FCC NPRM: State Opt-Out Requests

APPENDIX B

**Opt-out Technical Interoperability Requirements Based on the Board Document**

The requirements in this appendix are based on the Board document “Recommended Requirements” (“SHALLs”). Requirements attributable to the NPSBN or FirstNet shall be deemed for these purposes to refer to the applicable state RAN. The numbering is based on the original Board document numbering.

[1] Hardware and software systems comprising the NPSBN SHALL implement interfaces consistent with Table 2: Standards Implementation Methodology.

[2] Hardware and software systems comprising the NPSBN SHALL support the interfaces enumerated in Table 1: Minimum Interoperable Interfaces.

[3] Hardware and software systems comprising the NPSBN SHALL support management functions.

[7] The NPSBN SHALL support IPv4, IPv6, and IPv4/v6 PDN types defined in 3GPP TS 23.401.

[8] The NPSBN SHALL support IPv4 and/or IPv6 transport for the EPS interfaces enumerated in Table 1: Minimum Interoperable Interfaces, consistent with the FirstNet design.

[9] Any sharing agreement that FirstNet enters into SHALL implement network sharing according to 3GPP TS 23.251 and SHALL NOT impact public safety operations.

[10] The NPSBN SHALL include the capability to collect and convey UE location data to applications using a standardized interface in near real time.

 [20] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet required Interface Conformance Testing (e.g. testing S1-MME conformance to 3GPP) on the interfaces specified by FirstNet.

[21] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet required Interoperability Testing at a system level as per the specific IOT requirements for the NPSBN.

[22] Infrastructure deployed on the NPSBN SHALL be included in the FirstNet-required FOA process as part of the NPSBN deployment.

[23] The equipment comprising the NPSBN SHALL provide backwards compatibility of interfaces, from time of deprecation, for a minimum of two full major release/upgrades of the network. This requirement may be waived (i.e., interface obsolescence accelerated) if FirstNet can ascertain from the user community that there are no dependencies on a given interface.

[24] The NPSBN SHALL support user mobility across the entire NPSBN (including Opt-out states).

[25] The NPSBN SHALL support S1 and SHALL preferentially support X2 handover between adjacent NPSBN cells (including cells owned by opt-out states) whose proximity supports a handover opportunity.

[29] The NPSBN SHALL support the use of mobile VPN technology to support mobility between the NPSBN and other networks.

[30] The NPSBN SHALL provide the ability for national, regional, and local applications to dynamically change a UE‘s prioritization and QoS using the 3GPP ‗Rx‘ interface.

[31] The NPSBN SHALL support all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.

[32] QoS mechanisms in the NPSBN SHALL comply with 3GPP TS 23.203.

[33] The NPSBN SHALL support the usage of all 15 ARP values defined in 3GPP 23.203.

[34] The NPSBN SHALL support the ARP pre-emption capability and vulnerability functions as defined in 3GPP 23.203.

[35] The NPSBN SHALL implement a nationwide scheme for assigning Access Classes to public safety users and secondary users following the 3GPP recommendations in TS 22.011, Section 4.2.

[36] The NPSBN SHALL implement a nationwide scheme for assigning QoS Class Identifier priority to IP network and backhaul priority across the entire NPSBN.

[37] The NPSBN SHALL support the use of industry standard VPN and MVPN technology, while providing priority and Quality of Service for encapsulated applications.

[38] The NPSBN SHALL use a nationwide common security profile for user plane and control plane traffic between UEs, eNBs and MMEs, in accordance with 3GPP LTE Network Access Domain protocols. The profile SHALL be based on 3GPP TS 33.401, and will be determined by FirstNet based on a system design and other considerations as it deals with evolving cyber threats. As a minimum, the profile SHALL include specification of ciphering algorithms (for example, use of AES-128 vs. SNOW 3G).

[39] The nationwide common security profile SHALL include ciphering of control plane traffic in order to provide for interoperable cyber protection of the network. Ciphering of user plane traffic is optional and is based on policy decisions that involve FirstNet and user agencies.

[41] Network Domain Security SHALL be implemented in accordance with 3GPP TS 33.210, which stipulates the use of IPSec to protect IP communication between administrative domains (including all network connections used to interconnect the domains).

[42] The NPSBN SHALL comply with TS 33.310 as the authentication framework for Public Key Infrastructure to authenticate these network interfaces.