## < SHENZHEN TENDA TECHNOLOGY CO.,LTD > <6-8 Floor, Tower E3, No. 1001, Zhongshanyuan Road, Nanshan District,</p> Shenzhen, China. 518052>

Federal Communication Commission Equipment Authorization Division, Application Processing Branch 7435 Oakland Mills Road Columbia, MD 21048

Date: <2021-10-12>

Attn: Office of Engineering and Technology

Subject: Attestation Letter regarding UNII devices

FCC ID: V7TA21

Software security questions and answers per KDB 594280 D02:

	Software security questions and answers per KDB 594280 D02:					
1	Software Security description – General Description					
1	Describe how any software/firmware updates for	Software/firmware will be obtained by the				
	elements than can affect the device's RF	factory, downloaded from the ODM website, and installed by the end user.				
	parameters will be obtained, downloaded,	·				
	validated and installed. For software that is	Software is accessed through Web UI				
	accessed through manufacturer's website or	when computer is connected.				
	device's management system, describe the					
	different levels of security as appropriate.					
2	Describe the RF parameters that are modified by	The RF parameters cannot be modified by				
	any software/firmware without any hardware	software.				
	changes. Are these parameters in some way	All these parameters will not exceed the				
	limited such that any other software/firmware	authorized parameters. The firmware has				
	changes will not allow the device to exceed the	been complied as binary file. It couldn't				
	authorized RF characteristics?	change the setting RF parameter through				
		this binary file. It is read-only without				
		change.				
3	Describe in detail the authentication protocols	No any authentication protocol is used.				
	that are in place to ensure that the source of the	The RF Parameters is put in read-only				
	RF-related software/firmware is valid. Describe	partition of EUT's flash and are only				
	in detail how the RF-related software is protected	installed in the factory. RF parameters				
	against modification.	including frequency of operation, power				
		setting, modulation type, antenna types or				
		country code setting will be locked in this				
		partition.				
4	Describe in detail any encryption methods used	No encryption methods used.				
	to support the use of legitimate RF-related					
	software/firmware.					
5	For a device that can be configured as a master	This device cannot be configured as a				
	and client (with active or passive scanning),	master and client.				

## < SHENZHEN TENDA TECHNOLOGY CO.,LTD > <6-8 Floor, Tower E3, No. 1001, Zhongshanyuan Road, Nanshan District,</p> Shenzhen, China. 518052>

