile storage, in an area unaffected by factory reset. |
| | **5.** For modular devices, describe how authentication is achieved when used with different hosts. | This module follows 802.11 a/b/g/n standard. |

| SOFTWARE CONFIGURATION DESCRIPTION | | |
|---|---|---|
| USER CONFIGURATION GUIDE | **1.** To whom is the UI accessible? (Professional installer, end user, other.) | There is no UI for user configuration. |
| | **a)** What parameters are viewable to the professional installer/end-user?6 | N/A |
| | **b)** What parameters are accessible or modifiable to the professional installer? | N/A |
| | **i)** Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? | N/A |
| | **ii)** What controls exist that the user cannot operate the device outside its authorization in the U.S.? | N/A |
| | **c)** What configuration options are available to the end-user? | N/A |
| | **i)** Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? | N/A |
| | **ii)** What controls exist that the user cannot operate the device outside its authorization in the U.S.? | N/A |
| | **d)** Is the country code factory set? Can it be changed in the UI? | N/A |
| | **i)** If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? | N/A |
| | **e)** What are the default parameters when the device is restarted? | N/A |
| | **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. | The device 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? | Only support Wi-Fi client mode. |
| | **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)) | N/A |

**Name and surname of applicant (or authorized representative): LION HO**

**Date: 2015.1.29** Signature: Lion Ho