Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	)	WT Docket No. 06-150
	)	
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)	PS Docket No. 06-229
	)	
Amendment of Part 90 of the Commission's Rules	)	
	)	WP Docket No. 07-100

COMMENTS OF NOKIA SIEMENS NETWORKS US LLC

TABLE OF CONTENTS **PAGE**

I. INTRODUCTION AND SUMMARY 2
II. RESPONSES TO QUESTIONS POSED IN THE FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING 3
A. Technical Rules for the Public Safety Broadband Network 3
1. Architectural Framework 3
2. Architectural Guiding Principles 4
3. Open Standards 6
4. Technology Platform and System Interfaces 7
5. System Identifiers 10
7. Roaming Authentication and Interworking Functions 11
8. Interconnectivity of Regional or Tribal Broadband Networks 11
9. Prioritization and Quality of Service 12
10. Mobility and Handover 12
11. Out-of-Band Emissions and Related Requirements 13
12. Applications 14
14. Performance 17
15. Network Capacity 19
16. Security and Encryption 20
17. Robustness and Hardening 21
18. Coverage Requirements 22
19. Coverage Reliability 22
B. Public Safety Roaming on Public Safety Broadband Networks 23
1. Prioritization and Quality of Service to Support Roaming 24
2. Applications to Be Supported 26
D. Testing and Verification to Ensure Interoperability 27
1. Conformance Testing 27
2. Interoperability Testing 28
3. Interoperability Verification 29
E. Other Matters Relevant to Interoperability on Public Safety Broadband Networks 30
1. Network Operations, Administration and Maintenance 30
3. Devices 31
4. In-Building Communications 32
6. Operation of Fixed Stations and Complimentary Use of Fixed Broadband Spectrum 34
8. Public Safety Broadband and Next-Generation 911 Networks 34
F. Section 337 Eligible Users 35
III. CONCLUSION 37

I. INTRODUCTION AND SUMMARY

Nokia Siemens Networks US LLC (hereafter "Nokia Siemens Networks") respectfully comments in response to the *Fourth Further Notice of Proposed Rulemaking* (hereafter "*Fourth Further Notice*"), in the above-captioned proceeding.[1] Nokia Siemens Networks supports the Commission's efforts aimed at the creation of an effective technical framework for ensuring the deployment and operation of a nationwide interoperable public safety broadband network.

Nokia Siemens Networks is a leading global enabler of communications services. The company provides a complete, well-balanced product portfolio of mobile and fixed network infrastructure solutions and addresses the growing demand for services with 20,000 service professionals worldwide. NSN is one of the largest telecommunications infrastructure companies with operations in 150 countries. In the mobile broadband sector, Nokia Siemens Networks is a world leader in the emerging technology of Long Term Evolution (LTE).

In the comments that follow, Nokia Siemens Networks seeks to address many of the questions that the Commission poses in the *Fourth Further Notice.* The approach taken is to rely on the company's well-developed technical expertise. While refraining from expressing a view on some of the overarching policy questions, Nokia Siemens Networks believes that its comments should be read with one general theme in mind. Specifically, Nokia Siemens Networks believes that, ultimately it is the public safety community, along with its vendors, in combination representing the public safety ecosystem, that is best positioned to identify the most-detailed network requirements and resulting system parameters of the public safety systems that when deployed will constitute the nationwide, interoperable public safety broadband network. So while the Commission rightfully established a single technology platform for the network and is setting the overall framework and establishing minimum system guidelines, Nokia Siemens Networks urges it to maintain a level of humility about the massive undertaking that will be

[1] *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, FCC 11-6 (rel. Jan. 26, 2011).

required to make this network of networks a complete success. To that end, the Commission should issue guidelines and principles where feasible in lieu of detailed regulations that inadvertently could pose a risk of freezing technological innovation.

II. RESPONSES TO QUESTIONS POSED IN THE FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING

The Commission in the *Fourth Further Notice* considers and proposes requirements to further promote and enable nationwide interoperability among public safety broadband networks operating in the 700 MHz band. The Commission states that the purpose is to address interoperability from a technological perspective. Nokia Siemens Networks responds accordingly.

A. Technical Rules for the Public Safety Broadband Network

1. Architectural Framework

The Commission proposes a set of high-level principles to guide development of the network in a manner that ensures interoperability and seeks comment on them. Nokia Siemens Networks believes that the high level architectural guiding principles outlined in Section A.2 of the *Fourth Further Notice* are comprehensive and will provide a realistic framework to guide the development of a Public Safety Broadband Network. The Commission must consider the tradeoffs between providing architectural principles and creating architectural rules. Nokia Siemens Networks understands the Commission's need to foster the development of an interoperable broadband network. However, many important unanswered questions remain, including around the number of networks and whether core networks will be centralized or de-centralized. Architectural guidelines rather than rigid rules will enable Public Safety considerable deployment flexibility in order to deal with the market uncertainty while at the same time maintaining the overarching framework that is needed to enable interoperability.

2. Architectural Guiding Principles

Roaming Authentication and Internetworking Functions – Clearing House

Nokia Siemens Networks believes that a clearing house function directly aligns with the methodology that commercial carriers use worldwide to enable roaming and interchange traffic. Nokia Siemens Networks strongly recommends a similar approach be utilized for Public Safety Broadband Networks.

Roaming Authentication, however, is a function that remains with the roamers' home network. As a roamer attaches to a visited network, the visited network queries the Home Subscriber Server in the roamers home network. Nokia Siemens Networks would not recommend changing this functionality as it compromises the local control that an agency has over its resources/subscribers. The functions of the clearing house should focus on roaming agreements, clearing and interconnectivity between the individual or regional networks.

Nationwide Backbone Network

Commercial Network Operators utilize Internetwork Packet Exchange (IPX) protocol networks to provide interconnectivity for roaming and data interchange. Public Safety Broadband Networks will come online in phases over different geographic regions over the next few years, which will keep a contiguous Nationwide Backbone Network from emerging for a number of years. Nokia Siemens Networks believes that utilizing an existing network, potentially managed by a clearing house, will enable roaming and data interchange much more quickly and with much less complexity.

Evolution

One of the key benefits of basing a network on 3GPP standards is the backwards compatibility and interoperability that 3GPP ensures during the standardization process. As long as disparate networks follow the standards, interoperability between those networks will continue. As many questions still remain unanswered on topics like the number of PLMN-ID's, the number of core networks and even the ownership of the networks, in the event that networks independently evolve through differing releases of

3GPP features, Nokia Siemens Networks is confident that requiring networks to comply with 3GPP standards will ensure continued interoperability.

