Software Security Declaration

Model: **TCLPICOPRO**

This device is fully compliant with the requirement of KDB 594280 D02 U-NII Device Security v01r01.

SOFTWARE SECURITY DESCRIPTION		
General Description	1. Describe how anysoftware/firmware update will be obtained, downloaded, and installed.	**Celluon introduce new SW that has secured sign through Celluon website. Celluon product can only download the code and install.**
	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 radio frequency parameters are Transmit power, operating channel, modulation type but those authorized parameters are fixed.**
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.	**Celluon SW in our product runs a validation during the SW upgrade process to ensure the SW's legitimate, unaltered, and downloaded correctly by proprietary load validation.**
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	**Celluon SW contains MD5 signature and contains platform type imbedded in header.**
	5. Describe, if any, encryption methods used.	**Celluon SWs are not encrypted but are compressed.**
	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?	**The device is only a slaver.**
Third Party Access Control	1. How are unauthorized software/ firmware changes prevented?	**The SW has secure signed code that only released by Celluon. Any changes check the secure signed code.**

SOFTWARE SECURITY DESCRIPTION		
Third Party Access Control	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.	**No, the products are not allow any changes by any user. It is a proprietary system. The memory maps, SW algorithms are not published.**
	3. 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	**This is locked into the manufacturing data and cannot be changed.**
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	**The configuration for US is located in secure area, so cannot be changed any loadings non-US versions of SW/ firmware.**
	5. For modular devices, describe how authentication is achieved when used with different hosts.	**This is not a modular device.**
User Configuration Guide	1. To whom is the UI accessible? (Professional installer, end user, other.)	**The UI is not accessible except Celluon.**
	a) What parameters are viewable to the professional installer/end-user?	**All parameters are hidden.**
	b) What parameters are accessible or modifiable to the professional installer?	**Not support parameters access and modify.**
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	**Not support parameters access and modify.**
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	**The radios are configured at manufacturing to be US only and the configuration cannot be changed by any SW update for the product.**
	c) What configuration options are available to the end-user?	**Not support any configuration option.**
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	**Not support parameters access and modify.**
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	**The radios are configured at manufacturing to be US only and the configuration cannot be changed by any SW update for the product.**
	d) Is the country code factory set? Can it be changed in the UI?	**Yes, the country code is factory set. It does not support the UI menu.**

SOFTWARE SECURITY DESCRIPTION		
User Configuration Guide	i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	**The radios are configured at manufacturing to be US only and the configuration cannot be changed by any SW update for the product.**
	e) What are the default parameters when the device is restarted?	**The product goes to a default(approved) Tx channel and power level based on factory country setting.**
	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.	**No, can't configure 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 to ensure compliance.	**The product is a slave only.**