TAPCO®
Safe travels.

FCC ID: 2ANWN-RM8003-03

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 v01 r03**. 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 cannot be modified to operate with RF parameters outside of the authorization.

GENERAL DESCRITION	
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 to modify RF parameters. All RF parameters are calibrated and programmed at the factory and cannot be modified by third party users.**
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?	**All RF parameters are calibrated and programmed at the factory and cannot be modified by third party users.**
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 is programmed at the factory and cannot be modified by third party users.**
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	**The firmware is programmed at the factory and cannot be modified by third party users therefore no encryption is necessary.**
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?	**All RF parameters are calibrated and programmed at the factory and cannot be modified by third party users.**

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 a U.S.-sold device on any other regulatory domain, frequencies, or any other manner that would violate the U.S. certification.**
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.	**Third party software or firmware is not permitted. All RF parameters are calibrated and programmed at the factory and cannot be modified by third party users.**
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.	**RF parameters are not adjustable. All RF parameters are calibrated and programmed at the factor and cannot be modified by third party users. The module is not controlled by driver software on the host and RF parameters stored in memory cannot be overwritten.**

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.	**Frequency Hop Sequence, Binding code and Master/Client mode are permitted through the UI.**
a. What parameters are viewable and configurable by different parties?	**Frequency Hop Sequence, Binding code and Master/Client mode are permitted through the UI.**
b. What parameters are accessible or modifiable by the professional installer or system integrators?	**Frequency Hop Sequence, Binding code and Master/Client mode are permitted through the UI.**
(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized	**All relative parameters are limited when the device is calibrated and programmed and the factory.**
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	**All RF parameters are calibrated and programmed at the factory and cannot be modified by third party users. Adhesives and non-standard connectors are used in transmission path.**
c. What parameters are accessible or modifiable by the end-user?	**Frequency Hop Sequence, Binding code and Master/Client mode are permitted through the UI.**
(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	**All relative parameters are limited when the device is calibrated and programmed and the factory.**
(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	**All RF parameters are calibrated and programmed at the factory and cannot be modified by third party users. Adhesives and non-standard connectors are used in transmission path.**
d. Is the country code factory set? Can it be changed in the UI?	**Country code is programmed at the factory and no UI is provided for modification.**

(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	**Default is always FCC compliant, setup 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.	**The radio cannot be configured in a bridge or 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?	**Each mode uses the same bands.**
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 module is not an access point.**