## **DTEN Inc.**

Federal Communications Commission Authorization and Evaluation Division 7435 Oakland Mills Rd. Columbia, MD

Date: 2018-10-31 FCC ID: 2AQ7Q-DB0355

U-NII Device Security Statement

To Whom	It May	Concern
---------	--------	---------

SOFTWARE SECURITY DESCRIPTION	
General Description	
1.Describe how any software/firmware update	Re: Only system software, it can be update by
will be obtained, downloaded, and installed.	"system upgrade" software. The level of
Software that is accessed through	security is middle.
manufacturer's website or device's	
management system, must describe the	
different levels of security.	
2.Describe the RF parameters that are	Re: For wireless, the manufacturers of
modified by any software/firmware without	wireless have inherent firmware which will not
any hardware changes. Are these parameters	be modified by the whole machine firmware or
in some way limited such that any other	software RF parameters.
software/firmware changes will not allow the	
device to exceed the authorized RF	
characteristics?	
3. Describe in detail the authentication	Re: The wireless is in accordance with WIFI
protocols that are in place to ensure that the	802.11 protocol. The RF parameters are in
source of the RF-related software/firmware is	the case of FCC regulations, the parameters
valid. Describe in detail how the RF-related	are internet in firmware provided by
software is protected against modification.	manufacturers, and the firmware will not be
	modified by the whole machine firmware or
	software.
4.Describe in detail any encryption methods	Re: wpa-psk TIKP, wps-psk AES, wep40,
used to support the use of legitimate	wep104
RF-related software/firmware.	
5.For a device that can be configured as a	Re: It is not working in DFS bands, and
master and client (with active or passive	compliance for related FCC rules.
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?Re: The system of device starts with secure boot which can prevents flashing system software. The device has disable adb and root1. 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.Re: The system of device starts with secure boot which can prevents flashing system software. The device has disable adb and root2. Describe, if the device permits third-party software or firmware installation, what manufacturer to permit integration of such functions while ensuring that the RF usita 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 veriffies the functionality.Re: The wireless is powered by whole machanged and how the module grantee ensures that host manufacturer fully comply with these software security requirements for U-NII devices. If the module is controlled managed such that the modular transmitter RF parameters are not modified outside the grant of authorization.7Re: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.		
compliance ensured in each band of operation?Re: The system of device starts with secure boot which can prevents flashing system software. The device has disable adb and root1. 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.Re: The system of device starts with secure boot which can prevents flashing system software. The device has disable adb and root2. 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 us 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.Re: The wireless is powered by whole machine, and only legal circumstances permit the installation.3. For Certified Transmitter modular devices, 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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	device acts as master in some band of	
operation?Re: The system of device starts with secure boot which can prevents flashing system software. The device has disable adb and root1. 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.Re: The system of device starts with secure boot which can prevents flashing system software. The device has disable adb and root2. 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 usta athorization 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.Re: The wireless is powered by whole machine, and the parameters of the wireless is powered by whole machine, and the parameters of the wireless is powered by whole machine, and the parameters of the wireless is powered by whole machine, and the parameters of the wireless is powered by whole machine, and the parameters of the wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.0. For Certified Transmitter modular devices, describe how the drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside theRe: The wireless is powered by whole machine, and the parameters of the wireless is powered by the firmware and the wireless module. There is no authority outside the use of. </td <td>operation and client in another; how is</td> <td></td>	operation and client in another; how is	
Third-Party Access Control1. 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.Re: The system of device starts with secure boot which can prevents flashing system software. The device has disable adb and root2. Describe, if the device permits third-party software or firmware installation, what 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.Re: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.3. For Certified Transmitter 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 theRe: The wireless is no authority outside the use of.	compliance ensured in each band of	
<ul> <li>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.</li> <li>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.</li> <li>3. For Certified Transmitter modular devices, 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</li> </ul>	operation?	
capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.boot which can prevents flashing system software. The device has disable adb and root2. 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 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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	Third-Party Access Control	
other regulatory domain, frequencies, or in any manner that is in violation of the certification.software. The device has disable adb and root2. 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 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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	1. Explain if any third parties have the	Re: The system of device starts with secure
any manner that is in violation of the certification.root2. 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 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 therootRe and signature, and the parameters of the wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	capability to operate a US sold device on any	boot which can prevents flashing system
certification.Re: The wireless is in accordance with WIFI2. Describe, if the device permits third-party software or firmware installation, whatRe: The wireless is in accordance with WIFIsoftware or firmware installation, what802.11 and protocol. The RF parameters are in the case of FCC regulations, the parameters are internet in firmware provided by manufacturers, and the firmware will not be modified by the whole machine firmware or software. Before installation of software and firmware, the system will check the certificate 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.Re: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.V.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 theRe: The wireless is no authority outside the wireless module. There is no authority outside the	other regulatory domain, frequencies, or in	software. The device has disable adb and
