Software Security Declaration for U-NII Devices

Product: PanaCast 40 Video Bar System (Model: VSM050)

Software Security Description			
General Description	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.	Firmware updates are downloaded from GN Audio controlled websites. The firmware is validated by the device before any update. However, RF parameters cannot be changed by ordinary firmware updates.
	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?	Firmware updates will not modify any RF parameters.
	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.	The RF parameters can no be modified by users.
	4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	N/A
	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?	This device is client only.
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.	This device will operate as per instructed by the master (access point).
	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.	Third-party firmware is not permitted.
	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.	N/A – not a module.

Software Configuration Description			
	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.	There is only one level of UI. This is accessible to everyone.
		a. What parameters are viewable and configurable by different parties?	Users can select between Ethernet, 2.4 GHz WLAN or 5 GHz WLAN.
		b. What parameters are accessible or modifiable by the professional installer or system integrators?	Nothing additional.
		(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	N/A
		(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	N/A
		c. What parameters are accessible or modifiable by the end-user?	Users can select between Ethernet, 2.4 GHz WLAN or 5 GHz WLAN.
		(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	The user cannot access the regulatory settings of the device.
		(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	There is no such restriction.
		d. Is the country code factory set? Can it be changed in the UI?	There is no access to country setting.
		(1) If it can be changed, 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?	Last stored user setting + RF parameters
	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?	No - client only
	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 – this device is a client device – and operation is based on internal antennas.