Model: AURORA V2.2
FRN: 0024863870
FCC ID: 2AFSV-AURORA-V2-2
IC: 30959-AURORAV22

Subject: Software security requirements for U-NII device.

The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03.

General Description	
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.	There is no downloadable software provided by the manufacturer that can modify critical radio transmitter parameters. All critical parameters are programmed at the factory and cannot be modified by third parties.
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 are no RF parameters that can by modified. All RF parameters are programmed at the factory and cannot be modified by third parties. End-user cannot access them.
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 NVRAM of the module can only be written once and cannot be modified after delivery. End-user cannot access them.
4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	The NVRAM of the module can only be written once and cannot be modified after delivery.

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?	The device can only act in client mode. The device cannot act as a master in all bands.
3rd 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.	No. Any third parties are not approved to operate in any manner that is violation of the certification in the U.S. The third-party cannot access to any parameter.
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 firmware is programmed at the factory and cannot be modified by third parties. The third-party cannot access to it.
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.	Default mode is always FCC and ISED compliant, and the NVRAM of the module cannot be written after delivery. The third-party cannot access to it.

SOFTWARE CONFIGURATION DESCRIPTION	
1. To whom is the UI accessible? (Professional installer, end user, other.)	N/A
a) What parameters are viewable to the professional installer/end-user?	None of the parameters are exposed to anyone.
b) What parameters are accessible or modifiable to the professional installer?	None
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.?	Default mode is always FCC and ISED compliant. Other country modes cannot be activated without writing in the drive's bin files. However, bin files can only be modified at the factory. End user cannot access to it.
c) What configuration options are available to the end-user?	None
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	None
ii) What controls exist that the user cannot operate the device outside its authorization in the US?	Default mode is always FCC and ISED compliant. Other country modes cannot be activated without writing in the drive's bin files. However, bin files can only be modified at the factory. End user cannot access to it.
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?	Always FCC and ISED compliant.
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?	The device can only act in client mode. The device cannot act as a master in all bands.
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))	This device is not an access point.

Yours sincerely,

Company Officer : Mark Jamtgaard
Telephone Number : 1 408 884 2162
Email : mark@retailnext.net
Company name : Retailnext Inc.
Address : 60 S Market Street, Suite 310, San Jose, CA 95113, US
Date : Dec 7, 2023