SOFTWARE SECURITY DESCRIPTION		
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	Firmware updates will be obtained from the manufacturer's support website by the professional installer. The professional installer will install firmware updates.
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?	Center Frequency and Channel Width can be modified in firmware without hardware changes. The radio includes a per unit unique, factory loaded firmware option key which dictates the operational frequency band. The radio firmware does not allow the operational channel to exceed the authorized frequency band limits (high/low frequency).
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.	An RSA digital signature is verified after the firmware has been transferred to the unit but before it has been saved to non-volatile memory. Only if the digital signature is valid is the firmware stored to non-volatile memory.
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	An RSA digital signature is verified after the firmware has been transferred to the unit but before it has been saved to non-volatile memory. Only if the digital signature is valid is the firmware stored to non-volatile memory.
	5. Describe, if any, encryption methods used.	Wireless: AES-128 and AES-256 HTTPS: SSLv2*, SSLv3* and TLS 1.0; RC2*, RC4*, DES*, 3DES, AES SSHv2: 3DES, AES SNMPv3: DES*, AES Secure, encrypted file transfer of the firmware is available via HTTPS * Disallowed in FIPS 140-2 compatible mode
	6. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?	Both master and client modes may be used regardless of the band of operation. The radio includes a per unit unique, factory loaded firmware option key which dictates the operational frequency band. The radio firmware does not allow the operational channel to exceed the authorized frequency band limits (high/low frequency).

Third-Party Access Control	1. How are unauthorized software/firmware changes prevented?	An RSA digital signature is verified after the firmware has been transferred to the unit but before it has been saved to non-volatile memory. Only if the digital signature is valid is the firmware stored to non-volatile memory.
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.	No, only firmware that has been digitally signed by the manufacturer can be loaded onto the device.
	3. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.	Models sold to commercial customers are frequency band limited via unit specific, factory-loaded firmware option keys. Models sold to military customers are not frequency band limited.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	There are no non-US firmware versions. Because an RSA digital signature is verified after the firmware has been transferred to the unit but before it has been saved to non-volatile memory and the firmware is stored to non-volatile memory only if the digital signature is valid, a third party cannot load a non-US firmware version.
	5. For modular devices, describe how authentication is achieved when used with different hosts.	Not a Module

SOFTWARE CONFIGURATION DESCRIPTION		
USER CONFIGURATION Guide	1. To whom is the UI accessible? (Professional installer, end user, other.)	Professional installer
	a) What parameters are viewable to the professional installer/end-user?	Professional installer: All parameters End user: No parameters
	b) What parameters are accessible or modifiable to the professional installer?	All parameters are modifiable by a professional installer.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Frequency and Channel Width limited such that the operational channel remains within the authorized frequency band.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The radio includes a per unit unique, factory loaded firmware option key which dictates the operational frequency band. The radio firmware does not allow the operational channel to exceed the authorized frequency band limits (high/low frequency).
	c) What configuration options are available to the end-user?	None
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	N/A, end user cannot modify configuration.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	N/A, end user cannot modify configuration.
	d) Is the country code factory set? Can it be changed in the UI?	N/A, this product does not make use of country codes.
	i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	N/A
	e) What are the default parameters when the device is restarted?	All parameters are retained after a restart.
	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.	The radio can be configured in bridge mode.
	3. For a device that can be configured as a master and client (with active or passive scanning),if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?	Both master and client modes may be used regardless of the band of operation. The radio includes a per unit unique, factory loaded firmware option key which dictates the operational frequency band. The radio firmware does not allow the operational channel to exceed the authorized frequency band limits (high/low frequency).
	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	Guidance is provided to the professional installer in the manual.

	limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))	