June 12, 2017

Ex Parte

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Procedures for Commission Review of State Opt-Out Requests from the FirstNet Radio Access Network*, PS Docket No. 16-269

Dear Ms. Dortch:

Rivada Networks, LLC ("Rivada") hereby provides written feedback with respect to the draft Report and Order released on June 1, 2017,[1] and also responds to recent ex parte letters filed by AT&T and FirstNet.[2] Rivada was established to facilitate efficient secondary bandwidth markets, and our leadership team combines decades of public safety experience with experience leading commercial carrier operations. The Rivada leadership includes the former Chief of Police of California's third-largest city and members of the team that led Sprint – one of the United States' four nationwide mobile wireless carriers – from 2011 through 2015.

The nationwide, interoperable public safety broadband network envisioned by the Public Safety Spectrum Act[3] has the promise to be a critically important twenty-first century tool for law enforcement. It will provide a common set of broadband applications that can be used locally – which will be well over 90 percent of the public safety use – as well as when law enforcement agencies are cooperating across state lines or providing emergency assistance to other states to respond to events such as the 9/11 attacks or Hurricane Katrina. And because the Act specifies that both the core and the radio access network portions of the network must be based on commercial standards, it has the promise to be a network that will evolve as commercially deployed capabilities evolve from 4G LTE to 5G and the Internet of Things ("IoT") and beyond. In this way, the Public Safety Spectrum Act sets out deliberately to avoid past problems of locking public safety into a limited set of stove-piped, proprietary, and ultimately obsolete communications technologies.

---

1 *See Procedures for Commission Review of State Opt-Out Requests from the FirstNet Radio Access Network*, Draft Report and Order, FCC-CIRC1706-02, PS Docket No. 16-269 (rel. June 1, 2017) ("Draft Order").

2 *See* Letter from Joseph P. Marx, Assistant Vice President, Federal Regulatory, AT&T Services Inc., to Marlene H. Dortch, Secretary, FCC, PS Docket No. 16-269 (filed May 22, 2017) ("AT&T Letter"); Letter of Patrick Donovan, Attorney, FirstNet, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 16-269 (filed May 26, 2017) ("FirstNet Letter").

3 *See* Public Safety Spectrum Act, 47 U.S.C. §§ 1401-1443, 1457.

The Public Safety Spectrum Act reflects a carefully crafted congressional design to promote both interoperability and technological evolution within a "single, national network architecture" with both core elements and its radio access networks "based on commercial standards."[4] The Act directs the FCC to convene and oversee the Technical Advisory Board for First Responder Interoperability, which was charged with developing minimum interoperability requirements and with evaluating whether any states that operated their own radio access networks would meet those interoperability requirements and be able to interoperate with FirstNet.[5] The Act charges FirstNet with ensuring the use of nationwide standards for use of and access to the nationwide network, and – except in areas where states opt out – building and operating the network, "without materially changing, the minimum technical requirements" developed by the Technical Advisory Board.[6] At the same time, the Act specifically allows states to opt out so that they can build and oversee their own state radio access network.[7]

In mandating a single, national network architecture, however, the Act nowhere mandates that FirstNet control all traffic handled by that network. Allowing states to operate their own radio access network with attendant core elements interconnected and interoperating with FirstNet provides an important benchmark for evaluating FirstNet's operation of its portions of the nationwide public safety broadband network during the initial, and subsequent, ten-year terms of the statutorily mandated license. In other words, when some states operate and control their own state networks, and necessarily interoperate with FirstNet, those states may adopt and incorporate new technologies and capabilities ahead of FirstNet, providing a means to judge FirstNet's effectiveness in ensuring that the nationwide network "evolves with technological advancements," as Congress directed.[8] Opt-out alternative providers can continue to apply this competitive pressure on AT&T to evolve with 5G and IoT use cases over the course of FirstNet's ten-year license. States operating their own radio access networks can also use different means of sharing spectrum with commercial users, always subject to the principle that public safety traffic has absolute priority and can preempt other traffic – what Rivada calls "ruthless preemption." AT&T has recently adopted this term in its own marketing, likely under competitive pressure from Rivada. State network operation provides a market check to ensure that the funding and deployment of the nationwide public safety broadband network, particularly in higher cost rural areas, is not gated by the business choices of a single vendor: FirstNet's commercial partner, AT&T. Rural coverage is a crucial function of the nationwide, interoperable public safety broadband network, and if states and their partners can do a better job of deploying rural coverage than AT&T, the Act clearly allows them to do so.

