Panasonic
ideas for life

RICHARD MULLEN
Group Manager

Product Safety and Compliance Division

May 15, 2012

ITP-12-F015

Channel Plan and Software operation info

FCC ID: ACJ9TGFZ-A12

Question	Reply
Q1. A Statement of Conformity for the Client in Non-Associated mode is required. The Form 731 application must include a Cover Letter Attachment stating that the client software and associated drivers will not initiate any transmission on DFS frequencies without initiation by a master. This includes restriction on transmissions for beacons and support for ad-hoc peer-to-peer modes.	We declare that the device does not have "Ad Hoc on non-US frequencies" and/or "on DFS frequencies" while applying for the product. Our software and associated drivers will not initiate any transmission on DFS frequencies. This includes transmissions for beacon ad-hoc peer-to-peer modes. Also, this model is client device without radar detection.
Q2. A channel/frequency plan for the device showing the channels that have active scanning or passive scanning. Active scanning is where the device can transmit a probe (beacon) and passive scanning is where the device can listen only without probes.	The radio supports 802.11d and will not transmit until a valid Master device is detected. The device doesn't do active scanning in the DFS frequencies. This behavior is controlled by software.
Q3. For client devices that have software configuration control to operate in different modes (active scanning in some and passive scanning in others) or in different bands (devices with multiple equipment classes or those that operate on non-DFS frequencies), or modular devices that configure the modes of operations through software; the applicant must provide in the application software and operations description that discuss how the software and / or hardware is implemented to ensure that proper operations modes	On DFS channels, the WLAN driver of the device is controlled by an AP at all times, except when in ad-hoc mode on US non-DFS channels. The device passively scans DFS frequencies as mentioned above until a master device is detected. As part of the DFS functionality in the WLAN driver, software is implemented to react to radar detection messages and move to a new channel. This functional control is not accessible to anyone under any condition. Furthermore, the firmware is protected – it

cannot be modified by an end user or an installer. Also, include an attestation that the device complies with the requirements for software configuration control as discussed in KDB # 594280.	cannot be changed or modified by end user; Therefore, the device complies with the requirements for software configuration control as discussed in KDB #594280. Consequently, we declare that our device doesn't do active scanning in the DFS frequencies.

Sincerely yours,

Richard Mullen

Richard Mullen
Group Manager
Product Safety & Compliance Division