1 Software Security Description	
1.1 General Description	**Alcatel-Lucent Answers**
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.	Software is obtained only from the manufacturer's website after proper authentication and authorization of the customer account. The user is required to have administrator-level privileges in order to activate the new software on the device.
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?	1. TX Power 2. Modulation 3. Channel bandwidth 4. TX/RX RF frequency The hardware supports parameter settings that could exceed the authorized RF characteristics but the setting ranges are limited by the authorized software.
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.	All software is provided with MD5 checksums to validate the integrity.
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Software is provided by the manufacturer in compressed, compiled object form.
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?	N/A, Master/client operation is not supported

1.2 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.	Device is generally sold only to service providers, where equipment access is well controlled.. Operation outside of the certification limits is restricted through software as described in 2.1.1.b.1).
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.	Use of third-party software is not supported. Software is supplied by the manufacturer only in compiled object form. Source code is not publicly available.
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.	NA