Safety and Productivity Solutions
9680 Old Bailes Road
Fort Mill, SC 29707 USA
www.honeywell.com www.honeywellaidc.com

Date: September 13, 2018

To whom it may concern,
The information provided in this document applies to the following Wireless Adapter Modules:

FCC ID: HD5-TAP1000-01
Models: TAP1010-01, TAP1020-01, TAP1030-01

Software Security Description – KDB 594280 D02v01r03 Section II

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 as appropriate.

There are no downloadable options for the User.
The firmware updates are provided by the manufacture in binary format and is not modifiable by the User.

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, it will not exceed the authorized RF characteristics?

The driver is controlled by the manufacture in binary format programmed for default mode which is always FCC compliant set for FCC US and is not modifiable by the User.

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

The firmware is custom configured at the factory for sale in North America. After configuration, the User will have no control to change any settings.

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

There are no encryption methods used, the firmware is controlled by the manufacture given in binary format and is not modifiable by the User.

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

Honeywell
THE POWER OF CONNECTED

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 is a client module only.

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.

Third parties do not have the capability to operate in any manner that is violation of the certification in the U.S.

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.

RF parameters are programmed by the manufacture/Honeywell, 3rd party software cannot run on our devices.

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.

The driver is controlled by the manufacture given in binary format and is not modifiable by the User.

Sincerely,

Michael Robinson
Michael.Robinson3@Honeywell.com
Supervisor Quality Engineer Sr
Honeywell International Inc
SPS (Safety and Productivity Solutions)
Office:+1 (315) 554 6387