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 Security.

The information below describes how TI maintain WiLink8 module overall security measures and systems so that only:

1. Authenticated software is loaded and operating on the device
2. The device is not easily modified to operate with RF parameters outside of the authorization

The TI WL1837 / 07 module is controlled by firmware loaded from a Host device, the firmware controls all the RF parameters to operate the device.

The firmware is Texas instruments IP and the source code is not shared with customers; the firmware is a binary file and cannot be created by anyone else but Texas Instruments.

The country in which the device should be operated defined in the Host in a binary file that would be created by TI's customers and they should handle the protection mechanism of this file.

TI provides default BT initialization script with power tables aligned with FCC certification. End users have the ability to make modifications to the BT power tables through HCI command. This could result in a variance of the power output, and impact device operation. TI will notify users through the product datasheet that any such alterations could result in device performance outside the scope of the relevant FCC equipment authorizations, and that the users will need to seek appropriate FCC consents prior to introducing products incorporating modifications of the device BT power tables.

The user would have the ability to make modifications to the init file. This could result in a variance of the power output, and resultant impact on device operation. TI will notify users through the product datasheet that any such alterations could result in device performance outside the scope of the relevant FCC equipment authorizations, and that the users will need to seek appropriate FCC consents prior to introducing products incorporating modifications to the init file.

General Description	
1. Describe how any software /firmware update will be obtained, downloaded, and installed.	TI publishes official firmware files as Binary file to customers.
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?	Radio parameters are defined by the firmware, user cannot access to those parameters.
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	Firmware source code is not shared with customers, therefore only TI can modify it and release official binary firmware.

General Description	
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details	Firmware source code is not shared with customers, therefore only TI can modify it and release official verified binary firmware file.
5. Describe, if any, encryption methods used?	Firmware is a binary file.
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?	There is a CRDA bin file which contains the list of operational regulatory channels, as this file is a binary and provided by TI official release. The CRDA bin file should be protected by the customer on the host side.

3rd Party Access Control	
1. How is any unauthorized software/firmware change prevented?	Firmware changes cannot be done since it is a binary file and the source code is TI IP which is not shared with customers
2. 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.	RF parameters can be configured only from firmware, Ti customers cannot create different firmware binary file, but have the ability to change the Country by creating a new CRDA binary file and it is their responsibility to protect it and follow TI certification.
3. 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	Refer to section #2
4. What prevents third parties from loading non-US versions of the software/firmware on the device?	Refer to section #2
5. For modular devices, describe how authentication is achieved when used with different hosts.	Refer to section #2

SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[1]	
1. To whom is the UI accessible? (Professional installer, end user, other.)	Irrelevant since module certification only without GUI.
a) What parameters are viewable to the professional installer/end-user?[2]	Irrelevant since module certification only without GUI.
b) What parameters are accessible or modifiable to the professional installer?	Irrelevant since module certification only without GUI.

[1] This section is required for devices which have a "User Interfaces" (UI) to configure the device in a manner that may impact the operational parameter. Supporting information is required in the operational description. The operational description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

[2] The specific parameters of interest for this purpose are those that may impact the compliance of the device. These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[1]	
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Irrelevant since module certification only without GUI.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Irrelevant since module certification only without GUI.
c) What configuration options are available to the end-user?	Irrelevant since module certification only without GUI.
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Irrelevant since module certification only without GUI.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Irrelevant since module certification only without GUI.
d) Is the country code factory set? Can it be changed in the UI?	Irrelevant since module certification only without GUI.
i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Irrelevant since module certification only without GUI.
e) What are the default parameters when the device is restarted?	Irrelevant since module certification only without GUI.
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.	Irrelevant since module certification only without GUI.
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?	Irrelevant since module certification only without GUI.
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))	Irrelevant since module certification only without GUI.