The Commission seeks comment on its tentative conclusion that it should establish guiding principles for public safety broadband network architecture and whether the principles it outlined should serve as the basis.[2]

Nokia Siemens Networks believes that the Commission should establish guiding principals for network architecture but not specify architecture requirements that would make it difficult for public safety network operators to meet their performance and operational goals without exceeding their financial means. There are potentially many different Public Safety Broadband deployment scenarios required to meet the varying needs of agencies. In large metropolitan areas, a single but geographically dispersed core network would likely be the best solution. On the other hand, a small core network would likely best serve the needs of small rural county while also meeting the expected financial constraints.

There are considerable cost savings and reductions in overall network complexity achievable through utilization of shared network infrastructure. A significant part of the cost in a Public Safety Broadband network is attributable to the core network in small networks. In many instances the core network can support many more subscribers and radio access network elements than the typical jurisdiction will need. 3GPP Release 8 also provides many features that enable a model where a geo-redundant, shared, and regionally centralized core network can host many disparate radio access networks and enhanced packet core elements. The benefit of this is that the user traffic stays close to the radio access network which is assumed to be where the majority of the end user applications will be, regional traffic can be routed to applications that are centralized and the cost efficiencies of shared core networks can be realized.

Flexibility should be afforded for regional cores and in some instances entities will need their own core. The Commission should give the public safety community the flexibility to select whichever core deployment scenario best meets its needs. In fact, in some situations the capital involved with

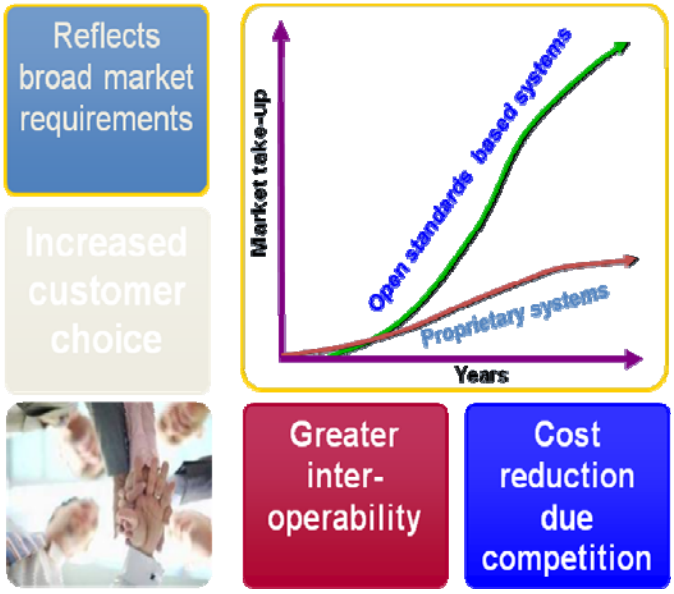
[2] *Fourth Further Notice*, ¶*25.*

establishing a unique core might be better spent on investing in radio network coverage.

While Nokia Siemens Networks agrees with the Commission's conclusion to adopt the described architectural framework, it also believes that there are a number of unanswered questions that will become more clear as funding, technology and deployment issues are resolved over the next one to two years. We further agree that this framework must be reviewed as the market and technology evolve. For example a body like the Emergency Response Interoperability Center Public Safety Advisory Committee (PSAC) or the Public Safety Communications Research (PSCR) program which have involvement from both the public safety community and industry would be able to provide guidance and address the evolution from both technological and policy perspectives.

3. Open Standards

Nokia Siemens Networks believes that open standards are essential to creating and maintaining a competitive marketplace, which in turn establishes a cost efficient ecosystem for the industry. Openness as developed by the Third Generation Partnership Project, 3GPP, for GSM, UMTS, and now LTE ensures a large number of equipment choices based on high levels of interoperability and competition. Finally, open standards reflect a broad set of market requirements which ensures robust feature development for the industry.



The Commission seeks comment on whether it should take additional measures to encourage public safety broadband network operators to adopt technologies that employ open standards.[3] To ensure high levels of interoperability and ubiquitous mobility the UNI (User to network interface) benefits the most from supporting open standards. Nokia Siemens Networks supports the use of conformance and interoperability testing to 3GPP standards at designated entities, which for example could include PTCRB or GCF for device conformance testing and the PSCR testing labs or Idaho National Laboratory (INL) for telecom infrastructure equipment.

4. Technology Platform and System Interfaces

The Commission seeks comment on additional capabilities within the LTE technology platform that it should require public safety broadband networks to support and asks about the future evolution of LTE standards and other future technology platforms.

Given the nature of 3GPP standards, basic interoperability is inherent to the standard and to industry support based on years of development and commercial operation. 3GPP system releases on average are available every two years, which introduce new capabilities. Nokia Siemens Networks

[3] *Id.*, ¶28.

believes that the decision to upgrade to a new release should be done by the stakeholders in the public safety network. New releases from 3GPP may have hardware and/or software impact whose applicability to public safety should be determined as part of operating a network.

3GPP Release 8 is the appropriate baseline release for an LTE deployment as a mobile broadband network. Additional features introduced in 3GPP Release 9 such as Location Services, CMAS (Commercial Mobile Alert Service, E911 Voice call support, etc) may be needed depending on public safety requirements, use cases, and deployment scenarios which are best determined by the system owner(s) either after the initial Rel-8 deployment or as part of deployment.

3GPP standards are built with backwards compatibility. In commercial networks software upgrades are done in stages with some networks depending on size taking months to complete an upgrade. Compatibility is still maintained during the transition period and for legacy devices which are still supported throughout. As an example, on current systems legacy WCDMA Release '99 devices are still operating on WCDMA Release 8 networks. Overall software and hardware feature introduction and decisions to upgrade from one 3GPP release to another is an operational issue which needs to be handled as part of running a network.

Nokia Siemens Networks believes that interoperability of the network elements and on-net devices are well handled by 3GPP standards and conformance testing. Interoperability of applications and services which run over the 3GGP LTE Radio and Evolved Packet Core Networks would depend on the use of open standard interface protocols and defined profiles which need to be agreed to by the stakeholders of the network.

The Commission asks about the use of both IP version 4 (IPv4) and version 6 (IPv6) and whether the use of both versions in various components of the nationwide network might create obstacles to achieving interoperability, either now or in the future.[4]

Nokia Siemens Networks observes that IANA ran out of the free IPv4 address pool on February

[4] *Id.*, ¶30.

3, 2011. The local RIRs (Regional Internet Registries) are expected to run out of their remaining addresses by the end of June 2011 (some may have reserves for slightly longer but not beyond 2012). Assuming IPv4 addressing for new services and large deployments is based on the lack of new IPv4 address space, public safety should look at the scalability and availability of IPv6.