<ul> <li>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.</li> <li>3. For Certified Transmitter modular devices, 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</li> <li>Re: The wireless is in accordance with WIFI 802.11 and protocol. The RF parameters are in the case of FCC regulations, the parameters are in the case of FCC regulations, the parameters, and the firmware provided by manufacturers, and the firmware will not be modified by the whole machine firmware or software security requirements for U-NII devices. If the module is controlled and managed such that the modular transmitter RF parameters are not modified outside the</li> </ul>	any manner that is in violation of the	root
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.802.11 and protocol. The RF parameters are in the case of FCC regulations, the parameters are internet in firmware provided by manufacturers, and the firmware will not be modified by the whole machine firmware or software. Before installation of software and firmware, the system will check the certificate and signature, and only legal circumstances permit the installation.3. For Certified Transmitter modular devices, 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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	certification.	
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.in the case of FCC regulations, the parameters are internet in firmware provided by manufacturers, and the firmware will not be modified by the whole machine firmware or software. Before installation of software and firmware, the system will check the certificate and signature, and only legal circumstances permit the installation.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 theRe: The wireless is no authority outside the use of.	2. Describe, if the device permits third-party	Re: The wireless is in accordance with WIFI
<ul> <li>manufacturer to permit integration of such functions while ensuring that the RF</li> <li>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.</li> <li>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</li> </ul>	software or firmware installation, what	802.11 and protocol. The RF parameters are
functions while ensuring that the RFby manufacturers, and the firmware will notparameters of the device cannot be operatedbe modified by the whole machine firmware oroutside its authorization for operation in thebe modified by the whole machine firmware orU.S. In the description include what controlsand/or agreements are in place with providersof third-party functionality to ensure thedevices' underlying RF parameters areunchanged and how the manufacturer verifiespermit the installation.3. For Certified Transmitter modular devices,Re: The wireless is powered by wholedescribe how the module grantee ensuresmachine, and the parameters of the wirelessthat host manufacturers fully comply withare determined by the firmware and thethrough driver software loaded in the host,wireless module. There is no authority outsidethrough driver software loaded in the host,managed such that the modular transmitterRF parameters are not modified outside themath an an aged such that the modular transmitter	mechanisms are provided by the	in the case of FCC regulations, the
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.be modified by the whole machine firmware or software. Before installation of software and firmware, the system will check the certificate and signature, and only legal circumstances permit the installation.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 theRe: The wireless is no authority outside the use of.	manufacturer to permit integration of such	parameters are internet in firmware provided
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.software. Before installation of software and firmware, the system will check the certificate and signature, and only legal circumstances permit the installation.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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	functions while ensuring that the RF	by manufacturers, and the firmware will not
<ul> <li>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.</li> <li>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</li> </ul>	parameters of the device cannot be operated	be modified by the whole machine firmware or
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.and signature, and only legal circumstances permit the installation.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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	outside its authorization for operation in the	software. Before installation of software and
of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.permit the installation.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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	U.S. In the description include what controls	firmware, the system will check the certificate
devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.Re: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	and/or agreements are in place with providers	and signature, and only legal circumstances
unchanged and how the manufacturer verifies the functionality.Re: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	of third-party functionality to ensure the	permit the installation.
the functionality.Re: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.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 theRe: The wireless is powered by whole machine, and the parameters of the wireless are determined by the firmware and the wireless module. There is no authority outside the use of.	devices' underlying RF parameters are	
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	unchanged and how the manufacturer verifies	
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	the functionality.	
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	3. For Certified Transmitter modular devices,	Re: The wireless is powered by whole
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 thewireless module. There is no authority outside the use of.	describe how the module grantee ensures	machine, and the parameters of the wireless
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	that host manufacturers fully comply with	are determined by the firmware and the
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	these software security requirements for	wireless module. There is no authority outside
describe how the drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside the	U-NII devices. If the module is controlled	the use of.
managed such that the modular transmitter RF parameters are not modified outside the	through driver software loaded in the host,	
RF parameters are not modified outside the	describe how the drivers are controlled and	
	managed such that the modular transmitter	
grant of authorization.7	RF parameters are not modified outside the	
	grant of authorization.7	

