

Date: 2020/3/31
FCC ID: ARS-WCT5GM2511
IC:9190A-WCT5GM2511

Software Security Description

We, Top Victory Electronics(Taiwan) Co., Ltd., hereby declare that requirements of WCT5GM2511 have been met and shown on the following question.

Software Security Description	
General Description	<p>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 software/firmware aren't provided through website or device's management.</p>
	<p>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? Any software/firmware can't modify RF parameters that can affect and exceed the authorized RF characteristics.</p>
	<p>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 answer is same with No.2 question.</p>
	<p>4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate. The answer is same with No.2 question.</p>
	<p>5. Describe in detail any encryption methods used to support the use of legitimate software/firmware. The answer is same with No.2 question.</p>
	<p>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 operates only as a client.</p>
Third-Party Access Control	<p>1. 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. The device isn't provided to any third parties but is used for in house host product only. Therefore, there is no case that third parties operate the device.</p>


	<p>2. What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from “flashing” and the installation of third-party firmware such as DD-WRT.</p> <p>The answer is same with No.1 question.</p>
	<p>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.</p> <p>The answer is same with No.1 question.</p>

Software Security Description	
User Configuration Guide	<p>1. To whom is the UI accessible? (Professional installer, end user, other.)</p> <p>Professional installer and end user.</p>
	<p>a) What parameters are viewable to the professional installer/end-user?</p> <p>-RF ON/OFF -Search WiFi access point. -Connect to WiFi access point.</p>
	<p>b) What parameters are accessible or modifiable by the professional installer?</p> <p>All parameters described in a) are accessible and modifiable by the professional installer.</p>
	<p>(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?</p> <p>Any parameters described in a) don't affect exceeding the authorization.</p>
	<p>(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?</p> <p>Because the UI is limited as described in a), the user can't operate the device outside its authorization.</p>
	<p>c) What parameters are accessible or modifiable to by the end-user?</p> <p>All parameters described in a) are accessible and modifiable by the professional installer.</p>
	<p>(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?</p> <p>Any parameters described in a) don't affect exceeding the authorization.</p>

	<p>(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Because the UI is limited as described in a), the user can't operate the device outside its authorization.</p>
	<p>d) Is the country code factory set? Can it be changed in the UI? Country code is factory set. And, the UI can't change country code.</p>
	<p>(1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? (This question is not valid.)</p>
	<p>e) What are the default parameters when the device is restarted? -RF ON. -Search WiFi access point:idle -WiFi access point: not connected to -country code:US(1-11ch), Canada(1-11ch)</p>
	<p>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.</p>
	<p>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 operates only as a client.</p>
	<p>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)) The device can't be configured as different types of access points, such as point to point or point to multipoint.</p>

If any questions regarding this declaration, please don't hesitate to contact us.

Sincerely

 /Senior Director
(Signature/Title)

Company name: Top Victory Electronics(Taiwan) Co., Ltd.

冠捷科技集團

新北市 23553 中和區連城路 230 號 10 樓 Tel:886-2-82261668 Fax:886-2-82261707

10F., No. 230, Liancheng Rd., Zhonghe Dist., New Taipei City 23553, Taiwan (R.O.C.)