Regarding the prices for IPv4 addresses, Microsoft set the market price in March 2011 for IPv4 addresses by buying 600 thousand IPv4 addresses at slightly over $11 each. This compares to IPv6 prices which are $0 (minus processing fees).

The benefit of launching with IPv6 is that public safety can take advantage of a one-time opportunity to plan its IP address space with IPv6. The minimum approach is to start with a dual stack IPv6/IPv4 network and migrate operations fully to IPv6 over time. The benefit to this approach is that early phase IPv6 planning and introduction is completed at the start of the network, which greatly simplifies the issues of introducing a new IP version addressing scheme at a later time.

Planning for IPv4 as a service enabler has indirect costs, which come in the form of extending IPv4 lifetime aggressively and prolonging the translation between IP version families. Depending on the number of available IPv4 address and the amount of devices connected to the public safety network, IPv4 brings large numbers of Network Address Translations (NAT), which creates scalability and application level (UN) SAF (UNilateral Self-Address Fixing) issues.

The biggest initial challenge of IPv6 introduction is the lack of operational experience and in-house tools, which can be obviously handled by training and development. There is a potential for some software or network nodes that do not support IPv6, but clear guidance on its use should expedite support cycles.

The main advantages of IPv6 are IP address space size, which will support public safety for the life of the system and re-establishment of true end-to-end client to server paradigm.

If the network is dual stack, then IPv4 and IPv6 can co-exist. There can be some problems arising from some IPv6 hosts or services needing to communicate with an IPv4 only host where a

transition has to be deployed. In general this kind of scenario should be minimized.

Nokia Siemens Networks views Dual-stack IPv4/IPv6 as a pragmatic way to enable transition mechanism from IPv4 to IPv6. In fact, dual stack IPv4/IPv6 is the preferred mechanism for 3GPP mobile networks.

Most operating systems and IP stacks have been dual-stack capable for many years. The problem mainly resides on the applications side, which have been hardcoded to IPv4 only communication. There is always a cost of running two address families in the network. The routing information on IPv4 and IPv6 are distinct, and need to be separately managed. This is also true for the reverse DNS.

The Commission asks whether it should require that public safety broadband networks adopt, in addition to the interfaces specified in the Third Report and Order, PMIP and the corresponding additional interface, Gxc.[5]

GTP is well proven and a widely deployed interface in 3GPP systems. Nokia Siemens Networks supports the notion of simplicity for network operations within the public safety systems. The use of another protocol (PMIP) does not appear to bring any additional value; and in fact, adds complexity to operating the network. GTP deployment is a requirement for widespread interworking with external 3GPP networks; therefore, to add PMIP for essentially the same functionality adds operational burden as well as requiring an extra policy interface due to PMIP only being a mobility protocol as compared to GTP.

5. System Identifiers[6]

Nokia Siemens Networks observes that there are many facets to take into account when considering the number of PLMN IDs needed. In commercial networks a single PLMN ID for a single network is the general implementation but not the rule. Due to consolidation between operators multiple

[5] *Id.*, ¶31.

[6] *Id.*, ¶¶32-34.

PLMN IDs do exist in networks around the world. Technically, having more than one is not prohibited but is an administrative burden which expands with each additional PLMN ID which needs to be maintained. In general Nokia Siemens Networks believes that minimizing the absolute number of PLMN codes used for public safety networks would reduce the long term operation burden for the network or individual networks. Having a logical national network made up of regional networks will reduce complexity and cost by minimizing the number of PLMN IDs but allowing regional control. A single PLMN ID still enables individual regional networks to be built which comprise parts of the overall national Public Safety Network.

7. Roaming Authentication and Internetworking Functions

The Commission tentatively concludes that within the context of public safety broadband networks, there would be significant efficiency gains if roaming authentication and clearing functions were performed by third party clearing houses rather than by each network operator.[7] Nokia Siemens Networks believes that operational efficiencies from a single clearing house or group of authorized clearing houses for all public safety networks would be beneficial. The extent of the gain from clearing house(s) or the need for more than one would depend on the number of networks which would compromise the national public safety network and how they are administratively operated.

8. Interconnectivity of Regional or Tribal Broadband Networks[8]

Nokia Siemens Networks observes that the complexity and cost of direct connectivity depends on the traffic volume and the total number of discrete networks which would ultimately compose the public safety network. In general, due to the need for high availability, minimal delay and security, more than one peering point is needed for public safety, which is further complicated when geo-redundant paths are considered.

---

[7] *Id.*, ¶37.

[8] *Id.*, ¶¶38-42.

Nokia Siemens Networks in, commercial networks, finds that operators do not use the public internet for interconnectivity due to design considerations such as reliability, security, latency, etc. For interconnectivity, private networks and peering points between networks are used which do meet these design considerations. Public Safety systems should follow a similar approach and specify requirements for interconnectivity related to performance, reliability, and security which would be followed regardless whether public safety or a 3rd party provider is used for interconnection.

9. Prioritization and Quality of Service

The Commission seeks comment on how public safety broadband networks should support both prioritization and quality of service among connections as well as applications over these connections.[9] Nokia Siemens Networks believes that the capability defined in 3GPP Release 8, i.e., ARP and QCI for QoS function and Access Class barring features are sufficient for supporting priority access within the public safety network. When the network is upgraded to 3GPP Release 10, the network can also support "enhanced Multimedia Priority Service" (eMPS) feature which allows Paging priority indication for terminating LTE access, and IMS priority handling with LTE access, and PCC (Policy Control and Charging) for setting priority level. These additional capabilities from 3GPP Release 10 eMPS feature may benefit the public safety network.

10. Mobility and Handover [10]

The Commission tentatively concludes that each operator's network must support seamless handover within its coverage region. Nokia Siemens Networks agrees that the commission should mandate handover between eNodeB's as long as there is coverage between them.

3GPP standards accounted for two use cases for HO which allows for a localized X2 or a S1 based HO due to there being cases where transmission interconnection is not practical or possible. Nokia

[9] *Id.,* ¶¶43-46.

[10] *Id.,* ¶¶47-50.

Siemens Networks would rather see the mandating of HO support versus choosing a specific method and leave it to deployments to determine what is best suitable.

The Commission asks about the case where handover occurs between two eNodeBs from two different neighboring networks, and how seamless handover would be possible in such situation. In response, Nokia Siemens Networks notes that the definition of neighboring network depends on if there is a different PLMN ID used or if, from network topology perspective, a different PDN-GW is needed. Inter-PLMN handovers's though possible are quite rare in commercial networks due to the complexity of maintaining the references between networks in synch. Depending on the actual network deployment, a handover can be made or the UE will need to re-connect on the other network.