---

4 47 U.S.C. § 1422(b).

5 *See* 47 U.S.C. §§ 1423, 1442(e)(3)(C).

6 47 U.S.C. § 1426(b)(1)(A)-(B).

7 *See* 47 U.S.C. § 1442(e)(2)(b).

8 47 U.S.C. § 1422(b).

The alternative would be to read the Act very narrowly with the explicit purpose of unreasonably constraining states' construction and operation of their own networks, obviating states' ability to opt out. The Act does not allow this, and the FCC rightly seeks to avoid this outcome.

Accordingly, we agree with the Draft Order that Congress intended state opt-out to provide a "meaningful opportunity" to opt out and to make "a deliberate, informed choice" as to whether to accept what FirstNet offers or to pursue an alternative that could better serve the state.[9] The singular objective must be, as Congress envisioned, to create a nationwide, interoperable public safety broadband network that is "based on a single, national network architecture and that evolves with technological advancements."[10] But to achieve that single, national network architecture, it is not necessary for all public safety broadband traffic to be handled by FirstNet. The existence of the statutory opt-out process confirms that the Act imposes no such requirement. Indeed, as discussed further below, forcing state radio access networks to use only FirstNet core elements would materially change the minimum technical requirements developed by the Technical Advisory Board, in violation of 47 U.S.C. § 1426(b)(1)(B). As we look ahead to the implementation of the nationwide, interoperable public safety broadband network, it must be implemented in a way that provides sufficient operational decisionmaking authority to state and local governments. This local authority will be necessary to integrate the nationwide, interoperable public safety broadband network into local communications systems without severing public safety broadband network traffic from all other traffic and it is the only way to avoid importing significant and ongoing bureaucratic interactions between local officials and a centralized federal agency.

Rivada supports the Draft Order's conclusion that the statute envisioned that the Commission would act as "neutral arbiter" of whether a state opt-out plan meets the Act's interoperability requirements.[11] In this regard, the Commission's review as to which FirstNet network policies are relevant to interoperability will be critical. A FirstNet policy, for example, that directed that a state's radios and towers (i.e., its radio access network) can only be connected directly to the FirstNet core in the same way that FirstNet radios and towers would be connected – through an S1 interface – would be unduly restrictive and unnecessary to interoperability. An LTE network's "core" comprises multiple components – such as the Home Subscriber Server ("HSS"), the Packet Gateway ("PGW"), the Serving Gateway ("SGW"), the Policy and Charging Rules Function ("PCRF") Server, and the Mobility Management Entity ("MME"). A unified national architecture does not require unified operation of these disparate, standardized elements. As the Technical Advisory Board for First Responder Interoperability recognized when it promulgated the required minimum interoperability technical requirements, state radios and towers can also be connected to FirstNet through state core elements by using multiple S6a, S8, S9 or S10 interfaces, or perhaps other interfaces; all of these interfaces support interoperability.[12] As discussed further below, the main

---

[9] Draft Order ¶ 17.

[10] 47 U.S.C. § 1422(b).

[11] Draft Order ¶ 60.

[12] *See* Technical Advisory Board for First Responder Interoperability, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, Final Report, at 39, Table 1 (May 22, 2012) ("RMTR" or "Recommended

effect of constraining interconnection to an S1 interface is to exclude the provision of other core elements by the state or its network partner, and thus to limit state innovation, flexibility, and local control well beyond the restrictions necessary to ensure interoperability or security.

