Ben Botros Manager – Regulatory Compliance
Panasonic Corporation of North America

FCC Software Configuration Control Declaration

July 15, 2024
HEG-24-U016

Federal Communications Commission
Authorization and Standards Division
7435 Oakland Mills Road
Columbia, MD 21046 USA

Subject: Original Application for Technics Wireless Speaker System, Model SC-CX700
Under FCC ID ACJ-SC-CX700

To whom it may concern:

In reference to FCC Country Code Selection guidelines identified in KDB 594280, Panasonic Corporation of North America declare that no third party will have software, or configuration control, to program the device out of compliance of the technical rules under which it has been certified.

Please contact me if you have any questions or need further information regarding this application.
.

Sincerely,

Ben Botros
Manager – Regulatory & Compliance
Panasonic Corporation of North America

Panasonic

Ben Botros Manager – Regulatory Compliance
Panasonic Corporation of North America

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

FCC ID: ACJ-SC-CX700

Pursuant to KDB 594280 D02, the overall security measures and systems that ensure that:

1. only properly authenticated software is loaded and operating the device; and
2. the device is not easily modified to operate with RF parameters outside of the authorization.

Are described.

The following questions are addressed the description of the software in the operational description for the device and clearly how the device meets the security requirements.

SOFTWARE SECURITY DESCRIPTION		
General Description	1. Describe how any software/firmware updates for elements than 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.	Software/firmware will be obtained by the factory, downloaded from the ODM website, and installed by the end user. Software is accessed through Web UI when computer is connected.
	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?	The RF parameters cannot be modified by software. All these parameters will not exceed the authorized parameters. The firmware has been complied as binary file. It couldn't change the setting RF parameter through this binary file. It is read-only without change.
	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 firmware is installed on each single module during manufacturing process. The correct firmware is verified and installed by the module manufacturer. In addition, the firmware binary is encrypted using open SSL encryption and the firmware updates can only be stored in non-volatile memory when the firmware is authenticated. The encryption key is known by the module manufacturer only.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Standard open SSL encryption is used (see #3).
	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	The device ensures the compliance by checking the configured parameter and operation values according to their regulatory domain and country code in each band.

	another; how is compliance ensured in each band of operation?	
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.	There are no third parties that would have the capability to operate a US 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.
	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.	The embedded software is protected via the measures explained in the previous section. Distributions of host operating software are encrypted with a key. Unauthorized firmware is not accepted by the firmware update process.
	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.	The module is not available for sale or installation outside of company licensing agreements. Modules are always installed in host systems in the factory by integrators (OEM) responsible for loading authorized software.

Ben Botros Manager – Regulatory Compliance
Panasonic Corporation of North America

SOFTWARE CONFIGURATION DESCRIPTION GUIDE

For devices which have “User Interfaces” (UI) to configure the device in a manner that may impact the operational RF parameters, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

SOFTWARE CONFIGURATION DESCRIPTION		
USER CONFIGURATION GUIDE	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.	The UI is accessible to anyone using the device….
	a. What parameters are viewable and configurable by different parties?	Nothing to operate RF parameters
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	Nothing to operate RF parameters
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Nothing to operate RF parameters
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The RF Parameters is put in read-only partition of EUT’s flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition.
	c. What parameters are accessible or modifiable by the end-user?	The end user is able to configure the operation frequency, modulation, reduce the output power levels etc. The end user cannot change the antenna gain and country code, those settings are programmed at factory production time.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Nothing to operate RF parameters
	(2) What controls exist so that the user cannot operate the device outside its	The RF Parameters is put in read-only partition of EUT’s flash and are only

	authorization in the U.S.?	installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition.
	d. Is the country code factory set? Can it be changed in the UI?	Yes, the country code is set by factory. It cannot be changed in the UI.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	The county code is factory set. It cannot change by UI.
	e. What are the default parameters when the device is restarted?	Factory setting.
	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, this device cannot be configured in both bridge and 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?	The device operates in Client mode only and user cannot change configuration.
	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 operates in Client mode only and user cannot change configuration.

Sincerely,

Ben Botros
Manager – Regulatory & Compliance
Panasonic Corporation of North America