Finally, Nokia Siemens Networks observes that LTE networks are designed to handle low mobility pedestrian speeds through high speed train mobility. A better metric for performance would be to define a handover interrupt time, which is a parameter independent of the actual speed of the UE.

11. Out-of-Band Emissions and Related Requirements[11]

As an initial matter, Nokia Siemens Networks concurs with the Commission's findings as stated in paragraph 51 of the *Fourth Further Notice.*

The important issue of OOBE limits and the use of guard bands in order to protect the use of the Public Safety Broadband Block and the D block[12] has been extensively studied - both within 3GPP as a collective study item as well as in an independent set of studies conducted separately by Nokia Siemens Networks. In 3GPP TR 36.942, the various corporate contributors to the study have concluded that in the worst-case scenario, wherein operators in adjacent bands do not cooperate in order to mitigate LTE-to-LTE interference, that there is a less than 1% loss in downlink throughput (assuming an Adjacent Channel

[11] *Id.,* ¶¶51-54

[12] *Id.,* ¶53.

Interference Ratio Power of 40 dB). Furthermore, these 3GPP studies also conclude that there is a less than 1% loss in the uplink cell throughput for (for an Adjacent Channel Interference Ratio Power of 35 dB). It is important to note that this negligible (<1%) loss in throughput is attained without the institution of a guard band between the adjacent LTE bands.

Furthermore, in its own independent study, Nokia Siemens Networks has analyzed the impact of an uplink LTE D block to the Public Safety broadband in a single mobile station – to – single Public Safety eNodeB setting. The overall objective of this study was to determine the statistical probability that the average desensitization (i.e., noise rise) at the Public Safety eNodeB would exceed 1 dB in the absence of a guard band. In this study, the analysis shows that overall there is less than a 2% probability that the average desensitization of the Public Safety eNodeB would exceed 1 dB.

Based on the numerous studies presented within 3GPP as well as independent studies that have been conducted within the company, Nokia Siemens Networks is of the opinion that a guard band is not needed between the D block and the Public Safety Broadband block.

The Commission tentatively concluded to adopt the OOBE limit specified in the *Waiver Order* for the nationwide public safety broadband network. Based on the aforementioned technical studies and measurements, which have concluded that the current OOBE limits are sufficient for protecting the Public Safety Broadband and D blocks, Nokia Siemens Networks agrees that these parameters provide adequate protection against harmful interference.

12. Applications[13]

Nokia Siemens Networks believes that the "applications" described here by the Commission are more appropriately viewed as services provided by a network. Internet and VPN access are fairly straightforward and easily implemented. For the remaining applications additional definition is required in order to specify exactly what they are and how they should operate. We see this as potential additional

[13] *Id.*, ¶¶55-57.

scope for the ERIC Public Safety Advisory Committee.

- Internet Access should be open to allow an agency to access whatever Public Safety users may need. There are standard requirements like firewalling and certain protocols that should be limited to ensure protection from typical attack vectors. The Internet Security environment changes on an hourly basis so the Commission should provide guidance that Security Best Practices should be used to protect Internet connected assets and access methodologies.
- VPN Access should be allowed as there are no limitation in the network that would prevent them. We believe that client based VPN's enable a users home agency to ensure that the users session is secure from end-user to the agency's security gateway. Agencies should be allowed to use the VPN technology and protocol that is best suited to their individual requirements. The LTE Network, when deployed with Transport Layer Security and the other 3GPP security mechanisms, provides a secure transport for user traffic. VPN's are not required between end users and the Core Network but Client VPN's are highly advisable for sensitive end user traffic.
- A status or information "homepage;" A set of guidelines and standard operating procedures must be developed to ensure that a user knows where to find the application and how to access it.
- Provision of network access for users under the Incident Command System A set of guidelines and standard operating procedures must be developed to ensure that a user knows where to find the application and how to access it.
- Field-based server applications A set of guidelines and standard operating procedures must be developed to ensure that a user knows where to find the

application and how to access them.

Nokia Siemens Networks encourages the addition of services like SMS, MMS, Location, Rich Communications, IP Multimedia Subsystem and Voice over LTE (telephony/PSTN) which mirror the existing functionality in wireless networks which commercial carriers will migrate to their LTE networks over the next several years. These services drive additional cost into the network which the benefits of may not outweigh the costs initially but the utility of which will greatly enhance the network over time. The omission of LMR Voice and other LMR technologies from these comments is not meant to detract from their importance; we see them as out of scope for Nokia Siemens Networks to respond to.

Application	**Currently Available**	**Interoperable**	**Mandatory**	**Comments**
Short Messaging	Yes	Yes	Yes	
Multimedia Messaging	Yes	Yes	No	
VoLTE (Telephony/PSTN)	Yes	Yes	Yes	Handset availability currently limits the commercial market
Location	Yes	Yes	Yes	Requires 3GPP Release 9 and UE Support
Rich Communications	Yes	Yes	No	
IP Multimedia Subsystem	Yes	Yes	No	

The Commission seeks comment on how it can promote the interoperability of key applications that are not included among the set of common applications that all public safety networks will be required to support. Nokia Siemens Networks encourages the Commission to utilize standards bodies like IETF, 3GPP and the Open Mobile Alliance, which work in concert to establish standards to ensure interoperability. Although 3GPP does not specify applications, the frameworks they define enable the network to host applications successfully. These bodies typically define interfaces as part of their standardization. We further believe that there is a need for a standards type organization that would govern Public Safety Applications with regards to interoperability.

14. Performance

Nokia Siemens Networks agrees that it is important to establish some common requirements for system performance based on the expected services and user mobility speeds. An efficient use of the radio frequency is determined in first instance by radio frequency (RF) planning, dimensioning, and SW functionalities that are able to adapt the system's behavior to changing load and radio conditions. To achieve this, performance recommendations need to be specified. However, there should be some form of accommodation in situations where performance recommendations cannot be met. Performance recommendations also enable Public Safety to properly compare vendors offerings against a known baseline so that competing offers are truly equivalent.

The requirements offered by the Commission in paragraphs 60-61[14] are reasonable for the expected performance of a 5MHz FDD LTE system. In the proposed values, the biggest constraint would be the uplink requirement of 256kbps at cell edge. This requirement usually determines the cell radius and inter-site distance, which will translate into the number of sites required for covering the target area. Sites required for coverage will typically dominate the cost of the network until load growth requires addition of extra sites to increase capacity. Using lower bitrate target for uplink would extend the maximum cell coverage and allow for less sites to service the same area (lower cost), but at the same time would reduce the cell's spectral efficiency and users performance at cell edge.

