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.	Initial configuration firmware is loaded into the device at the manufacturer level through a secure network management system. Only Acuity Brands approved and released software may be accepted by the device through authentication protocols listed in Item #3.
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?	No hardware changes are permitted. Radio frequency parameters are locked into firmware release at the manufacturer's factory under device approved per FCC rules. The FM TX/Rx and Bluetooth functionality is turned off by firmware. Channel 12 and 13 are disabled by firmware.
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.	Device will only connect to an authenticated trusted server using TLS 1.2 protocol. Sensity self-signing certificate is trusted by implementation of PKI solution using RSA-2048 encryption.
4. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	Installed software/ firmware occurs through an authenticated trusted server using RSA-2048 encryption method. Radio parameters are loaded at time of manufacturer within the factory. Software is only released for distribution though a software release process internally controlled through Sensity Software design personnel. Only Acuity Brands staff administrators are allowed to release firmware packages, through authentication via user control methods.
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 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?	Device is identified as a 'client' per rules defined in 15.202. Device is not identified or operate as a 'master' in any normal operating parameters. Device is under control of a certified master and does not initiate a network.

THIRD PARTY ACCESS CONTROL	
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 device's authorization if activated in the U.S.	No. Acuity Brands does not authorize any third-party access to firmware/ software related to radio parameters set forth within the certification grant.
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.	Installed software/ firmware occurs through an authenticated trusted server using RSA-2048 encryption method. Unauthorized firmware/ software installation will require physical access and addition of hardware not shipped with device.
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 parameters are not modified outside the grant of authorization.	The manufacturer is not allowed to change any trace or any parts. The Gerber files will be provided to the manufacturer to be followed exactly. The only exception is adding or removing the GPS module.
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.	Device does not support UI. UI available to the end-user, via cloud-based control system, allows access to basic functionality and monitoring of device(s) while in service. End-user has no access to device core device security/ functionality settings established at the factory.
a. What parameters are viewable and configurable by different parties?	Professional Installer may have viewing rights to verify SSID/ PSK and other security configurations are set during device commissioning. End User will not have access as a Professional Installer.
b. What parameters are accessible or modifiable by the professional installer or system integrators?	Professional Installer has no access in modifying factory installed firmware/ software within FCC frequency domain regions.

(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Parameters are defined by firmware/ software conducted at time of manufacturer/ factory
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	All devices are shipped with firmware/ software configured for under FCC certification/ grant limits. Professional Installers and End Users do not have access or permission to change region or country codes.
c. What parameters are accessible or modifiable by the end-user?	None.
(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	N/A
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	N/A
(d)Is the country code factory set? Can it be changed in the UI?	Country code is set at the manufacturing factory to FCC limits defined within the device grant of approval. Country code cannot be set via Cloud-Based UI.
(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Country code is set at the manufacturing factory to FCC limits defined within the device grant of approval. Country code cannot be set via Cloud-Based UI.
(e)What are the default parameters when the device is restarted?	Firmware/ software set at the manufacturer factory is default during device reset condition.
2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.	No
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?	N/A Device cannot be configured as a Master and Client.
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 Section 15.407(a))	N/A