IAdea Corporation
3F, No. 21, Lane 168, Xingshan Road, NeihuDist.,
Taipei City 11469, Taiwan, R.O.C.
Tel : 886-2-2791-1110/ Fax: 886-2-2791-1170
Tel : 886-2-2791-1110/ Fax: 886-2-2791-1170

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

Date: June， 23, 2022

ATTN: FCC

Subject: Attestation Letter regarding UNII devices

FCC ID: Y9E-IAD16005E, Software security questions and answers per KDB 594280 D02 v01r03:

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 is no downloadable software provided by the manufacturer that can modify critical radio transmitter parameters. All critical parameters are programmed in Chip memory at the factory and cannot be modified or overridden by third parties.
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 are no RF parameters that can be modified. All RF parameters are programmed in Chip memory at the factory and cannot be modified or overridden by third parties.
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 in the factory has been fixed in to chip, can't change, so there is need for validation. Driver under it operating system provides a digital certificate authentication.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. The firmware in the factory has been fixed in chip, can't be changed, there is no need for validation. Driver is in binary form, it is own closure, no need for verification.
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? Not applicable, this device only supports client without radar detection. The RF parameters has been fixed in the wifi module firmware and cannot be altered, so the user has no way to break the compliance on the device.
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. Third parties do not have the capability to operate in any manner that is violation of the certification in the U.S

IAdea Corporation
3F, No. 21, Lane 168, Xingshan Road, NeihuDist.,
Taipei City 11469, Taiwan, R.O.C.
Tel : 886-2-2791-1110/ Fax: 886-2-2791-1170
Tel : 886-2-2791-1110/ Fax: 886-2-2791-1170

	1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Programmed for default mode which is always FCC compliant. Always set for default for all start-ups, resets, timeouts or other host or network events. e) What are the default parameters when the device is restarted? Always FCC 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, it can't work in the bridge or the 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? It can only work in client mode, and cannot be configured.
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.

Signature:

Printed Name: Yung-Tsai Wang
Position: Director of product development
Company Name: IAdea Corporation