The main impact of not having a common baseline for service requirement would be higher probability of users falling into areas where the minimum performance is below its expectations. In the worst case, even risk of service unavailability.

It is reasonable and recommended to have a common set of minimum performance requirements among different public safety networks. Common performance metrics that may be used include user throughput, upper bounds on latency, network element availability, dropped call rate and successful call setup rate. This is a non-exhaustive list of performance metrics, and other metrics may be used to more

[14] *Id.*, ¶¶60-61.

completely quantify network performance.

In paragraph 62, the Commission says it seeks additional comments on these technical specifications. Are there additional requirements that should be included to ensure access to applications and other communications tools, which will enable interoperable public safety broadband networks nationwide?

- Quality of service (QoS) needs to be supported in all network elements to host various types of applications. Cell edge spectral efficiency or throughput should be defined for both uplink and downlink. Typically the uplink will define the design criteria of the network, but it is recommended to have a downlink target as well to ensure that system doesn't fail to provide downlink service level.
- Minimum bit rate at cell edge is typically used for design purposes. In addition certain coverage probability or confidence level typically is defined as well. This may change depending on the type of area (e.g. urban 95%, suburban 90%, rural 85%).
- It is recommended to measure spectral efficiency with users that have data to transmit available all the time (FTP or UDP continuous transfer). This generates a reference of what is the maximum capacity that the system can deliver, by ensuring that resources do no stay unused due to traffic not being available. Spectral efficiency obtained with any other application mix would be expected to result in lower values than the one obtained with continuous transfer. Users should be distributed around the coverage area, but some requirement about SINR (signal to interference and noise ratio) should be defined for every user or group of users, in order to have comparable results between different tests. The minimum number of users should be also defined and consistent among all tests.
- Coverage and throughput plots based on simulations are recommended as reference of the network design. Additionally certain minimum amount of drive test data would be necessary for verification of the design. It may be reasonable

to restrict the amount of drive test data required considering the cost that extensive drives generate.

- It is recommended to include information about site location in the maps.
- It is acceptable to use 70% loading per sector for design purposes. However, for testing and drive tests, the generation of load in the uplink for multiple cells may be difficult and costly. For this reason, Nokia Siemens Networks recommends to load the downlink up to 70% to perform testing and focus on downlink maps.
- 768 kb/s in downlink and 256kb/s in uplink for one user at cell edge are acceptable values for 5MHz FDD LTE system but please refer to our previous comment for additional discussion on the cost/benefits of providing 256kb/s in the uplink.
- Periodic reports based on agreed network monitoring key performance indicators (KPIs) should be provided. Updates on coverage maps should be provided at least whenever significant changes in network topology or configuration are implemented.

15. Network Capacity[15]

Nokia Siemens Networks believes that a minimum capacity for backhaul is a reasonable requirement for homogeneous performance over the public safety network. The strategy based on 3 times sector capacity per eNodeB in a 3 sector site could be used as minimum capacity requirement, as it leverages trunking efficiency between the 3 sectors. However, this method may fall short to ensure that individual cells' peak throughput can be achieved. This would limit the capability of the radio interface to demonstrate the maximum performance.

[15] *Id.*, ¶¶63-64.

In 5MHz FDD LTE with 2x2 MIMO, the peak throughput per TTI in optimal conditions is 36Mbps. Additional criteria for backhaul capacity could be to ensure that at least 1 sector in a 3 sector site can achieve the peak throughput when the other sectors in the same eNodeB are lightly loaded.

Interoperability may be affected by an under dimensioned system. This may cause dropped packets or excessive delays on different services. In addition to a minimum requirement for backhaul dimensioning, it is necessary to define certain procedures to monitor the KPIs that identify inadequate dimensioning (e.g. average backhaul utilization, peak backhaul utilization, percentage of dropped packets, latency, jitter, etc.).

16. Security and Encryption

As an initial matter, the Commission notes that according to LTE specifications five feature groups are defined.[16] However, Nokia Siemens Networks observes that the *Fourth Further Notice* appears to omit, presumably through an oversight, TS 33.401, clause 4, which reads "Network domain security (II): the set of security features that enable nodes to securely exchange signaling data, user data (between AN and SN and within AN), and protect against attacks on the wireline network." Nokia Siemens Networks would recommend that this be substituted for the current second bullet in paragraph 65 which may have been placed in the wrong section of the document.

The Commission seeks comment on its tentative conclusion that all three security features for the network access security, as specified in 3GPP TS 33.401, should be fully required.[17] Nokia Siemens Networks would recommend including Network Domain Security (NDS) based on 33.401. Note that the rules in TS 33.401, clause 12 (adds requirements for NDS in the user plane) are stricter than TS 33.210 regarding the interface between eNodeB and MME and should be followed. The use of 33.401 should be sufficient for NDS security.

In terms of optional features, the use of cryptographic protection on intra-domain (Zb) interfaces

[16] *Id.*, ¶65.

[17] *Id.*, ¶66.

is optional according to TS 33.210. The need for additional cryptographic protection depends on confidence in the physical security on intra-domain (Zb) interfaces and as such is optional.

The Commission asks if there would be any interoperability issues should the Commission choose not to require network domain security features, or to not select them.[18] Nokia Siemens Networks believes that there would not be any issues for communication inside a security domain (intra-domain). However, for inter-domain communication, 3GPP requires the use of a Security Gateway (SEG). 3GPP standard (33.210) requires that for communication between Security Gateways (SEG) in different security domains (inter-domain) IPSEC shall be used. There is a potential for interoperability issues if SEGs do not follow the mandatory features in TS 33.210.

The Commission asks whether it should adopt rules for application domain security.[19] Nokia Siemens Networks observes that in 3GPP standards, the area of reference to application domain security is limited to the USIM application Toolkit as stated in TS 33.102 and 31.111. Further comment and discussion regarding the scope for Application Domain Security should be facilitated with all stakeholders as part of a public safety applications standards body or forum.

17. Robustness and Hardening

The Commission seeks comment on whether it should require more or less than eight hours of back-up power to each eNodeB site within a public safety broadband network.[20] It also ask a series of related questions. Nokia Siemens Networks believes that backup power is essential for robustness and hardening and should be a requirement. At the same time, situations may arise that will preclude the deployment of either batteries or generators at some locations and this needs to be fully considered.

---

[18] *Id.*, ¶67.

[19] *Id.*, ¶68.

[20] *Id.*, ¶70.