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 Security description — Third-Party Access Control  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.  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.  For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these 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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are accessible or modifiable to the professional installers is one professional install device.  i. Are the parameters in some way		avalain have the device angunes compliance for							
master in some band of operation and client in another; how is compliance ensured in each band of operation?  Software Security description — Third-Party Access Control  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.  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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?		explain how the device ensures compliance for							
another; how is compliance ensured in each band of operation?  Software Security description — Third-Party Access Control  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.  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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?		1							
Software Security description — Third-Party Access Control    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.    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.    For Certified Transmitter modular devices, describe how 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.    Software Security description — USER CONFIGURATION GUID		1							
Software Security description — Third-Party Access Control  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.  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.  3 For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fally 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.  Software Security description — USER CONFIGURATION GUID  Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe how deconfigurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?		<u> </u>							
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.  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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professionalinstall device. This is not professionalinstall device.		-							
operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.  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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  The regulatory domain, frequencies, or in any manner that is in violation device's authorization for operate in violation device's authorization flegulation gratition of perate in violation device's authorization flegulation flegulation gratition of perate in violation device's authorization flegulation flegulation gratition of the device's authorization flegulation gratition of the device setting, manufacturers is put integrated in the U.S.  The RF Parameters is put in egal control of country code setting modulation flegulation flegulation flegulation flegulation flegulation f		Software Security description - Third-Party Access Control							
domain, frequencies, or in any manner that is in violation of the 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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  The RF Parameters is put in read-only partition of EUT's flash and are only installed evice.  This is not a modulation type, antennat types of country code setting will be locked in this partition.  This is not a module device.  This is not professional install device.	1		No any third parties have the capability to						
violation of the certification.  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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  The RF parameters is put in read-only partition of EUT's flash and are only partition of EUT's flash and are including frequency of operation, power setting, modulation the factory. RF parameters including frequency of operation, power setting, modulation the factory. RF parameters including frequency of operation, power setting, modulation the factory. RF parameters including frequency of operation, power setting, modulation the factory. RF parameters including frequency of operation, power setting, modulation the factory. RF parameters including frequency of operation installed in the factory. RF parameters including frequency of operation include viting partition.  This		operate a US sold device on any other regulatory	operate a US sold device on any other						
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  The RF Parameters is put in read-only partition of EUT's flash and are only installer only partition of EUT's flash and are only partition of EUT's flash and are only partition of country code setting will be locked in this partition.  The RF Parameters is put in read-only partition of EUT's flash and are only partition of EUT's flash and report of the device setting will be locked in this partition.  This is not a module device.  This is not professional install end vices, and the parameters are not partition.  The RF Parameters is put in read-only partition occurry code setting will be lo		domain, frequencies, or in any manner that is in	regulatory domain, frequencies, or in any						
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  The RF Parameters is put in read-only installed in the factory, RF parameters including frequency of operation, power setting, modulation type, antenna types of country code setting will be locked in this partition of EUT's flash and areonly installed in the factory, RF parameters setting, modulation type, antenna types of country code setting, modulation type, antenna typ		violation of the certification.	manner that may allow the device to						
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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  The RF Parameters is put in read-only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types of country code setting, modulation, partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation, partition of country code setting, modulation type, attenned to country code setting, modulation			operate in violation of the device's						
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.  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.  Software Security description — USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional installed vice. This is not professional install device. This is not professional install device.			authorization if activated in the U.S.						
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device. This is not professional install device. This is not professional install device.	2	Describe, if the device permits third-party	The RF Parameters is put in read-only						
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device. This is not professional install device.  This is not professional install device.  This is not professional install device.  This is not professional install device.		software or firmware installation, what	partition of EUT's flash and are only						
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device. This is not professional install device.  This is not professional install device.  This is not professional install device.  This is not professional install device.		mechanisms are provided by the manufacturer to	installed in the factory. RF parameters						
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?			including frequency of operation, power						
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  b. What parameters are accessible or modifiable to the professional installer?		1.							
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not a module device.		1							
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.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device. This is not professional install device.		1							
providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device. This is not professional install device.		1 *							
the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not a module device.									
unchanged and how the manufacturer verifies the functionality.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not a module device.									
functionality.  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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not a module device.									
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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.									
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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device. This is not professional install device.	3	·	This is not a module device						
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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.		· ·	mis is not a module device.						
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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.									
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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.		1							
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.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.  This is not professional install device.									
drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside the grant of authorization.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.									
modular transmitter RF parameters are not modified outside the grant of authorization.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.  This is not professional install device.		· ·							
modified outside the grant of authorization.  Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  There are no different levels of access.  Authorized channel, bandwidth, and modulation.  This is not professional install device.  This is not professional install device.  This is not professional install device.		_							
Software Security description – USER CONFIGURATION GUID  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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.  This is not professional install device.									
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.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  Authorized channel, bandwidth, and modulation.  Authorized channel, bandwidth, and modulation.  This is not professional install device.  This is not professional install device.			AUDICHE ATION CLIED						
through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  modulation can be configured through the UI.  There are no different levels of access.  Authorized channel, bandwidth, and modulation.  This is not professional install device.  This is not professional install device.	1	1							
permitted for professional installers, system integrators or end-users, describe the differences.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  UI.  There are no different levels of access.  Authorized channel, bandwidth, and modulation.  This is not professional install device.  This is not professional install device.									
integrators or end-users, describe the differences.  a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  There are no different levels of access.  Authorized channel, bandwidth, and modulation.  This is not professional install device.  This is not professional install device.									
a. What parameters are viewable and configurable by different parties?  b. What parameters are accessible or modifiable to the professional installer?  Authorized channel, bandwidth, and modulation.  This is not professional install device.  This is not professional install device.		1							
configurable by different parties? modulation.  b. What parameters are accessible or modifiable to the professional installer? This is not professional install device.  This is not professional install device.									
b. What parameters are accessible or modifiable to the professional installer?  This is not professional install device.  This is not professional install device.		<u> </u>							
to the professional installer?  This is not professional install device.		<u> </u>							
		1							
i. Are the parameters in some way		-	This is not professional install device.						
· · · · · · · · · · · · · · · · · · ·		i. Are the parameters in some way							

## < SHENZHEN TENDA TECHNOLOGY CO.,LTD > <6-8 Floor, Tower E3, No. 1001, Zhongshanyuan Road, Nanshan District, Shenzhen, China. 518052>

	ii. c. What of the end	limited, so that the installers will not enter parameters that exceed those authorized?  What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition.  Authorized channel, bandwidth, and modulation.
	i.	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those	This is not professional install device.  The RF Parameters is put in read-only partition of EUT's flash and are only
	ii.	authorized?  What controls exist that the user cannot operate the device outside its	installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this
	authorization in the U.S.?  d. Is the country code factory set? Can it be changed in the UI?		Yes, the country code is set by factory. It cannot be changed in the UI.
	i.	If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	The country code cannot be changed in the UI.
		are the default parameters when the is restarted?	The default RF parameters include frequency of operation, power setting, modulation type, country code(U.S.). For operation in the U.S, the default parameters of the device cannot be modified to operate outside its authorization.
]	mode? If y Further inf	dio be configured in bridge or mesh ves, an attestation may be required. Formation is available in KDB a 905462 D02.	No, this device cannot be configured in both bridge and mesh mode.
1	and client this is user exist, withi	that can be configured as a master (with active or passive scanning), if configurable, describe what controls in the UI, to ensure compliance for a. If the device acts as a master in some	This device cannot be configured as a master and client.

## < SHENZHEN TENDA TECHNOLOGY CO.,LTD > <6-8 Floor, Tower E3, No. 1001, Zhongshanyuan Road, Nanshan District,</p> Shenzhen, China. 518052>

	bands and client in others, how is this configured	
	to ensure compliance?	
4	For a device that can be configured as different	This device cannot be configured as
	types of access points, such as point-to-point or	different types of access points.
	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).	

Sincerely

Name:

Shen Yu

Company: SHENZHEN TENDA TECHNOLOGY CO.,LTD

Address: 6-8 Floor, Tower E3, No. 1001, Zhongshanyuan Road, Nanshan District,

Shenzhen, China. 518052

Phone: 86-755-27657098
Fax: 866-755-27657178
E-Mail: cert@tenda.cn