SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

REF KDB 594280 D02 U-NII Device Security v01r03

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. AN: When the product leaves the factory, the RF parameters have been written to the fixed parameter area of the Flash, which is not affected by the software upgrade; if the product firmware is updated, it can only be upgraded via OTA, and no local firmware upgrade interface is provided;
	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 nay other software/firmware changes will not allow the device to exceed the authorized RF characteristics? AN: 1、All the radio frequency parameters are completed and fixed in the process of production. Once leave factory, you can’t change it. 2、The device only supports OTA upgrade and does not provide any form of local upgrade interface.
	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. AN: The BOOT and firmware of this device use a private encryption/decryption and use verification mechanism. Any modification of the firmware by a third party will cause the system to fail to start.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. AN: One original driver and the original driver is encrypted.
	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? AN: The device is master with active scanning, the operation frequency are 5150-5250MHz, 5725-5850MHz.

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. AN: Any third parties don't have the capability.
	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. AN: The device does not support the installation of third-party software and firmware.
	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 RF parameters are not modified outside the grant of authorization.7 AN: This device does not have a "User Interface" (UI) and only supports APP configuration;

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. AN: This device does not have a "User Interface" (UI) and only supports APP configuration;
	a) What parameters are viewable and configurable by different parties? AN: The customer cannot configure any parameters.e
	b) What parameters are accessible or modifiable by the professional installer or system integrators? AN: The customer cannot configure any parameters.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? AN: The installation interface does not display other parameters.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? AN: The customer cannot configure any parameters.
	C) What parameters are accessible or modifiable to by the end-user? AN: The customer cannot configure any parameters.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? AN: The installation interface does not display other parameters.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? AN: The installation interface does not display other parameters.
	a) Is the country code factory set? Can it be changed in the UI? AN: Country code is set in factory stage, it cannot be changed.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	b) What are the default parameters when the device is restarted? AN: Wireless network name, wireless security and wireless network password are the default.
	1. 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. AN: Cannot.
	2. 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? AN: The device cannot be configured as a client.
	3. 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)) AN: Device cannot be configured as different types of access points.

Company name: AUO Display Plus Corporation

FCC ID:2A639-P1000-R

Name:CL. Chang

Title: Principal Engineer

Signature of applicant: Clchang **Date:** 2023.6.29