18. Coverage Requirements[21]

The Commission seeks comment on its tentative conclusion that it should impose coverage and performance requirements on the networks that will comprise the nationwide public safety broadband network. Although Nokia Siemens Networks recognizes the need to provide as much coverage and capacity as possible, it believes that scenarios may exist where mandated coverage requirements will be costly and technically prohibitive for public safety broadband network operators. In these cases, some coverage may be better than none. To the extent that coverage rules are imposed, Nokia Siemens Networks encourages the FCC to provide an avenue for relief from requirements in situations where such requirements cannot be met without great expense or hardship.

19. Coverage Reliability[22]

Nokia Siemens Networks cautions that one size fits all requirements may not be the best approach when it comes to coverage reliability considerations. Each jurisdiction will have different challenges but technology may enable improving coverage and capacity. Even such diminished level of service is better than no service. To the extent that coverage rules are imposed, Nokia Siemens Networks encourages the Commission not to set hard requirements that do not account for unique challenges arising in each situation and providing flexibility for problem solving to occur within the public safety market that may markedly improve coverage reliability.

Nokia Siemens Networks agrees that coverage reliability is a reasonable criteria to ensure good coverage in radio networks. 95% cell coverage probability is commonly used for mature networks in dense urban and urban scenarios and seems to be a reasonable target. In Suburban scenarios, 95% to 90% could be used as well. In rural areas, this requirement usually is lowered to 90% or 85% in order to reduce the number of sites required for coverage. In general, increasing the cell coverage probability has the

[21] *Id.*, ¶¶71-73.

[22] *Id.*, ¶¶74-75.

impact of requiring shorter distances between sites and therefore increasing the overall cost of deploying the network.

Mounting the RF module on top of the tower (reducing the cable and insertion losses at the eNodeB), using 4 Receive Paths for uplink, the use of higher gain antennas and antenna tilting/azimuth optimization may help to improve coverage probability without adding specific indoor coverage solutions.

95% Coverage probability is a difficult target for indoor planning. Due to the particular characteristics of buildings (e.g. high rise buildings with multiple floors, thick concrete walls, underground locations, etc.), specific planning and solutions may be needed to achieve high probability indoor coverage. 95% Coverage probability will result in significantly higher costs. Nokia Siemens Networks would encourage the Commission to let individual public safety jurisdictions perform the cost benefit analysis for indoor coverage.

B. Public Safety Roaming on Public Safety Broadband Networks

Nomenclature

The Commission proposes and seeks comment on a definition of a 700 MHz public safety roamer and broadly dividing intra-system public safety roamers into three categories based on the nature of their mission: "itinerant roamers," "interoperability roamers," and "response roamers."[23]

Nokia Siemens Networks agrees that the three categories cover normal uses cases for public safety user movements. The 3GPP definition of a roamer may also need to be considered at least in order not to have confusion between the public safety roaming use cases versus the physical act of roaming.

A 3GPP roamer is a user which has moved from his/her own home PLMN to visited PLMN. Normally, access to the visited PLMN is facilitated by a pre-existing roaming agreement between the two networks. This establishes the user's ability to access the physical radio and data transport resources of

[23] *Id.*, ¶87.

the visited network including resources in the home network. If there is a single PLMN over multiple networks there is no 3GPP concept of real roaming as the user is still within the home network. Of course, the network can be configured to limit user access to geographical areas if desired. Subscriber priority is configurable in the subscription profile which is used for police enforcement both on the home network and for roamers (visited PLMN) there are multiple methods to control priority access.

The one expected difference between an itinerant and interoperability roamer versus a response roamer is the need to access incident management applications in the visited network which is outside of the 3GPP network domain. This scenario may also come up within a single PLMN network depending on where the service is hosted. Roaming or intra-network movement from the 3GPP domain is built into a normal network deployment. Access to services which are in different local IT networks need to be considered as well especially in for response roamers.

Interoperability and roaming (if needed, more than one PLMN) for public safety whether it be inter-system or intra-system is beneficial for the future of public safety users. Existing network constructs easily allow for interoperability which public safety should follow.

1. Prioritization and Quality of Service to Support Roaming

The Commission seeks comment on public safety needs and standards for prioritization in the context of public safety intra-system roaming.[24] Nokia Siemens Networks believes that the means of providing differentiated prioritization as provided by LTE (Allocation and Retention Priority (ARP) and Access Class barring) allow a wide range of flexibility in the use of these mechanisms. However, especially in roaming situations, it is important that those mechanisms are applied in a consistent manner across networks. In commercial networks, application of those mechanisms would typically be subject to commercial negotiations between operators leading to roaming agreements. However, this open process does not ensure such agreements will be successfully negotiated between all network operators, so that the ability to roam into any other network and receive consistent service in a visited network is not

[24] *Id.*, ¶90.

ensured. Based on the requirements set for roaming between public safety networks, this seems not acceptable. Therefore, it seems advisable to establish a nationally applicable prioritization scheme for all regional public safety broadband networks. A body representing relevant stakeholders from all levels, i.e. federal, state, regional, local and tribal governments as well as relevant industry representatives would appear to be the appropriate entity to define such a nationally applicable prioritization scheme. The Emergency Response Interoperability Center (ERIC) could be a suitable body.

The Commission seeks comment on when a prioritization scheme should be triggered and related issues.[25] Nokia Siemens Networks observes that, from a technical perspective, the two prioritization schemes considered need to be discussed separately. The Allocation and Retention Priority (ARP) scheme is a mechanism that gives operator policy guidance to network nodes that allows them to autonomously react to high load conditions that may potentially impair their proper operation while respecting operator policy. Thus, for this scheme, it seems that no explicit external trigger is needed. This is different for the Access Class barring mechanism, which requires explicit operator intervention to set the desired prioritization level. In this case, it seems useful to define a standard nationally applicable prioritization trigger mechanisms for all regional public safety broadband networks. The rationale for this is that while many incidents of smaller scope would typically affect only a single regional public safety broadband network, larger incidents spanning more than a single regional public safety broadband network would require consistent triggering of the prioritization mechanisms. While this can of course also be achieved by coordinating the activation of regionally applicable prioritization trigger mechanisms for the regional public safety broadband networks, this introduces an additional layer of indirection. Avoiding this removes a potential source of inconsistency in the activation of the prioritization trigger mechanism. The timing of the trigger mechanism should be determined by the authority initially assessing an incident and coordinating the initial response. Similarly, the initiation of the trigger mechanism should be possible for any authority involved in initially assessing an incident and coordinating the initial response, as well as any authority that may be responsible for coordinating the incident response beyond the initial response.

[25] *Id.*, ¶91.

In line with this, it seems useful to have a sliding scale of authority based upon the extent of the network being put under a prioritization scheme, similar to the sliding scale of authority defined for coordinating the incident response and resource deployment in that context.