As the Commission evaluates which of FirstNet's policies are necessary for interoperability and thus must be evaluated pursuant to 47 U.S.C. § 1442(e)(3)(C), the Commission should not constrain itself to blindness if FirstNet acts in an exclusionary manner. It is possible to devise network policies that facially appear to relate to interoperability, but unnecessarily frustrate the congressionally mandated opt-out provisions. In this regard, we suggest that in Paragraph 61 of the Draft Order, the Commission make clear that "relevant to interoperability" means necessary to interoperability. The Act directs that the state plan "demonstrate . . . interoperability with the nationwide public safety broadband network," which is accomplished by showing that the state plan meets all requirements necessary for interoperability, not merely ones that may in some way relate to, but are not determinative of, interoperability.[13] These recommendations are entirely consistent with the Act, and are an entirely reasonable way to ensure that FirstNet and the states are implementing all of the Act's provisions faithfully.

Finally, we note that on June 5, 2017, FirstNet filed a document that it stated was an "interoperability compliance matrix that documents the technical standards that will be necessary to ensure a state or territory's RAN [radio access network] is interoperable with the NPSBN [Nationwide Public Safety Broadband Network]."[14] It is unclear whether this is the final matrix of criteria that, in FirstNet's view, must be applied in order for a state plan to satisfy 47 U.S.C. § 1422(e)(3)(C)(i)(II). The Commission should request that FirstNet clarify what this document represents.

I. There Is No Technical or Legal Reason That a State RAN Must Exclusively Use the FirstNet Core for All Core Functions, As Compared with Using the FirstNet Core for Some Functions with States or Their Partners Providing Others.

FirstNet devotes a substantial portion of its ex parte to asserting that a state operating its own RAN must use the FirstNet core.[15] At one level, this conclusion is unremarkable to the extent that it simply reflects a reality: all state networks will be interconnected into the nationwide, interoperable public safety broadband network and will communicate with and interoperate with the FirstNet core.

Minimum Technical Requirements"), https://ecfsapi.fcc.gov/file/7021919873.pdf. Appendix 1 reproduces this table listing the various interfaces that can be used in the nationwide, interoperable public safety broadband network depending on the network elements being connected. These interfaces are not predicated upon implementation by a single operator, but can be used between different operators.

[13] 47 U.S.C. § 1442(c)(3)(C)(i).

[14] Letter of Patrick Donovan, Attorney, FirstNet, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 16-269, at 1 (filed June 5, 2017).

[15] *See* FirstNet Letter at 2-5.

FirstNet, however, appears to be asserting without explicitly stating that its core elements can be the *only* core used to provide *any* core functions. That is not what the Act says. If actually implemented, such a narrow restriction would render opt-out meaningless. Essentially, it would constrain a state to running nothing more than a collection of unintelligent and unmanaged radios and towers, strung together by transmission facilities, and thus preclude states from exercising local control over quality of service, priority, and pre-emption in their territory, a feature that FirstNet otherwise touts as a key benefit of the nationwide, interoperable public safety broadband network.[16] Moreover, accepting such a restriction would eliminate a fundamental benefit of opt-out mentioned above: states would be unable to act as an initial check (and market-based prod) on the deployment plans offered by FirstNet's partner, AT&T, and, over the longer term, opt-out states would not become laboratories for the adoption of additional new technologies and benchmarks for FirstNet's own performance in ensuring that the nationwide, interoperable public safety broadband network continues to evolve as commercial technologies advance. In all, accepting FirstNet's very narrow and unsupported reading of what the Act allows would create the very situation that the FCC rightly seeks to avoid – rendering opt-out a "false choice" contrary to the plain language of the Act.[17]

