

**Neusoft Group (Dalian) Co., Ltd.**  
**No. 901-7 Huangpu Road, Ganjingzi District, Dalian City, Liaoning Province,**  
**China**

## **FCC Software Configuration Control Declaration**

Date: August 8, 2025

Federal Communications Commission  
7435 Oakland Mills Road  
Columbia, MD 21046  
USA

Attn: OET Dept.

**Product/ Model Number:** cockpit domain controller/CUSP000D00  
**FCC ID:** 2AZAXC4SP000D00

Regarding FCC Country Code Selection guidelines identified in KDB 594280 D01.

“All applications for equipment authorization for transmitters that can have radio parameters, or other technical parameters, reported to the Commission set by software must have an attestation indicating that no third party will have software, or configuration control, to program the device out of compliance of the technical rules under which it has been certified.”

We declare that no third party will have software, or configuration control, to program the device out of compliance of the technical rules under which it has been certified.

Signature: 

Name: sheng wang

Title: Quality Manager

Company: Neusoft Group (Dalian) Co., Ltd.

Address: No. 901-7 Huangpu Road, Ganjingzi District, Dalian City, Liaoning Province, China

Date: 2025.8.8

**Neusoft Group (Dalian) Co., Ltd.**

**No. 901-7 Huangpu Road, Ganjingzi District, Dalian City, Liaoning Province,  
China**

**Software security questions and answers per KDB 594280 D02:**

**Product/ Model Number:** cockpit domain controller/ C4SP000D00

**FCC ID:** 2AZAXC4SP000D00

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 that 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 the firmware on our website for downloading. Our direct host manufacturer (OEM) can request the firmware from us and it will be made available via secure server.
	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 by the module manufacturer 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 manufacturing process. The correct firmware is verified and installed by the module manufacturer. In addition, 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.	Only firmware with a special signature can be programmed to the non-volatile memory.
	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?	The default mode is master. Client mode can only be enabled by running special commands on CLI at test mode. So technically only master is supported.

**Neusoft Group (Dalian) Co., Ltd.**

**No. 901-7 Huangpu Road, Ganjingzi District, Dalian City, Liaoning Province,  
China**

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 modules 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.	The device does not allow the installation of third-party software involving RF control, and the hardware does not have interface driver support for RF
	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 module is not available for sale or installation outside of company licensing agreements. Modules are always installed in host systems in a factory by end integrators (OEM) responsible for loading authorized software.

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 UI is accessible to anyone who knows credentials..
	a) What parameters are viewable and	Various device status information is made available

**Neusoft Group (Dalian) Co., Ltd.**

**No. 901-7 Huangpu Road, Ganjingzi District, Dalian City, Liaoning Province,  
China**

	configurable by different parties?	like log information, connection status, operation mode, operation frequency, etc.  Radio parameters are described in c.i
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	This device is not subject to professional installation
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	This device is not subject to professional installation
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	This device is not subject to professional installation
	c) What parameters are accessible or modifiable to by the end-user?	The end user is able to configure the operation frequency,
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	modulation, reduce the output power levels etc. The end user cannot change the antenna gain, those settings are programmed at factory production time.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Yes, the parameters can only be changed within the limits of country code US.
	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) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	The country code is factory set and is never changed by UI
	e) What are the default parameters when the device is restarted?	At each boot up the country code and the antenna gain are read from the non-volatile memory, those values are configured during module production.
	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 supported
	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?	Not supported

**Neusoft Group (Dalian) Co., Ltd.**  
**No. 901-7 Huangpu Road, Ganjingzi District, Dalian City, Liaoning Province,**  
**China**

	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.
--	---	---

Signature: 

Name: sheng wang

Title: Quality Manager

Company: Neusoft Group (Dalian) Co., Ltd.

Address: No. 901-7 Huangpu Road, Ganjingzi District, Dalian City, Liaoning Province, China

Date: 2025.8.8