U-NII Device Security

for

RF-7800W-OUxxx
Broadband Ethernet Radio

THIS INFORMATION IS EAR CONTROLLED
THIS INFORMATION IS CONTROLLED BY THE U.S. DEPARTMENT OF COMMERCE EXPORT ADMINISTRATION REGULATIONS 15 CFR 730-774, ECCN EAR99. EXPORT OR DISCLOSURE TO FOREIGN PERSONS MAY VIOLATE U.S. FEDERAL REGULATIONS

Harris Corporation
Communication Systems Division
1680 University Avenue
Rochester, NY 14610
USA

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.	Firmware updates will be obtained from the manufacturer's support website by the professional installer. The professional installer will install firmware updates. An RSA digital signature is verified after the firmware has been transferred to the radio but before it has been saved to non-volatile memory. Only if the digital signature is valid is the firmware stored to non-volatile memory. The support website is protected by HTTPS (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS 1.2). Access to the support website is using a username and password. User accounts for the support website are granted only after a customer has been vetted by the manufacturer's security department.
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?	Center Frequency, Channel Width, Transmit Power, and Dynamic Frequency Selection can be modified in firmware without hardware changes. The radio includes a per unit unique, factory loaded firmware option key which dictates the operational frequency band. The radio firmware does not allow the operational channel to exceed the authorized frequency band limits (high/low frequency). Configuration parameters can only be modified by the professional installer.
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 RSA digital signature is verified after the firmware has been transferred to the unit but before it has been saved to non-volatile memory. Only if the digital signature is valid is the firmware stored to non-volatile memory. The radio checks the integrity of the firmware using a 16-bit error detection code (EDC). A CRC-16 is used to verify that the image has not been modified. At power-up the module computes a new digest and compares it to a pre-computed digest value. If the values are the same the test passes. Otherwise, the test fails.
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Wireless: AES-128 and AES-256 HTTPS: SSLv2*, SSLv3* and TLS 1.0; RC2*, RC4*, DES*, 3DES, AES SSHv2: 3DES, AES SNMPv3: DES*, AES Secure, encrypted file transfer of the firmware is available via HTTPS or SFTP * Disallowed in FIPS 140-2 compatible mode
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?	Both master and client modes may be used regardless of the band of operation. The radio includes a per unit unique, factory loaded firmware option key which dictates the operational frequency band. The radio firmware does not allow the operational channel to exceed the authorized frequency band limits (high/low frequency).

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.	Models sold to commercial customers are frequency band limited via unit specific, factory-loaded firmware option keys. Models sold to military customers are not frequency band limited.
2. Describe, if the device permits third-party software or firmwareinstallation, 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 third-party software or firmware is permitted.
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, the radio is not a module.

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.	Only professional installers have access to configuration parameters. End users may have access to read-only statistics.
a. What parameters are viewable and configurable by different parties?	Professional installer: All parameters End user: No parameters
b. What parameters are accessible or modifiable by the professional installer or system integrators?	All parameters are modifiable by a professional installer.
(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Frequency and Channel Width limited such that the operational channel remains within the authorized frequency band.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The radio includes a per unit unique, factory loaded firmware option key which dictates the operational frequency band. The radio firmware does not allow the operational channel to exceed the authorized frequency band limits (high/low frequency).
c. What parameters are accessible or modifiable by the end-user?	No configuration options are available to the end user.
(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	No, guidance is provided to the professional installer in the manual.
(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	N/A, end user cannot modify configuration.
d. Is the country code factory set? Can it be changed in the UI?	N/A, this product does not make use of country codes.
(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	N/A
e. What are the default parameters when the device is restarted?	All parameters are retained after a restart.
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.	The radio can be configured in bridge 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?	Both master and client modes may be used regardless of the band of operation. The radio includes a per unit unique, factory loaded firmware option key which dictates the operational frequency band. The radio firmware does not allow the operational channel to exceed the authorized frequency band limits (high/low frequency). Guidance is provided to the professional installer in the manual.
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))	Guidance is provided to the professional installer in the manual.