The Act never bars states from operating elements of a core network. In fact, it does not say anything about state core elements at all. AT&T and FirstNet both seek to interpret this silence as a ban on state-operated public-safety cores, but this conclusion defies both modern LTE network management practices and common sense. The Act does require FirstNet to construct a core network – which FirstNet would have to do in order to ensure that there could be a nationwide public safety broadband network in any state in which the state did not operate the RAN.[18] States should be free to contract with FirstNet for any or all "core services," as provided for in the Act. But nothing in the Act compels them to do so if they choose to provision those services to their own first responders, using only a more limited set of FirstNet core elements, provided only that the state's solution is interoperable with FirstNet's. This is not as difficult as AT&T or FirstNet would have the Commission, Congress, and the states believe.

---

[16] *See* Jeff Posner, *Local Control and the NPSBN*, FIRSTNET, (Mar. 16, 2016) ("FirstNet Local Control Blog"), https://firstnet.gov/newsroom/blog/local-control-and-npsbn.

[17] Indeed, opt-out and ensuring that states have a true right to opt out was the subject of questions at a recent hearing of the United States Senate Committee on Commerce, Science, and Transportation. *See Nomination Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, at 1:03:15 to 1:06:07 (June 8, 2017), https://www.commerce.senate.gov/public/index.cfm/hearings?ID=45F84816-5320-41D3-9B87-F7814B56DB84.

[18] *See* 47 U.S.C. § 1422(b)(1).

There is broad consensus over the functions that need to be performed within the nationwide, interoperable public safety broadband network through all core elements acting collectively, irrespective of who owns or operates each element. In its RFP, FirstNet had sixteen objectives:[19]

- Building, Deployment , Operation, and Maintenance of the NPSBN
- Financial Sustainability
- First Responder User Adoption
- Device Ecosystem
- Application Ecosystem
- Accelerated Speed to Market
- User Service Availability
- Service Capacity
- Cybersecurity
- Priority Services
- Integration of State-Deployed RANs
- Integration of Existing Commercial/Federal/State/Tribal/Local Infrastructure to Support NPSBN Services
- Life-Cycle Innovation
- Program and Business Management
- Customer Care and Marketing
- Facilitation of FirstNet's Compliance with the Act and Other Laws

States share these objectives, and a network in which a state or its partner operated core elements in conjunction with that state's radio access network would have to be part of meeting these objectives.

That does not, however, mean that these objectives must only be achieved through FirstNet-owned and operated core elements. Although FirstNet prefers to talk about the core network as if it were a monolith, it is not. Indeed, the Act itself recognizes that the core consists of "national and regional data centers, and other elements and functions that may be distributed geographically, all of which shall be based on commercial standards."[20] As noted above, an LTE eNodeB core has a variety of server, gateway, and other standardized elements. It is an everyday occurrence for LTE networks to interoperate with multiple providers each controlling these elements, with them interconnected as necessary.[21] Moreover, the precise implementation of these core functions has evolved, and continues to evolve, and the commercial standards and commercially available solutions have evolved in parallel. In any potential nationwide, interoperable public safety broadband network architecture, there can be duplicates of many core elements in the solution, some of which are necessary simply to maintain a robust, geographically diversified network and also to

---

[19] Interior Business Center and FirstNet, *Solicitation No. D15PS00295 – Section C: Statement of Objectives*, at C-3 to C-6 (amended Mar. 9, 2016), https://www.fbo.gov/utils/view?id=ffcfb92f71c55096812b3378c34cfd7f.

[20] 47 U.S.C. § 1422(b)(1)(A).

[21] *See* Appendix 2.

minimize inefficiencies. It is unlikely, for example, that AT&T will route all traffic through a single nationwide router; instead, it will likely have multiple traffic routers distributed around the country. And core-to-core interaction between entirely separate cores will be necessary even to implement AT&T's network: AT&T will maintain both a commercial core for its non-public safety subscribers and a "FirstNet" core for the public-safety business in opt-in states, and those cores will have to communicate with each other constantly in order to manage network priority and, when necessary, preemption of secondary commercial traffic. With the commercially deployed LTE standards, as the guidance provided by the Recommended Minimum Technical Requirements demonstrates, it is simply not a substantial technical challenge to integrate state core elements with FirstNet core elements such that they are interconnected and interoperable.

