



## Software Security/Configuration Description (Jabra PanaCast 50 – model: VSM020)

This document holds the software security description and the software configuration description for our product model, VSM020, which makes use of the U-NII frequency band.

<b>SOFTWARE SECURITY DESCRIPTION</b>	
<b>General Description</b>	<p>1. Describe how any software/firmware updates for elements that can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate.</p> <p><b>There is no downloadable software provided by the manufacturer that can change critical radio transmitter parameters. All critical parameters are programmed into factory OTP memory and cannot be modified or overridden by third parties.</b></p>
	<p>2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?</p> <p><b>There are no RF parameters that can be modified. All RF parameters are programmed in factory OTP memory and cannot be modified or overridden by third parties.</b></p>
	<p>3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification.</p> <p><b>The firmware is programmed from the factory and cannot be modified by third parties.</b></p>
	<p>4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.</p> <p><b>The firmware is programmed from the factory and cannot be modified by third parties, so there is no need for encryption.</b></p>
	<p>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 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?</p> <p><b>This is a client module only.</b></p>

SOFTWARE SECURITY DESCRIPTION	
<b>Third-Party Access Control</b>	<p>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.</p> <p><b>Third parties are not able to operate the device in any way that is in violation of the U.S. authorization.</b></p>
	<p>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.</p> <p><b>Third parties are not able to operate the device in any way that is in violation of the U.S. authorization.</b></p>
	<p>3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers 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 RF parameters are not modified outside the grant of authorization.</p> <p><b>This not a modular device, but an end product.</b></p>

## SOFTWARE CONFIGURATION DESCRIPTION

<b>User Configuration Guide</b>	<p>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.</p>
	<p>a. What parameters are viewable and configurable by different parties? <b>No UI is provided.</b></p>
	<p>b. What parameters are accessible or modifiable by the professional installer or system integrators? <b>None</b></p>
	<p>(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? -</p>
	<p>(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? -</p>
	<p>c. What parameters are accessible or modifiable by the end-user? <b>None</b></p>
	<p>(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? -</p>
	<p>(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.? -</p>
	<p>d. Is the country code factory set? Can it be changed in the UI? <b>This is a client device that receives the country code information from the local access point - no UI is provided for modification.</b></p>
	<p>(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? -</p>
	<p>e. What are the default parameters when the device is restarted? <b>After a restart, the device receives country code information from the local access point and sets default parameters accordingly.</b></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. <b>No</b></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? <b>This is a client device.</b></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)) <b>This device is not an access point.</b></p>	