The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

Software Security Description based on KDB 594280 D02 U-NII Device Security

1. Describe how any software/firmware update will be obtained, downloaded and installed Description: **It is only one way (USB) to copy and install the Software/Firmware.**
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? **Parameters. The product follows AP setting to adjust the frequency parameters. Software/Firmware are encryped with integrity check.**
3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification **Software/Firmware are encrypted with integrity check (AES128) to ensure the validity of its content.**
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details **It is not support the wireless updating. So it is not use the verification protocol. But software has encrypted by AES128, Because Software/Fimware are legitimate.**
5. Describe, if any, encryption methods used **Description: Firmware encrypted by AES128**
6. 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 be operated as master and client, but the software only support a way to operated, if operate as master then client can't to operate and if operated as client then master can't to operate. Only 149 channel can be operated as master for this device, without radar detection.**
7. How are unauthorized software/firmware changes prevented? **Software/Firmware are protected by signing, encryption and its checksum for integrity check Without passing the firmware integrity check, no upgrade will be performed**.

8. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded. **It is not possible, The device block unauthorized device driver so that only allowed drivers can be loaded.**
9. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification. **The software/firmware are encrypted and controlled by the manufacturer through an integrity check (AES128). So, it is not possible.**
10. What prevents third parties from loading non-US versions of the software/firmware on the device? **Softeawre/Firmware are protected by signing, encryption and its checksum for integrity check Without passing the firmware integrity check, no upgrade will be performed.**
11. For modular devices, describe how authentication is achieved when used with different hosts. **It is not modular device.**

In addition to the general security consideration, for devices which have “User Interfaces” (UI) to configure the device in a manner that may impact the operational parameter, the following questions shall be answered by the applicant and the information included in the operational description.

USER CONFIGURATION GUIDE

1. To whom is the UI accessible? (Professional installer, end user, other.)
a) What parameters are viewable to the professional installer/end-user?

In UI, there are just for end user, they can contol only user interface like navigation and AV function. Both professinal installer and end user couldn't contect detail setting.

b) What parameters are accessible or modifiable to the professional installer?

They can not access any detail parameters in devices cause in UI, there are no menu for modifiable menu.

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

All above parameters have pre-defined rang according to the certification test result. They are stored in the ROM, which not allow user to adjust beyond the pre-set value.

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

All parameters indicating different countries are permanent setting in the ROM. If a device is a product for US, it cannot be changed for another region.

c) What configuration options are available to the end-user?

End user can not contect any detail configuration options.

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

All above parameters have pre-defined rang according to the certification test result. They are stored in the ROM, which not allow user to adjust beyond the pre-set value.

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

All parameters indicating different countries are permanent setting in the ROM. If a device is a product for US, it cannot be changed for another region.

d) Is the country code factory set? Can it be changed in the UI?

It has country code but cannot be changed in the UI.

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?

It is depend on country code, If it is US region, country code will be loaded US.
Our Wi-Fi related paramters are permenant even if the device is restarted.

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.

Wifi mesh network not supported.

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 be operated as master and client, but the software only support a way to operated, if operate as master then client can't to operate and if operated as client then master can't to operate. Only 149 channel can be operated as master for this device, without radar detection.**
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)) **Only point-to-point mode, no any other modes for configuration.**

How the product comply 15.407(c)

Data transmission is always initiated by Software, which is then passed down through the MAC, through the digital and analog baseband, and finally to the RF chip. Several special packets (ACKs, CTS, PSPoll, etc,...) are initiated by the MAC. These are the only ways the digital baseband portion will turn on the FR transmitter, which it then turns off at the end of the packet. Therefore, the transmitter will be on only while one of the aforementioned packets is being transmitted.