The Commission seeks comment on the adoption of a standardized QoS scheme for all regional networks.[26] In order to properly support the applications that will be required to be supported also in roaming situations, Nokia Siemens Networks believes that it is advisable to define a minimum QoS level to be provided for each application that is nationally applicable. This does not prevent regional networks from choosing to implement support above this minimum level thus allowing flexibility for individual regional control over QoS (though it depends on the type of application and the QoS level defined for it whether providing higher QoS than defined is useful, e.g. applications requiring Guaranteed Bit Rate type QoS often do not benefit from providing such a Guaranteed Bit Rate above what is specified by the application). Roamers would request the level of QoS based on their subscriber information available in their home network. Through defined interfaces, the visited network can modify this level to the locally applicable QoS level, which per nationally-applicable QoS scheme defined as discussed above would ensure the minimum level of QoS capability for the roaming user.

2. Applications to Be Supported for Roamers

The Commission tentatively concludes that public safety broadband networks must support the following five applications to intra-system roamers: (1) Internet access; (2) VPN access to any authorized site and to home networks; (3) a status or information "homepage;" (4) access to responders under the Incident Command System; (5) and field-based server applications.[27] Nokia Siemens Networks believes that both Internet and VPN Access are relatively simple to provide and there is little network information needed by the roaming user to make full use of the service. The remaining applications require

[26] *Id.*, ¶92.

[27] *Id.*, ¶93.

considerable information from the visited network to enable the roaming user to utilize these services. For example, a user would have to know how to access a field-based server or the Incident Command System to include such details as IP address, access protocol and authentication credentials. At a very high level, these applications are a good idea, but more work must be done at a deeper technical level to specify what exactly these applications are. Otherwise these applications will not gain universal acceptance and interoperability.

D. Testing and Verification to Ensure Interoperability

1. Conformance Testing

The Commission tentatively concludes that it should require that all user devices be subject to conformance testing and seeks comment on its tentative conclusion.[28] Nokia Siemens Networks observes that device interoperability is based on industry wide principles and standards. Nokia Siemens Networks, like other vendors, develops its own test cases and specifications that use 3GPP conformance testing as a guideline.

The Commission also seeks comment on conformance testing for LTE infrastructure equipment.[29] Nokia Siemens Networks observes that there is no conformance testing with certification for network infrastructure equipment beyond normal regulatory conformance requirements which equipment is tested to at FCC certified labs. Network infrastructure vendors participate in bi-lateral testing with each other and with device vendors to verify interoperability and software release regression testing, and in operator lab testing of network elements. Infrastructure vendors have formed the Network Vendor Interoperability Testing Forum (NVIOT) to identify common IOT methods and procedures to improve the IOT process. NVIOT creates master test catalogs which contain the possible IOT environment tests for interfaces including LTE networks. Nokia Siemens Networks support the PSCR process for testing network

[28] *Id.*, ¶106.

[29] *Id.*, ¶108.

equipment and the issuance of conformance certificates for tests which are agreed to by the industry and public safety as relevant for use in public safety systems.

2. Interoperability Testing (IOT)[30]

Nokia Siemens Networks operates in accordance with industry wide accepted principles in verifying interoperability. Nokia Siemens Networks additionally uses a process with elaborate attention to quality which includes in depth analysis, planning and implementation tied to the product life cycle. Nokia Siemens Networks agrees with those parties who have stated that self-certification is sufficient, as noted by the Commission. While we understand the concern about compromises to interoperability resulting from a vendor's desire to differentiate, a focus on 3GPP requirements and specifications should address this. We believe that most vendors adhere to these standards as a baseline and hence self-certification through existing interoperability procedures should suffice.

The Commission tentatively concludes that it should require that public safety broadband networks perform IOT for the LTE roaming interfaces identified in the *Third Report and Order*.[31] Nokia Siemens Networks observes that the listed interfaces are all standard LTE interfaces that are 3GPP based and compliant. IOT requirements for these are generally accepted and considered valid by all major network suppliers including Nokia Siemens Networks.

In the case of LTE-LTE roaming S6a, S8 and S9 are the main interfaces as identified by the Commission. The costs and benefits of testing each combination of interfaces will vary based on the number of vendors involved.

The Commission asks whether it should adopt IOT rules to ensure multi-vendor interoperability on public safety broadband networks.[32] Nokia Siemens Networks acknowledges a need for IOT for public

---

[30] *Id.*, ¶¶109-115.

[31] *Id.*, ¶110.

[32] *Id.*, ¶113.

safety broadband networks. The interfaces listed by the Commission represent the main ones requiring IOT. All major vendors perform IOT in adherence to industry wide principles. Nokia Siemens Networks is an active participant of the NVIOT forum jointly with other vendors to determine and develop best operating practices and 3GPP compliance and specification development.

Nokia Siemens Networks has dedicated IOT labs in multiple locations in Nokia Siemens Networks facilities. These are used to perform device as well as Network IOT. While public safety access to multi-vendor labs can be designated, it is Nokia Siemens Networks' recommendation that if this indeed is the chosen approach, it be standardized or set under the oversight of one body. The greatest benefits in terms of contributions to such a process, where needed from the infrastructure vendors, likely comes from vendors on the basis of joint planning efforts.

Nokia Siemens Networks supports an independent laboratory environment such as the PSCR facility and the Idaho National Laboratory. From our own experience/investigation both appear to have the facilities (physical as well as RF environments) to conduct testing on a regular basis. It is our belief this should be funded from the Public Safety Community and/or from a Federal body like ERIC.

3. Interoperability Verification[33]

In addition to IOT testing, device and infrastructure vendors perform their own internal tests in order to bring a mature product to IOT. Operators may also have acceptance testing procedures in place. Field testing and First Office Application(FOA) testing are also commonly performed by carriers.

The use of federal laboratories like NIST/PSCR and the Idaho National Laboratory for FOA could be supported as a second phase to IOT. For example, the INL range has the large unencumbered real estate to support FOA activities emulating incident scenes and could provide real-world environments from which FOA testing could verify compliance with the technical requirements of a nationwide network.

[33] *Id.*, ¶116.

