The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within ASSY-1859ATMBA-00 U-NII Security.

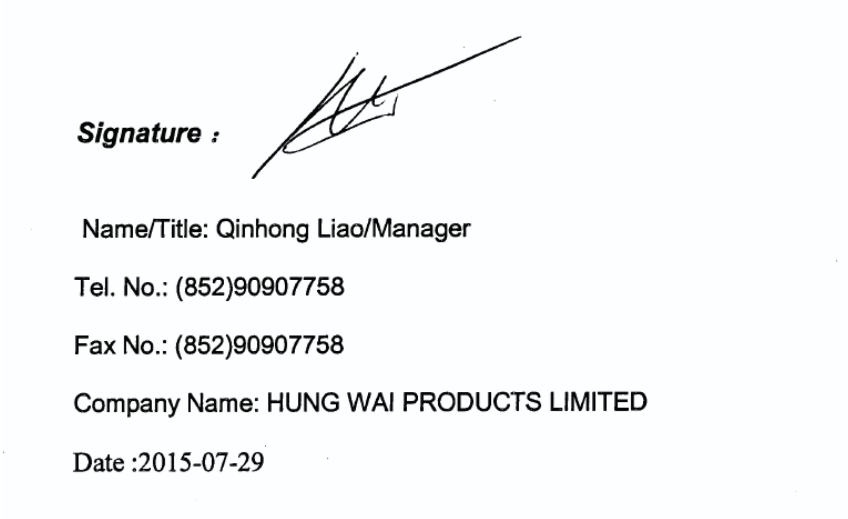
The information below describes how we maintain the overall security measures and systems so that only:

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

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.	User can download the new FW and the update tool from official WEB page.
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?	All the parameter limitations are hard-coded into special permanent memory space to not exceed the authorized limits. Professional installer has no access to change radio parameter limits.
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	Yes. Platform goes through a secure boot process every time it is powered. System verifies the root of trust to verify all the software components are signed with right set of keys
4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate	Yes, System Control Unit the software which runs first when the device boots up verifies all the software components are signed with the right keys. If the component is signed with a wrong key or altered, system will not boot.
5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	Header of each firmware component is encrypted with an RSA private key
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?	Since the software can work in both modes (Master and Client) software was developed to update limitations, during configuration, instantly to meet compliance in any operating mode. Only authorized operating bands are allowed to configure by the professional installer.
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	No prevention present today to load non-U.S. version of software/firmware on a U.S. version of the same device

installation of third-party firmware	
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	Certified transmitter modules have sufficient 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. 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.
SOFTWARE CONFIGURATION DESCRIPTION GUIDE ?USER CONFIGURATION GUIDE	
1. To whom is the UI accessible? (Professional installer, end user, other.)	Professional installer
a. What parameters are viewable to the professional installer/end-user?	"Settings" menus offered by Android OS and other Software Applications. It includes selection of available WiFi networks and related passwords.
b. What parameters are accessible or modifiable by the professional installer?	None
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Parameters for settings in "Settings" menu are controlled/ checked by Android OS and SW Apps
ii) What controls exist that the user can not operate the device outside its authorization in the U.S.?	WLAN driver follows IEEE 802.11d standard protocols, the country code settings are automatically configured according to the AP or Network.
c. What parameters are accessible or modifiable to by the end-user?	"Settings" menus offered by Android OS and other Software Applications. It includes selection of available WiFi networks and related passwords
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Parameters for settings in "Settings" menu are controlled/ checked by Android OS and SW Apps
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The end user has no access to parameter settings. The device automatically adjusts to the appropriate authorized bands for each country managed by the AP or Network infrastructure based on IEEE 802.11d standard protocols.
d. Is the country code factory set? Can it be changed in the UI?	The country code is set in the initial OS setup, once the user chooses the country of preference there is no way to change the country code settings unless the system is "reset to default factory settings". End users do not have any access to country code settings post initial setup. Access to these settings are non-existent to the user within the UI.
i). If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	WLAN driver follows IEEE 802.11d standard protocols, the country code settings are automatically configured according to the AP or Network

e. What are the default parameters when the device is restarted?	Default parameters are based on Android OS installed on the device
2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required.	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?	Device can be used as master in Bluetooth tethering, but this is not user configurable.
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.	External antenna type， gain， supplier， model no all have been listed in user manual， changes or modifications not expressly approved could void the user's authority to use the device



Signature：

Name/Title: Qinhong Liao/Manager

Tel. No.: (852)90907758

Fax No.: (852)90907758

Company Name: HUNG WAI PRODUCTS LIMITED

Date :2015-07-29