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.

Software Security Description

1. Describe how any software/firmware update will be obtained, downloaded and installed Description: The firmware can be updated via Astro Command Center – an application to adjust audio settings in the headset
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? Description: Frequency and channels can be changed by firmware. Only authorized wifi channels available. Cannot be changed by end user.
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 Description: 1. No authentication protocol. The proprietary nature of the file format hinders counterfeiting the firmware.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details Description: Basic proprietary validation protocol (checksum, data format check)
5. Describe, if any, encryption methods used Description: No.
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 Description: Cannot be reconfigured
7. How are unauthorized software/firmware changes prevented? Description: 1. Proprietary binary format for firmware

8. 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. Description: It is not possible
9. 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. Description: It is not possible
10. What prevents third parties from loading non-US versions of the software/firmware on the device? Description: There is no non-US version, same FW ships to all countries where the product is sold.
11. For modular devices, describe how authentication is achieved when used with different hosts. Description: It is not modular device.

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.

USER CONFIGURATION GUIDE

1. To whom is the UI accessible? (Professional installer, end user, other.)
a) What parameters are viewable to the professional installer/end-user?
Description:
The UI is available to any end-user but no RF parameters are available through the UI.

b) What parameters are accessible or modifiable to the professional installer?
Description:
None

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
Description:
There are no accessible parameters in the UI

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
Description:
There are no accessible parameters in the UI

c) What configuration options are available to the end-user?
Description:
There are no accessible parameters in the UI

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
Description:
There are no accessible parameters in the UI

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
Description:
There are no accessible parameters in the UI

d) Is the country code factory set? Can it be changed in the UI?
Description:
It is factory set and 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.?
Description:
FW is provided by binary file in a proprietary format.

e) What are the default parameters when the device is restarted?
Description:
Parameters cannot be changed, they are the same as set in the factory

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.
Description: 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? Description: Cannot be configured as 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)) Description: Only point-to-point mode, no any other modes for configuration.

How the product comply 15.407(c)

Description: WIFI chip support automatically discontinue transmission in case of either absence of information to transmit or operational failure, if the chip detect absence of information to transmit or operational failure, it will be automatically shut off.