SOFTWARE CONFIGURATION DESCRIPTION		
USER CONFIGURATION GUIDE		
1.Describe the user configurations permitted Re: end user		
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	Re: NONE	
configurable by different parties?		
b) What parameters are accessible or	Re: NONE	

modifiable by the professional installer or system integrators?       Re: YES         (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?       Re: YES         (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?       Re: The firmware is write in ROM. The end user cannot modify it.         (a) What parameters are accessible or modifiable to by the end-user?       Re: NONE         (b) What parameters are accessible or modifiable to by the end-user?       Re: The country code is fixed for US, and it cannot be changed in the UI.         (c) What are the default parameters when the device is restarted?       Re: All the parameters is fixed for US, whatever the device is restarted or not.         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.       Re: No         S. 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?       Re:No         4. For a device that can be configured as point-to-point or point-to-multipoint, and use 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		[]
(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?Re: YES(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?Re: The firmware is write in ROM. The end user cannot modify it.(2) What parameters are accessible or modifiable to by the end-user?Re: NONE(3) Is the country code factory set? Can it be changed in the UI?Re: The country code is fixed for US, and it cannot be changed in the UI.(a) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.(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.Re: No(3) For a device that can be configured 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?Re:No(4) For a device that can be configured 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. (SeeRe:No	modifiable by the professional installer or	
<ul> <li>so that the installers will not enter parameters that exceed those authorized?</li> <li>(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?</li> <li>c) What parameters are accessible or modifiable to by the end-user?</li> <li>d) Is the country code factory set? Can it be changed in the UI?</li> <li>e) What are the default parameters when the device is restarted?</li> <li>Re: The country code is fixed for US, and it cannot be changed in the UI.</li> <li>e) What are the default parameters when the device is restarted?</li> <li>Re: All the parameters is fixed for US, whatever the device is restarted or not.</li> <li>Re: No</li> <li>Re: No</li> <li>Re: No</li> <li>S. For a device that can be configured as a master and client (with active or passive scanning), if this is user configured 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?</li> <li>A. 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</li> </ul>	system integrators?	
that exceed those authorized?Re: The firmware is write in ROM. The end user cannot modify it.(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?Re: The firmware is write in ROM. The end user cannot modify it.c) What parameters are accessible or modifiable to by the end-user?Re: NONEd) Is the country code factory set? Can it be changed in the UI?Re: The country code is fixed for US, and it cannot be changed in the UI.e) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.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.Re: No3. 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 	(1) Are the parameters in some way limited,	Re: YES
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?Re: The firmware is write in ROM. The end user cannot modify it.(2) What parameters are accessible or modifiable to by the end-user?Re: NONE(3) Is the country code factory set? Can it be changed in the UI?Re: The country code is fixed for US, and it cannot be changed in the UI.(2) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.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.Re: No3. 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 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. (SeeRe:No	so that the installers will not enter parameters	
<ul> <li>user cannot modify it.</li> <li>user cannot modify it.</li> <li>the U.S.?</li> <li>c) What parameters are accessible or modifiable to by the end-user?</li> <li>d) Is the country code factory set? Can it be changed in the UI?</li> <li>e) What are the default parameters when the device is restarted?</li> <li>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.</li> <li>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 as a master in some bands and client in others, how is this configured as a 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</li> </ul>	that exceed those authorized?	
the U.S.?Re: NONEc) What parameters are accessible or modifiable to by the end-user?Re: NONEd) Is the country code factory set? Can it be changed in the UI?Re: The country code is fixed for US, and it cannot be changed in the UI.e) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.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.Re: No3. 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?Re:No4. For a device that can be configured as 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. (SeeRe:No	(2) What controls exist that the user cannot	Re: The firmware is write in ROM. The end
