Date: 2021.11.09

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES
(594280 D02 U-NII Device Security v01r03, 11/12/2015)

FCC ID: 2AZTCMOTH
Product Name: Infrared Thermal Camera
Model No.: FOTRIC 326M and derived model

SOFTWARE SECURITY DESCRIPTION
General Description

Q.	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.
A.	The user or installer cannot modify the software/firmware context. FW version will only be deployed over the air. The cloud platform can push a new firmware version to the device when it is available.
Q.	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?
A.	Wi-Fi channel area code ID is only set in factory, all RF parameters (include Frequency range, transmitter output power etc.) cannot be access by the user.
Q.	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.
A.	The firmware is programmed at the factory and cannot be modified by third parties.
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	The firmware is programmed at the factory and cannot be modified by third parties therefore no encryption is necessary.
Q.	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?
A.	This is a client device only.

	Third-Party Access Control
Q.	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.
A.	No, third party have no capability to operate.
Q.	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.
A.	Installation of third-party software or firmware is not permitted.
Q.	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.
A.	Not applicable.

	SOFTWARE CONFIGURATION DESCRIPTION
	USER- CONFIGURATION GUIDE
Q.	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.
A.	No UI provided
Q	a. What parameters are viewable and configurable by different parties?[9]
A	None
Q	b. What parameters are accessible or modifiable by the professional installer or system integrators?
A	None
Q	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
A	Yes
Q	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
A	Firmware does not provide any interface to user to operate outside its authorization.
Q	c. What parameters are accessible or modifiable by the end-user?
A	None.
Q	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?

A	Yes
Q	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
A	Firmware does not provide any interface to user to operate outside its authorization
Q	d. Is the country code factory set? Can it be changed in the UI?
A	Yes. No
Q	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
A	Not applicable
Q	e. What are the default parameters when the device is restarted?
A	Same as factory set.
Q.	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.
A.	No
Q.	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?
A.	This is a client device only
Q.	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.
A.	Only point-to-point type

Signature Qiuxiang He

Company: FOTRIC INC.
Address: No. 14, Lane 2500, Xiupu Road, Pudong District, Shanghai, PRC
Name: Qiuxiang He
Title: Manager