There are, of course, certain functions that FirstNet will have to perform to ensure a smoothly operating, nationwide public safety broadband network. In order for first responders to move from a geographic area in which FirstNet operates and controls the radio access network to an area in which a state operates and controls the radio access network, the state radio access network, and its associated core elements, will need to obtain from FirstNet confirmation that the first responder is an authorized user and information as to the appropriate levels of priority that user is accorded. This can be accomplished in the same manner in which commercial roaming operates today, with the visited network confirming with the end user's home network that the end user is an authorized user. This requires databases in each network to be able to talk to each other and to communicate the relevant information, which, in the case of public safety, would also include the priority to be accorded the user that has travelled from one state to another. But FirstNet need not control or operate the Home Subscriber Services server for the opt-out state in order for the first responder to move seamlessly from a FirstNet-run radio access network to a state-run radio access network. Similarly, when first responders from a FirstNet state need to be assigned to a user group in an opt-out state, that assignment can also be accomplished simply by coordinating the exchange of relevant data between FirstNet and the opt-out state, such that the opt-out state can then populate its own core databases accordingly.

With respect to network security, the required minimum technical requirements issued by the Technical Advisory Board contained provisions governing network and cybersecurity.[22] In its RFPs, FirstNet developed a set of requirements, which, by statute, were required to utilize the minimum technical requirements without material change.[23] State networks, including state-controlled core elements, can meet these same requirements; it is not necessary to replace them with FirstNet core elements to protect the nationwide, interoperable public safety broadband network from cyberattacks.

It will also be greatly beneficial for FirstNet to be the entity that certifies devices and applications that will be used on the nationwide, interoperable public safety broadband network. Applications testing is itself complicated and is critical to maintaining security for users. FirstNet,

---

[22] *See* RMTR at 79-90 (Section 4.8).

[23] *See* Interior Business Center and FirstNet, *Solicitation No. D15PS00295 – Attachment J-3: FCC TAB RMTR*, at J-3 – 11 to J-3 – 12, J-3 – 15 to J-3 – 16 (Sections 1.3.7 and 1.4.8).

however, can control certification of applications and devices without exerting direct control over every part of every function of the network core. It need not control every core element used by a state radio access network, it need not control the flow of traffic over the nationwide, interoperable public safety broadband network, and it need not directly register every public safety user. FirstNet would control all of these functions and more, however, if it were to limit state radio access networks to operating only with FirstNet core elements.

As these examples show, it is not necessary to bar states from performing or controlling any "core" functions within their state. All that is required is that the FirstNet core and the opt-out state core elements be capable of communicating, using standards-defined interfaces, and exchanging the necessary information about subscriber privileges and priorities when it becomes necessary for public-safety users to move between opt-in and opt-out states.

Indeed, as Appendices 1 and 2 show, when the Technical Advisory Board for First Responder Interoperability developed its statutorily mandated minimum interoperability requirements, it specifically included examples of situations that leveraged existing state core elements, where they existed, and multiple core configurations with scale and scope. Although FirstNet would need to work with states to develop methods and procedures to implement these interactions, as the statute intended, there is no significant technical or operational impediment to doing so.

Accordingly, claims that state-operated core elements threaten interoperability and security are simply untrue. States have a long history of operating public safety communications networks, and local control of those networks remains essential to executing their missions.

II. Requiring That States Only Use FirstNet Core Elements Significantly Impinges on Local Operational Control of Public Safety Broadband Communications.