c) What parameters are accessible or modifiable to by the end-user?Re: NONEd) Is the country code factory set? Can it be changed in the UI?Re: The country code is fixed for US, and it cannot be changed in the UI.e) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.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.Re: No3. 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 as a fifterent 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. (SeeRe:NO	operate the device outside its authorization in	user cannot modify it.
modifiable to by the end-user?Re: The country code is fixed for US, and it cannot be changed in the UI?(d) Is the country code factory set? Can it be changed in the UI?Re: The country code is fixed for US, and it cannot be changed in the UI.(e) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.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.Re: No3. 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?Re:No4. 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. (SeeRe:No	the U.S.?	
d) Is the country code factory set? Can it be changed in the UI?Re: The country code is fixed for US, and it cannot be changed in the UI.e) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.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.Re: No3. For a device that can be configured as a master and client (with active or passive scanning), if this is user configured to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this 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. (SeeRe:No	c) What parameters are accessible or	Re: NONE
changed in the UI?cannot be changed in the UI.e) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.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.Re: No3. 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 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. (SeeRe:No	modifiable to by the end-user?	
e) What are the default parameters when the device is restarted?Re: All the parameters is fixed for US, whatever the device is restarted or not.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.Re: No3. 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 as a 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. (SeeRe:No	d) Is the country code factory set? Can it be	Re: The country code is fixed for US, and it
device is restarted?whatever the device is restarted or not.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.Re: No3. 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?Re:No4. 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. (SeeRe:No	changed in the UI?	cannot be changed in the UI.
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.Re: No3. 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 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. (SeeRe: No	e) What are the default parameters when the	Re: All the parameters is fixed for US,
mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.Re: No3. 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?Re: No4. 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. (SeeRe:No	device is restarted?	whatever the device is restarted or not.
required. Further information is available in KDB Publication 905462 D02. 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? 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	2. Can the radio be configured in bridge or	Re: No
KDB Publication 905462 D02.Re: No3. 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?Re: No4. 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. (SeeRe:No	mesh mode? If yes, an attestation may be	
<ul> <li>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?</li> <li>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</li> </ul>	required. Further information is available in	
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?Re:No4. 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 	KDB Publication 905462 D02.	
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? 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	3. For a device that can be configured as a	Re: No
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?Re:No4. 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. (SeeRe:No	master and client (with active or passive	
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?Action ensure compliance4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use 	scanning), if this is user configurable,	
device acts as a master in some bands and client in others, how is this configured to ensure compliance?Re:No4. 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. (SeeRe:No	describe what controls exist, within the UI, to	
client in others, how is this configured to ensure compliance? 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	ensure compliance for each mode. If the	
ensure compliance?Re:No4. 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	device acts as a master in some bands and	
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. (SeeRe:No	client in others, how is this configured to	
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	ensure compliance?	
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	4. For a device that can be configured as	Re:No
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	different types of access points, such as	
controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See	point-to-point or point-to-multipoint, and use	
applicable limits and the proper antenna is used for each mode of operation. (See	different types of antennas, describe what	
used for each mode of operation. (See	controls exist to ensure compliance with	
	applicable limits and the proper antenna is	
Section 15.407(a))	used for each mode of operation. (See	
. ,,	Section 15.407(a))	

Sincerely, Company: DTEN Inc.

Signature

No Ma

Typed name and Title: Na Ma and Manager