105 Edgeview Drive, Suite 300
Broomfield, CO 80021
USA

+1 303 301 3200

business.gogoair.com

Date: 26 June 2015

American Certification Body
6731 Whittier Avenue Suite C110
McLean, VA 22101
USA

Gentlemen:

FCC ID: Y7A-P24486
IC: 10226A-P24486
Model: GVPU, Part Number P24486

Please be advised that the product is manufactured and labeled for worldwide use. For clarification, this means that the unit will not transmit on any channel that is not approved for use in the United States as well as member countries of the International Telecommunication Union. The product's configuration file will be programmed to operate at the factory to use WLAN functionality of the chipset only on these specific channels:

Channels 1 – 11, 2412-2462 MHz 802.11b mode
Channels 1 – 11, 2412-2462 MHz 802.11g mode
Channels 1 – 11, 2412-2462 MHz 802.11n mode (20 MHz channel)

Channels 12 and 13 are not utilized in this device and locked out at the factory. Ad-hoc and other peer to peer modes are disabled on these channels.

U-NII-1: Channels 36 – 48, 5180-5240 MHz 802.11a
U-NII-1: Channels 36 – 48, 5180-5240 MHz 802.11n 802.11n (20 MHz channel)
U-NII-3: Channels 149-165, 5745-5825 MHz 802.11a
U-NII-3: Channels 149-165, 5745-5825 MHz 802.11n (20 MHz channel)

Channels 52-140, 5260-5700 MHz are not utilized in this device and locked out at the factory. Ad-hoc and other peer to peer modes are disabled on these channels.

Kindly refer to the following page for response to questions outlined in FCC KDB 594280 D02.

The only configuration changes that can be made are selection of a different Wi-Fi channel (from the approved list of channels). The selection of a different channel is only done by approved personnel and the port is password protected. All systems will ship to customers set to a default channel in 802.11n mode.

The device drivers, approved channels, and RF characteristics when programmed into the configuration file will not be accessible and cannot be changed by the end user in accordance with FCC KDB 594280 D01 and D02.

Sincerely,

SOFTWARE SECURITY DESCRIPTION		Response
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	Software updates are only provided by the original equipment manufacturer via USB drive. These updates are managed by onboard software such that no user intervention is required or allowed in the upgrade process. Software upgrades are not available on any public website or file server.
	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?	All software upgrades affect application and platform software only. They do not affect firmware or configuration files that could modify the RF characterstics. The configuration files are set to not utilize channels 52-140 in the UNII-2 band.
	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.	Applications are signed with the same certificate key as the platform operating system. Only applications with this key will work. The OEM controls this key.
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	Our software upgrade manager ensures that only files with appropriate credentials and sequential version numbers are allowed to be installed on the system. It also verifieds the embedded checksum to ensure that the file has not been tampered with.
	5. Describe, if any, encryption methods used.	No encryption is used in the core software or software upgrade process.
	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?	Not applicable to this unit.
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented?	Firmware changes can only be made at build time. The source code is controlled by the OEM and only built in-house. No firmware changes affecting RF characterstics can be made by unauthorized personnel. Checksums are used to verify file uploads before processing a proposed update.
	2. 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.	Device drivers can be only loaded through a maintenance port on the unit. This port has username/password credentials on it to prevent unauthorized access.
	3. 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.	Gogo as the OEM does not allow any third parties to operate or modify the device contrary to its certification.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	Loading firmware to control RF characteristics requires root access and access to the maintenance port.
	5. For modular devices, describe how authentication is achieved when used with different hosts.	Not applicable to this unit.
SOFTWARE CONFIGURATION DESCRIPTION		
USER CONFIGURATION GUIDE	1. To whom is the UI accessible? (Professional installer, end user, other.)	User interface is accessible only to a professional installer (aircraft mechanic)
	a) What parameters are viewable to the professional installer/end-user?	Turning WiFi On and Off is viewable by installer
	b) What parameters are accessible or modifiable to the professional installer?	Turning WiFi On and Off is viewable by installer
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	No parameters are viewable or settable that could exceed those authorized.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	No parameters are viewable or settable that could exceed those authorized.
	c) What configuration options are available to the end-user?	No configuration options are available to the end-user that affect the RF characteristics of the unit.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	No configuration options are viewable or settable that could exceed those authorized.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	No configuration options are viewable or settable that could exceed those authorized.
	d) Is the country code factory set? Can it be changed in the UI?	Country code is factory set. It cannot be changed in the user interface.
	i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Not applicable to this unit.
	e) What are the default parameters when the device is restarted?	The unit defaults to worldwide frequency availability to ensure it operates withn its intended function.
	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.	Not applicable to this unit.
	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	Not applicable to this unit.
	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	Not applicable to this unit.