Requiring that FirstNet be the exclusive provider of core elements and functions even for state-operated radio access networks has a significant impact on the amount of operational control that public safety agencies in opt-out states will have with respect to use of the nationwide public safety broadband network on a day-to-day basis. It would leave opt-out states with considerably less operational control than AT&T is currently promising opt-in states, which is surely contrary to the intent and plain language of the opt-out provisions of the Act, is unnecessary to maintain a nationwide, interoperable public safety broadband network, and serves only to deter opt-out even when use of an alternative solution clearly benefits the state, its citizens, and first responders.

In a March 2016 blog, FirstNet outlined some key functions over which public safety agencies should be able to "directly configure the operations of the network to their own needs."[24] These included:

- **Quality of Service, Priority and Preemption** (QPP) – This provides authorized users the ability to raise or lower settings of one or more users

[24] FirstNet Local Control Blog.

- **Users & Groups** – provides authorized users the ability to manage users and groups within their control and map these to roles and profiles
- **Roles & Profiles** – provides authorized users the ability to manage roles & profiles that simplify user management
- **Devices & Provisioning** – provides authorized users the ability to manage devices and the provisioning of those devices on the network
- **Applications & Services** – provides authorized users the ability to whitelist and blacklist applications and assign applications to specific users or devices

FirstNet was right. These are all aspects of service for which direct local control is best.

It is therefore mystifying why FirstNet views state-run local core elements that effectuate these functions with such hostility. Take quality of service, priority, and preemption, for example. The vast majority of the use of the nationwide, interoperable public safety broadband network by public safety agencies day-to-day will be by local first responders within their own communities, conducting routine police activities or responding to local fires or other emergencies. In this situation, it makes sense for public safety agencies within the state to be able to set the priority levels for different individual first responders, to add and remove users, and to be able to do all of that on a day-to-day basis. That can be done with a remote server at FirstNet or a local server in the state-run network. However, if there is a problem, it may be easier to resolve with the local server and network provider than at a remote location through systems and personnel tasked with dealing with the entire country. The same is true with respect to the other functions that FirstNet identified for local control.

Of course, there may be rare, but important, situations such as major disasters or other events that either span multiple states (such as a hurricane) or high-impact incidents like the 9/11 attacks, in which it makes sense not just to have first responders from other states roam into the opt-out state, but to add those individuals into the opt-out state's own database of authorized users. As discussed above, FirstNet should facilitate the information exchange necessary to make that level of seamless operation possible. But FirstNet itself does not need to operate the state's Home Subscriber Server in order to make that happen.

Moreover, forcing a state to use FirstNet's core could significantly reduce rural coverage by raising the costs of operating an opt-out network, and thus reducing the net revenues available to be plowed back into expanding and upgrading rural deployment. The vast majority of the costs – more than eighty-five percent – of deploying a public safety broadband network in a state are the costs of building, operating, maintaining, and upgrading the radio access network. And, as the Commission is well aware, these costs are substantial, particularly in sparsely populated rural areas in which fiber backhaul is not also supported by substantial commercial business activity. If a state is required to use FirstNet's core entirely – and thus to pay fees to FirstNet for every core function – states lose the option of contracting with a state partner to bear the incremental costs of the state core elements – which Rivada believes frequently will be less than FirstNet's fees. Depriving states of a lower cost self-provisioning option diverts to FirstNet revenues that could otherwise fund additional rural network deployment within the state. This will especially be the case if the state's partner is better than AT&T at monetizing secondary commercial use of the 700 MHz spectrum. It should not

simply be assumed that AT&T has devised the optimal means of monetizing secondary use of the 700 MHz public safety spectrum. If a state believes it has a partner that can operate more efficiently or with a superior means of monetizing commercial secondary use, so as to develop a better, more fully deployed interoperable public safety broadband network in that state, the Act creates the vehicle to do so – state operation of the radio access network – provided that the state and its partner can also operate the associated core elements necessary to effectuate that means of managing and utilizing the spectrum commercially, subject to ruthless preemption. Denying states that ability could significantly reduce rural coverage – and certainly would deprive states of the ability to market-test AT&T/FirstNet's network deployment offers.

