U-NII Device Security and Software Configuration Control

October 22, 2014

U-NII Device Security KDB Pub 594280 D02

- ET Docket No. 13-49 added security requirements for **ALL** U-NII devices (master and client)
  - Only authenticated software loaded and operating on device
  - Not easily modified to operate with RF parameters outside of the authorization
- KDB 594280 D02 U-NII Device Security - applies ONLY to devices seeking certification under new rules (June 2, 2014)
  - All questions must be answered and descriptions must be provided. If a specific question does not apply, explain why.

U-NII Device Security (cont.)

- Software Security Description
  - General Description – Software update, authentication, verification, encryption
  - Third-Party Access Control – Capabilities of third-parties
- Software Configuration Description
  - User Configuration Guide – Capabilities of end- users, professional installers, or others; different configuration modes.
- Software Security document must be in the operational description or software exhibit, preferably as a separate document (See ft. 3)

U-NII Device Security (cont.)

- U-NII SDR Devices
  - Must address selected security questions in KDB 594280 D02, in addition to questions in KDB 442812.

Software Configuration Control KDB Pub 594280 D01

- Client Device Operations Control
  - Transmissions of the device are under control of the master. Is not able to initiate a network. **§15.202**
  - If a master stops transmitting beacons or is no longer active, client must stop transmitting; may require use of a timer to detect absence of master beacons
- Peer-to-Peer / Ad Hoc Communications
  - Connection initiated without network master
    - Such devices generally must be approved as master device with DFS capability in the U-NII-2A and U-NII-2C bands, *unless*

Software Configuration Control

- "Listen-only" clients protocol (PBA)
  - Both parties must listen to the same access point
  - At least one is fully associated with the master
  - A timer or other mechanism to determine if the master is no longer "active"
- WiFi Client Devices on Ch.12 and 13
  - In US, max transmit adjusted to comply with OBE
  - Effective January 1, 2015, new authorizations must comply with guidance in 594280 D01
  - Passive Scanning alone is not sufficient (a client that does not "initiate a network" as defined in Section 15.202) to meet US requirement

Software Configuration Control

- Default mode must be a compliant in US mode
- Must use supplement information i.e. geo-location, to determine operation outside US

– Geo-location data
  - GNSS sensors in device
  - MCC, or MCC with MNC
  - Country data derived from multiple APs (PBA)
  - IP addresses or other reliable source (PBA)
  - Device must recheck geo-location data at least once per hour

Software Configuration Control

- Authorizations must include
  - Detailed operational description
  - Verification and validation of geo-location procedure
- Rules apply to US and all territories