Software Security Declaration

FCC ID : PY317200378

SOFTWARE SECURITY DESCRIPTION		
General Description	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.	Software / firmware updates for the MR1100-320 mobile hotspot is available via an over-the-air update process through a FOTA server managed by AT&T. The update process is secure through unique username and password device combinations that are authenticated by the server via encrypted SSL connection.
	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?	Two Wi-Fi radio frequency parameters can be configured via the user interface: Wi-Fi Channel, Wi-Fi Channel Bandwidth. These parameters are limited to a pre-set list for the user to select from UI.
	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 update package is only available via a secure server, using SSL and username / password for authentication. This ensure the source of the software/firmware is legitimate.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	SSL / AES / TKIP /PKCS#1 /PKCS#7
	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?	The AC815S cannot be configured as Wi-Fi client, it only operates as an access point (master).

SOFTWARE SECURITY DESCRIPTION		
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.	It is impossible, because RF parameters, country of operation and other parameters related to device compliance are permanent settings in the NVRAM
	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. *Note : See*, for example, www.XXXXX.com/	The product firmware uses an NVRAM SKU value to check and validate any update package to ensure that it is applicable to the appropriate region. Furthermore, all parameters indicating different countries are permanent settings in the NVRAM. The software/firmware itself doesn't contain these parameters and so it will not be affected by version of software.
	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.	The product is a mobile hotspot, not a modular device.

	Note that Certified Transmitter Modules must have sufficient level of security to ensure that when integrated into a permissible host the device's RF parameters are not modified outside those approved in the grant of authorization. (See, KDB Publication 99639). This requirement includes any driver software related to RF output 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 SECURITY DESCRIPTION		
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.	User can view the following parameters: Wi-Fi Mode, Channel Bandwidth, Channel, SSID, Security Type. There is no different level of access.
	a. What parameters are viewable and configurable by different parties? *Note: The specific parameters of interest for this purpose are those that may impact the compliance of the device (which would be those parameters determining the RF output 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.*	User can view the following parameters: Wi-Fi Mode, Channel Bandwidth, Channel, SSID, Security Type. There is no different level of access
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	There is no professional installer for this type of product
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	There is no professional installer for this type of product
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	There is no professional installer for this type of product
	c. What parameters are accessible or modifiable by the end-user?	End user can modify the following parameters: Wi-Fi Mode, Channel Bandwidth, Channel, SSID, Security Type
	(1) What parameters are accessible or modifiable by the end-user?	End user can modify the following parameters: Wi-Fi Mode, Channel Bandwidth, Channel, SSID, Security Type
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	All parameters (RF, frequencies, etc.) indicating different countries are permanent settings within the NVRAM. If a device is a product for the US, it cannot be changed for another region.

	d. Is the country code factory set? Can it be changed in the UI?	The country code is factory set and cannot be changed by UI
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	The country code is factory set and cannot be changed by UI
	e. What are the default parameters when the device is restarted?	The parameters that the user last saved in the UI.

SOFTWARE SECURITY DESCRIPTION		
USER CONFIGURATION GUIDE	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.	Neither mesh nor bridge mode is supported on this device
	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 cannot be configured as a client, it operates only as a master / access point
	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))	The device cannot be configured to operate as a different type of access point. The internal PCB antennas are not user-accessible or user-serviceable. All applicable limits are permanent settings within NVRAM, as tested in compliance process