May 25, 2017

Federal Communications Commission
Equipment Authorization Branch
7435 Oakland Mills Road
Columbia, MD 21046

Company name: Voyetra Turtle Beach, Inc.

FCC ID: XGB-TB3340 and XGB-TB3341

FCC Part 15 Certification

Product / Model No.: Stealth 600P RX & Stealth 600P TX

Software Security Questionnaire

General Description

1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.

   Once the Stealth 600P system, comprised of the Stealth 600P RX (Wireless Audio Headset, XGB-TB3340) and Stealth 600P TX (Wireless Audio Transmitter, XGB-TB3341) leave the factory, neither their software nor firmware can be altered or changed through any update in the field These types of configuration changes can only be done at the factory.

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?

   The operational radio frequency parameters, such as channel frequency and output power, of the Stealth 600P system, cannot be changed or modified through any software or firmware update. These parameters are hard-coded into the RX and TX devices at the factory and are set based on the grants provided by the FCC.

   The output power is well below the +30 dBm limit, typically around +0-6 dBm and the operating channels can only be on 1.0 MHz channels from 2403.35 – 2477.35 MHz band. The firmware does not allow for operation on any other frequency.

3. Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.

   There are no user accessible hardware connections or ports between the RF chipset and the flash memory. Only the factory installed firmware can run on the hardware once it gets loaded and tested at the factory.

4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.

    The hardware section of the device that controls the RF operation does not have the capability of receiving firmware or software updates. New software cannot be loaded into the device by the end-user. The RF parameters are tested and verified during the manufacturing process at the factory through special test-mode software. Once the unit passes these tests and is properly configured, the test mode software is disabled and only the application software that contains the proper operating parameters is allowed to run the system.

5. Describe in detail any encryption methods used to support the use of legitimate software/firmware

    There is no encryption methods used in this product. The software used to control the RF operating parameters is hardcoded into the design at the time of manufacture with the application and test mode software.

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?

    This configuration is not applicable to the Stealth 600P system. Since this is an audio gaming system, the Stealth 600P TX device primarily transfers the audio from the host gaming console over the air to the Stealth 600P RX device. There is a reverse path from the RX to the TX device but that is primarily for error correction and acknowledgement packets.

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 certification.

    No, this operation cannot happen with the Stealth 600P system because the parameters that would cause any type of violation are not available to the end user or any third party. These parameters are set at the factory and cannot be altered in the field.

2. What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.

    The RF IC has its own dedicated flash and cannot be updated by any software download. An end-user cannot access this from any connection or port and therefore cannot update the operating parameters. All updates of this type would require disassembly of the unit.

USER CONFIGURATION GUIDE

1) To whom is the UI accessible? (Professional installer, end user, other.)

    End-user, there are no professional installers required for this device

    a) What parameters are viewable to the professional installer/end-user?[9]

Gaming audio controls, such as bass, treble and volume settings are viewable to the end-user. The end-user does not have any access to frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings.

b) What parameters are accessible or modifiable by the professional installer?

None

    (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

    Not Applicable as these parameters are not available to the end-user.

    (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

    The Stealth 600P can only operate on 1.0 MHz channels from 2403.35 – 2477.35 MHz. These parameters are set at the factory and cannot be altered or updated in the field. In addition, the output power is set to a fixed value at the factory based on the FCC grant and cannot be altered.

c) What parameters are accessible or modifiable to by the end-user?

Gaming audio controls, such as bass, treble and volume settings are modifiable by the end-user.

    (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

    Not Applicable as these parameters are not available to the end-user

    (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

    The Stealth 600P can only operate on 1.0 MHz channels from 2403.35 – 2477.35 MHz. These parameters are set at the factory and cannot be altered or updated in the field. In addition, the output power is set to a fixed value at the factory based on the FCC grant and cannot be altered.

d) Is the country code factory set? Can it be changed in the UI?

The country code is factory set and cannot be changed in the UI.

    (1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

    Not Applicable as these parameters are not available to the end-user

e) What are the default parameters when the device is restarted?

The default parameters are what is set at 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.

No, not applicable

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?

This mode is not available and therefore not applicable

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)).

This mode is not available and therefore not applicable

Voyetra Turtle Beach, Inc. hereby attests that the answers listed above in regards to the Stealth 600P RX and Stealth 600P TX devices for the Software Security Questionnaire are true and accurate to the best of their knowledge.

Sincerely,

Signature:

Name: **Tim Blaney**   **Title:**   **Compliance Manager**

Company: **Voyetra Turtle Beach, Inc.**

Address: **100 Summit Lake Drive, Suite 100**

            Valhalla, New York 10595 USA