Furthermore, because the vast majority of traffic on the state-run portion of the nationwide public safety broadband network will be intrastate traffic, it is also perplexing that FirstNet would apparently require that all traffic be routed to FirstNet's core for handling. One would think that it would be much more efficient – and consistent with the way that AT&T is likely to design FirstNet's network in the non-opt-out states – for that traffic to remain local, handled and managed by local servers for routing between local first responders and public safety agencies. In addition, it would allow for autonomous state operation in the event that the connection to FirstNet's core were severed.

States and localities may also decide that they want to evolve their technological capabilities faster than FirstNet does for the rest of the country. When states operate their own core elements that are interconnected with FirstNet's core and rely upon FirstNet's core for the functions that only FirstNet can provide, states can choose to introduce new technologies and features. For example, consider the path to Mission Critical Push to Talk ("MCPTT"). States have existing assets, unique needs, and potentially different roadmaps for the deployment of MCPTT features. When a state controls core elements, which are interoperable with the FirstNet's core elements, the state can independently determine both the timing and scope of MCPTT feature functionality deployment, without being tied to FirstNet's or its network partner's plans. States may also wish to move ahead of FirstNet in implementing IoT and or 5G or successor generation technologies while remaining backward compatible with FirstNet to preserve nationwide interoperability. States cannot do that if FirstNet has divested them of the opportunity to operate any of their own public safety core elements.

Finally, in its legal interpretations, FirstNet stated:[25]

> 26. FirstNet concludes that the Act provides sufficient flexibility to allow the determination of whether FirstNet or a State plays a customer-facing role to public safety entities in a State assuming RAN responsibilities to be the subject of operational discussions between FirstNet and the State in negotiating the terms of the spectrum capacity lease.

---

[25] Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012, 80 Fed Reg. 63,504, 63,506 (Oct. 20, 2015).

> 27. FirstNet concludes that it will maintain a flexible approach to such functions and interactions in order to provide the best solutions to each State so long as the agreed upon approach meets the interoperability and self-sustainment goals of the Act.

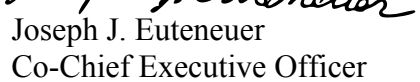
If FirstNet maintains the position that it must operate all core elements, and the state or its partner must not operate any, then FirstNet will have effectively foreclosed the possibility of the state playing a "customer-facing role" to state public safety entities. The legal conclusion is correct that these are operational and functional interactions that can be worked out through agreed-upon procedures. They are not themselves related to interoperability.

* * *

Rivada looks forward to working with states, FirstNet, and AT&T to make the nationwide public safety broadband network a success. As in all areas of communications technology, that success will be fueled, not restrained, by maintaining the competitive discipline that Congress envisioned when it provided for state-operated radio access networks as part of its framework for a nationwide, interoperable public safety broadband network.

