SOFTWARE SECURITY DESCRIPTION

An applicant must describe the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device; and
2. The device is not easily modified to operate with RF parameters outside of the authorization.

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements. While the Commission did not adopt any specific standards, it is suggested that the manufacturers may consider applying existing industry standards. Also, this guide is not intended to be exhaustive and may be modified in the future. There may be follow-up questions based on the responses provide by the applicant for authorization. The device complies with KDB 594280D01 and D02

SOFTWARE SECURITY DESCRIPTION	
General Description	1.Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate. Reply: Software upgrades are retrieved from the manufacturers WatchDocs account. The Manufacturer is Domo Tactical Communications Ltd. To access the WatchDocs system a login and password are required. These are issued to legitimate customers only. The product is mature now and there have been no software upgrades for the last 12 months. A login provides access to specific products only.
	2.Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics? Reply: To achieve FCC compliance the frequency range is limited by factory set-up to 5.73 – 5.84GHz. These factory set range is not influenced by software upgrade. The RF parameters controlled by the software include frequency, modulation type (64QAM, 16QAM and QPSK), attenuation of maximum power, bandwidth (8,7,6MHz) and Guard interval. Only frequency is limited to achieve FCC compliance.
	3.Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification. Reply:Software is inherently tied to the hardware architecture. Software contains a checksum check when downloaded.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. Reply: Compiled software is not encrypted, but is controlled by checksum
	5. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for eachmode? In particular if the device acts as master in some band of operationand client in another; how is compliance ensured in each band of operation? Reply: Not applicable
	1. Explain if any third parties have the capability to operate a U.S.-solddevice on any other regulatory domain, frequencies, or in any manner thatmay allow the device to operate in violation of the device's authorization ifactivated in the U.S. Reply: They do not have that capability, the frequency band is limited at the time of sale.

Third-Party Access Control	2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permitintegration of such functions while ensuring that the RF parameters of thedevice cannot be operated outside its authorization for operation in theU.S. In the description include what controls and/or agreements are inplace with providers of third-party functionality to ensure the devices'underlying RF parameters are unchanged and how the manufacturer verifies the functionality. Reply: The device does not allow third party software.
	3. For Certified Transmitter modular devices, describe how the module

	grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization. Reply: The unit is supplied at equipment level in the USA.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE

In addition to the general security consideration, for devices which have "User Interfaces" (UI) to configure the device in a manner that may impact the operational parameter, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE	
USER CONFIGURATION GUIDE	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences. Reply: RF User settings are Frequency (limited to within 5.73 to 5.84GHz, bandwidth (8,7,6MHz), attenuation (max output power = 100mW), Modulation (64QAM, 16QAM and QPSK) and guard interval. Only frequency range is limited to achieve FCC compliance.
	a) What parameters are viewable and configurable by different parties? Reply: All of the above
	b) What parameters are accessible or modifiable tothe professional installer? Reply: All of the above
	i. Are the parameters in some way limited, so thatthe installers will not enter parameters that exceed those authorized? Reply: Frequency range is limited to 5.73 to 5.84GHz at time of supply
	ii. What controls exist that the user cannot operatethe device outside its authorization in the U.S.? Reply: Hard frequency limits programmed into the software at time of supply
	c) What parameters are accessible or modifiable by the end-user? Reply: All of the above
	i. Are the parameters in some way limited, so thatthe installers will not enter parameters that exceed those authorized? Reply:
	ii. What controls exist that the user cannot operatethe device outside its authorization in the U.S.? Reply: Frequency range is limited to 5.73 to 5.84GHz at time of supply
	d) Is the country code factory set? Can it be changedin the UI? Reply: There is no country code as such just as frequency limit.
	i. If it can be changed, what controls exist to ensure that

	the device can only operate within its authorization in the U.S.? Reply: Not applicable
	e) What are the default parameters when the deviceis restarted? Reply: The device restarts in its previous settings
	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. Reply: No
	3. For a device that can be configured as a master andclient (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? Reply: Not Applicable
	4. For a device that can be configured as different typesof access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a)) Reply: Not Applicable