InnoComm Mobile Technology Corporation

3F, No. 6, Hsin Ann Rd., Hsinchu Science Park, Hsinchu, 300092, Taiwan

Software Security Declaration

FCC ID : **YAIWB15**

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.	All Software downloads are supplied and controlled by the host device manufacturer. Download is Implemented via a secure server.
	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?	Centre Frequencies of channels, channel bandwidth, modulations, active or passive scanning and transmit power levels are defined in software. Hardware specific configuration data is stored in non-volatile memory which limits frequency and transmit power levels to U.S. compliant values.
	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 software image is installed at time of manufacture of the module. The correct embedded software is verified and installed by the module manufacturer. The signature validation procedure in 4) below is used to validate the authenticity of the image using a public key or hash of the public key stored in the module's non-volatile memory.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	A hash on the firmware binary is computed at the CASS server using SHA256 hashing algorithm. The hash is then secured using the private key using RSA-PSS algorithm. The secured hash is downloaded from the host to the target along with the firmware binary. After firmware binary download from

		the host, the target uses the public key to decrypt the hash that is sent & computes the hash on the firmware binary & compares them for authentication. If the hash does not match the firmware binary is discarded from target memory.
	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?	Software limits operation to passive only and No Master modes (WiFi Direct, SoftAP, etc) in radar channels. This configuration cannot be changed by end user or installer.

InnoComm Mobile Technology Corporation

3F, No. 6, Hsin Ann Rd., Hsinchu Science Park, Hsinchu, 300092, Taiwan

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.	Country domain is set in non-volatile memory during manufacture. It's not possible for 3rd party to load drivers, no such interface.
	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.	Embedded software is protected via the measures explained in the previous section. Ex-factory setting is for US version, no control if a 3 party operate in other areas.
	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.	Modules are always installed in host systems in a factory by end integrators responsible for loading authorized software.

InnoComm Mobile Technology Corporation

3F, No. 6, Hsin Ann Rd., Hsinchu Science Park, Hsinchu, 300092, Taiwan

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.	End-user only.
	a. What parameters are viewable and configurable by different parties?	End user cannot see any RF parameters, other than frequency channel setting and RSSI.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	End user cannot access any RF parameters, other than frequency channel setting and RSSI. They can select frequency channel from authorized frequency channels list.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	End user cannot access any RF parameters, other than frequency channel setting and RSSI. They can select frequency channel from authorized frequency channels list.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The parameters of country, frequencies and etc. are permanent settings and cannot be configured.
	c. What parameters are accessible or modifiable by the end-user?	The end user can select frequency channel from authorized frequency channels list.
	(1) What parameters are accessible or modifiable by the end-user?	The End-user can select frequency channel from authorized frequency channels list.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	The parameters of country, frequencies and etc. are permanent settings and cannot be configured.
	d. Is the country code factory set? Can it be changed in the UI?	It is factory set and cannot be changed in the UI.
	(1) If it can be changed, what controls exist to ensure that the device can only	The parameters of country, frequencies and etc. are permanent settings and

	operate within its authorization in the U.S.?	cannot be configured.
	e. What are the default parameters when the device is restarted?	The parameters of country, frequencies and etc. are permanent settings and cannot be configured.

InnoComm Mobile Technology Corporation

3F, No. 6, Hsin Ann Rd., Hsinchu Science Park, Hsinchu, 300092, Taiwan

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.	Our device does not support mesh mode or bridge 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?	User can select our product feature and the product software controls working as master or client depending on it in 2.4G band & 2.4G channels. But in 5G Band & 5G channels don't support software controls working as master, only client mode in 5G band. All the functions are checked and ensured working complied with the regulation.
	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 does not support these modes/features.

Name / Title: **Bruno Tsai/Product Manager**

Signature: 

TEL: **886-3-5781868**

Fax: **886-3-5781187**

Email: **bruno.tsai@innocomm.com**