Sincerely,

Declan Ganley
Executive Chairman
& Co-Chief Executive Officer



Joseph J. Euteneuer
Co-Chief Executive Officer

cc: Zenji Nakazawa
Daudeline Meme
Erin McGrath
Lisa Fowlkes
David Furth

APPENDIX 1

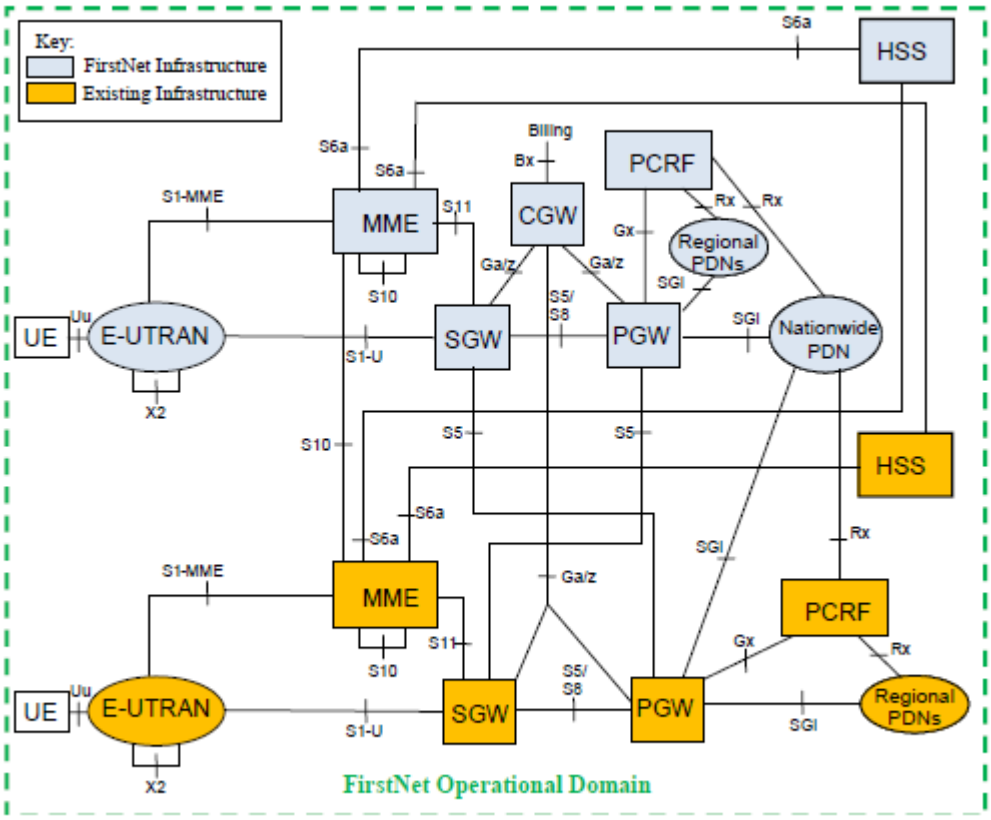
Table 1: Minimum Interoperable Interfaces

Interface Name	Description	Required Standards
Uu	Air Interface between Device (aka, UE) and eNB.	3GPP TS 36.101, 36.104, 36.133, 36.141, 36.201, 36.211, 36.212, 36.213, 36.214, 36.314, 36.321, 36.322, 36.323, 36.331
S1	Comprised of two interfaces: S1-U user plane between eNB and S-GW; S1-MME signaling plane between eNB and MME, UE and MME.	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.412, 36.413, 36.414, 33.210, 33.310
S6a	Signaling plane interface between MME and HSS.	3GPP TS 29.272
S5/S8	User plane interface between S-GW and P-GW.	3GPP TS 29.274, 29.281
S9	Signaling plane interface between PCRF in home network and PCRF in visited network.	3GPP TS 29.215
S10	Signaling plane interface between MMEs.	3GPP TS 29.274
S11	Signaling plane interface between MME and S-GW.	3GPP TS 29.274
SGi	User plane interface between P-GW and external IP networks.	3GPP TS 29.061
Gx	Signaling plane interface between PCRF and P-GW.	3GPP TS 29.212, 29.213
Rx	Signaling plane interface between PCRF and external Application Functions.	3GPP TS 29.214
X2	User plane and Signaling plane interface between eNBs.	3GPP TS 36.420, 36.421, 36.422, 36.423, 36.424

Source: Technical Advisory Board for First Responder Interoperability, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, Final Report, at 39, Table 1 (May 22, 2012), https://ecfsapi.fcc.gov/file/7021919873.pdf.

APPENDIX 2

Configuration 1 – Leverage User Plane and Signaling Plane Elements of the Existing Infrastructure Networks



Source: Technical Advisory Board for First Responder Interoperability, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, Final Report, at 31 (May 22, 2012), https://ecfsapi.fcc.gov/file/7021919873.pdf.