The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D01 and D02 U-NII Security. The information below describes how we maintain the 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

3 The equipment meets the requirement of 594280 D01 KDB

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 way to get.
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?	These parameters cannot exceed authorized parameters. SSS(CCK,DQPSK,DBPSK):2412-2462MHz OFDM(64QAM, 16QAM, QPSK, BPSK): 2412-2462MHz; 5180-5240MHz; 5745-5825MHz
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	No authentication protocols
4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	No verification protocols
5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	No encryption methods used to support the use of legitimate software/firmware
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?	This is an active SRD equipment only one mode.If surrounded by the corresponding wireless signal automatically

3rd Party Access Control	
1. 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.	Not aware of any such method/ capabilities today for 3rd parties .
2. What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.**1**	No prevention present today to load non-U.S. version of software/firmware on a U.S. version of the same device
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.**2**	The hosts manufactures fully comply with these software security requirements for U-NII devices.

1. To whom is the UI accessible? (Professional installer, end user, other.)	End user
a) What parameters are viewable to the professional installer/end-user?**3**	No parameters is viewable to the professional installer/end-user.
b) What parameters are accessible or modifiable by the professional installer?	No parameters is accessible or modifiable by the professional installer.
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes

1 See, for example, www.dd-wrt.com/ **2** Note that Certified transmitter modules must havesufficient level of security to ensure that when integrated into a permissible host the device parameters are not modified outside those approved in the grant of authorization. (See, KDB Publication 99639). This requirement includes any driver software that may be installed in the host, as well as, any third party software that may be permitted to control the module. A full description of the process for managing this should be included in the filing. **3** The specific parameters of interest for this purpose are those that may impact the

SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[1]	
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	No controls exist that the user cannot operate the device outside its authorization in the U.S.
c) What parameters are accessible or modifiable to by the end-user?	No parameters are accessible or modifiable to by the end-user
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes
d) Is the country code factory set? Can it be changed in the UI?	Can not be
i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	None
e) What are the default parameters when the device is restarted?	No default parameters when 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.	Bridge or Mesh mode is 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?	No UI control.
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))	Use only one type of antenna

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.