U-NII devices declaration letter

We, **Bluebird Inc.** declare that:

FCC ID: SS4EK430

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.	There's a software update program installed in the device that can download and install latest software/firmware to the device over the air.
	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?	There is no RF parameter change during FW update. All critical parameters are programmed in ROM cannot be modified
	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.	There's a signature in the software binary images that is certified by the certificate in the device. If the authentication fails, the device does not boot up.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Same above.
	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 can only be configured as a client in 5GHz(NII) bands where it operates using passive scanning only. It is supported Hotspot Mode that The 2.4 GHz band for channels 1 through 11 only. RF parameters are set up in compliance with FCC regulations for each band/mode.

Reference (active link): 594280 D02 U-NII Device Security v01r03

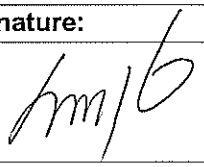
Third-Party Access Control	1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.	Not applicable
	2. Describe, 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 SW device drivers include parameters about channels and country and are made out from the S/W source and not accessible to any user.
	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.	This device is not a transmitter modular device.

Reference (active link): 594280 D02 U-NII Device Security v01r03

SOFTWARE SECURITY 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.	
	a. What parameters are viewable and configurable by different parties?	Signal strength and SSID are viewable on the UI. There is no other RF parameters view able to user
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	Professional installer can't access to any parameters
	1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	There is no input method.
	2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	There is no control that user operate the device outside its authorization
	c. What parameters are accessible or modifiable by the end-user?	Not applicable
	1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Not applicable
	2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	Not applicable
	d. Is the country code factory set? Can it be changed in the UI?	Yes, it's setup but it's never can 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.?	Not applicable
	e. What are the default parameters when the device is restarted?	This product boots with release parameter by the developer.
	2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available	Not applicable

Reference (active link): 594280 D02 U-NII Device Security v01r03

	in KDB Publication 905462 D02.	
	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?	Refer to answer 5 of the General Description.
	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))	Not applicable

City and Country:	Date:	Name:	Function:	Signature:
Seoul, Korea	Sep. 30, 2021	KyeJeong Baek	HW Team Director	

Reference (active link): 594280 D02 U-NII Device Security v01r03