Software security for UNII Devices

Lucid USA, Inc.

7373 Gateway Blvd, Newark, CA 94560, USA

To Whom It May Concern:

Product/Model/HVIN: (Unified Cockpit Controller) UCC / P21-K2C000

FCC ID: 2AXZJ-K2B100

IC: 27970-K2B100

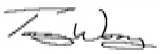
SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES acc. to KDB 594280

SOFTWARE CONFIGURATION DESCRIPTION	
General Description	
1	Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate. We do not release firmware on our website for downloading. Software is only updated when sent to device as an over the air update that is prepared by Lucid and initiated by Lucid.
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 any other software/firmware changes will not allow the device to exceed the authorized RF characteristics? Radio frequency parameters are limited by US regulatory domain and country code to limit frequency and transmit power levels. These limits are stored in non-volatile memory at the time of production. They will not exceed the authorized values.
3	Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification. The firmware is installed on each single module during the manufacturing process. The correct firmware is verified and installed by the manufacturer. In addition, the firmware binary is encrypted and the firmware updates can only be stored in non-volatile memory when the firmware is authenticated.

4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. The firmware is only available via an over the air update from Lucid. The firmware is binary encrypted. The process to flash a new firmware also requires a second secret key to enable flashing.
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 if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation? There is a country code regulatory parameter to limit product to operate the device under its authorization in the U.S. This regulatory parameter would define which channel would be available to operate in active or passive scan to meet UNII requirements. The device is not use as a master and client at the same time. No end user controls or user interface operation to change master/client operation.
Third-Party Access Control	
1	Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S. No, third parties don't have the capability to access and change radio parameters. US sold units are factory configured to US.
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. No. The device does not permit third-party software or firmware installation.
3	For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers 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 RF parameters are not modified outside the grant of authorization. Not Applicable. This device does not permit third party installation.
	SOFTWARE CONFIGURATION DESCRIPTION
USER CONFIGURATION GUIDE	

1	Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences. The product does not allow professional installers, system integrator or end users to change configuration.
1.a	What parameters are viewable and configurable by different parties? None. All default parameters are programmed or in both driver and firmware which would be embedded in system firmware. The system firmware is programmed and protected in flash memory.
1.b	What parameters are accessible or modifiable by the professional installer or system integrators? None. There is not any Wi-Fi parameter which is accessible or modifiable to the professional installer.
1.b(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? This device is programmed at factory production line. The end user or installers are not able to enter any parameters.
1.b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.? This device is programmed at factory production line. The end user cannot change the antenna gain and country code.
1.c	What parameters are accessible or modifiable by the end-user? The end user cannot change the antenna gain and country code, those settings are programmed at factory production time.
1.c(1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? Yes. The system firmware is programmed and protected in flash memory. The end-user or installers cannot access the flash memory.
1.c(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.? There is a country code regulatory parameter to limit product to operate the device outside its authorization in the U.S. No parameters are accessible or modifiable by end-users or installers.
1.d	Is the country code factory set? Can it be changed in the UI? The country code is factory set and is never changed by UI.
1.d(1)	If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

	Not Applicable. Cannot be change by end-user or installers. The country code is factory set and is never changed by UI
1.e	What are the default parameters when the device is restarted? The default parameters are what was configured when the product was manufactured. There are no controls that allow an end-user or installer to change the parameters.
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. Device does not utilize bridge or mesh mode.
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? The device does not operate as a master or client at the same time. Only client mode.
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)) The device does not support these modes/features



Name: Tommy Wong

Title: Technical Specialist, EMC Compliance Engineer

Lucid USA, Inc.

7373 Gateway Blvd, Newark, CA 94560, USA

(650) 802-8181