E. Other Matters Relevant to Interoperability on Public Safety Broadband Networks

1. Network Operations, Administration and Maintenance

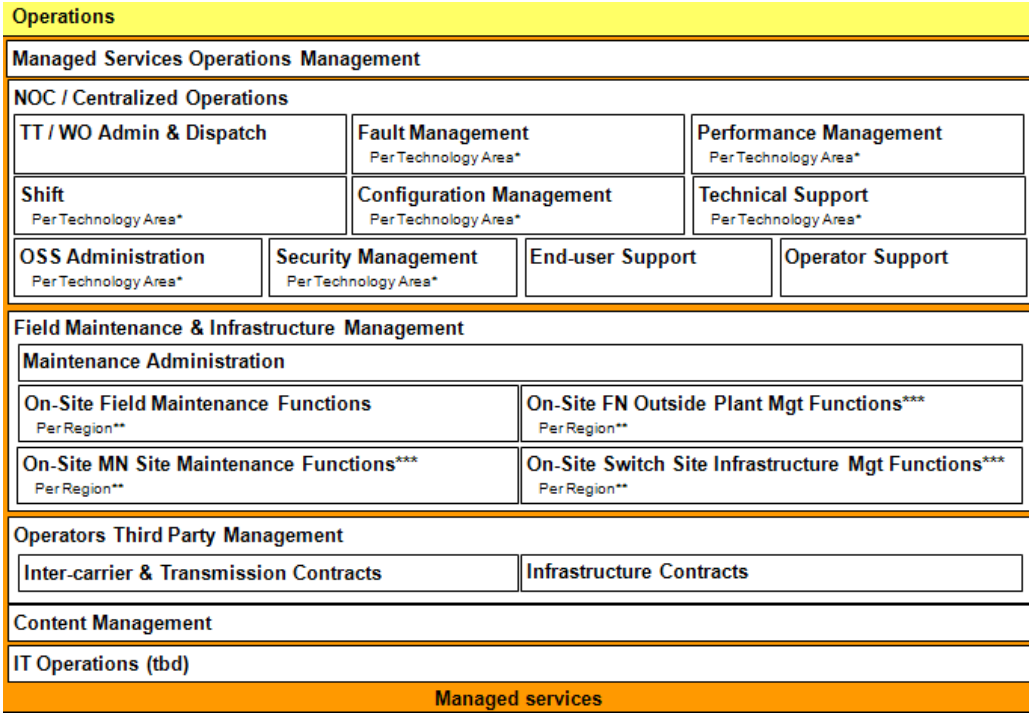
The Commission seeks comment regarding the operational capability, if any, that should be required in order to maintain and enhance interoperability.[34]

Nokia Siemens Networks employs an operational model that to some extent is technology agnostic since the functions and activities are the same, only different once at a network element level. The difference at this level is only what specific actions are taken to accomplish a given operational activity, such as system administration, corrective maintenance, preventative maintenance, etc.

It is not necessary that special requirements be imposed in order to manage the broadband public safety network. Nokia Siemens Networks uses a standard operations model based on the enhanced Telecom Operations Map (eTOM), published by the TM Forum, for all of its telecommunications operational service deliveries. The same operational model could and would be used as the foundation to create a model specific to the local public safety requirements.

The following is a highlight on the model NSN leverages as a common foundation to create operations per customer / entity requirements:

[34] *Id.*, ¶117.



In summary, Nokia Siemens Networks suggests that a common model that allows an operational structure/organization to be able to have inherent interoperability across networks can be utilized in the public safety broadband realm. The solution or technology itself does not drive the common model or approach.

3. Devices [35]

The Commission seeks comment on whether public safety LTE devices should be required to support 1.4/3 MHz channel bandwidth in the public safety broadband spectrum.

Nokia Siemens Networks observes that applications for less than 5 MHz bandwidth user equipment are for mobile operators with limited initial spectrum for LTE services typically resulting from their transition from legacy technology to LTE. In addition, less than 5 MHz bandwidths carry significant control channel signaling overhead versus user payload. Mandating other bandwidths for the public safety band would add testing and development costs where there is no benefit for the public safety band

[35] *Id.*, ¶¶119-122.

itself. 3GPP has removed some of the mandated channel bandwidths allowed for particular bands to reduce testing complexity and development costs.

The market is best suited to decide what is commercially viable and technically possible over a period of time related to band support and multimode support. The device ecosystem for public safety will be much wider than in the past with examples ranging from embedded car modems to handheld cell phone like devices. The use cases and volume of devices along with the continual development of technology determine what is possible to support.

In terms of Band Class 14 support, Nokia Siemens Networks believes that from a practical perspective, treating the full ten megahertz in Band Class 14 upfront is prudent. Ultimately the market will decide what bandwidths and combinations of bands are included in public safety devices based on the networks ultimately available to public safety users.

4. In-Building Communications[36]

The Commission tentatively concludes that it should adopt a framework to achieve in-building coverage and seeks comment on the issues involved.

Nokia Siemens Networks reports that an in-building penetration margin similar as in a narrowband system should be considered for wideband design. The in-building penetration loss depends on the type of building and is typically assumed different for dense urban, urban, suburban and rural areas. In addition, particular characteristics of buildings (e.g. high rise buildings with multiple floors, thick concrete walls, underground locations, etc.), may require specific planning and solutions to achieve high probability indoor coverage. This may result in higher costs.

To answer the question of whether the lack of such margins will lessen the effectiveness and safety of emergency responders, Nokia Siemens Networks believes it is similar to narrowband services. If these margins are not considered for network design, the coverage probability on indoor locations will be

[36] *Id.*, ¶¶123-126.

reduced.

Nokia Siemens Networks offers that not having building penetration margins in the design may result in higher need of specific indoor coverage solutions, or later addition of sites which might result in additional cost at later stages of network deployment.

For situations where in-building communications may be blocked due to specific circumstances, emergency teams could have directive antenna devices which would help to increase the coverage over baseline design criteria, or specific devices such as relays could be used to temporally increase the indoor coverage on target building. Relays are an LTE Advanced, Release 10 option, which might help in these situations. A portable relay device that is deployed in emergency situation next to a window would give better coverage within a building. Even an emergency vehicle could be equipped with its own relay and directive antenna that can be pointed to the side of the building. This would require some self organizing networks (SON) features for auto-configuration, etc. Indoor coverage could be increased when there is need for it in an emergency situation, without having to impose additional requirement over all buildings.

Using increasing margins for design will result in shorter distance requirements between sites and a denser network. Initial cost will be increased due to the need for more sites to cover the same area. This cost may be partially compensated over time in high loaded areas, as fewer sites are needed to grow network capacity. It should not have any effect on borders between different jurisdictions. In any case some coordination between jurisdictions will be required to configure handover settings.

The Commissions asks how public safety may best take advantage of Distributed Antenna System approaches. Nokia Siemens Networks believes that Distributed Antenna Systems are a good solution for indoor-coverage, and Public Safety should use them wherever they are available and coverage is needed. Deployment must be evaluated on a case-by-case using established criteria to classify the benefit of coverage in certain areas or in buildings versus the cost of having a specific indoor solution.

Exhaustive certification of in-building coverage could be a very costly and slow process. A combination of outdoor data rate maps and selection of critical indoor locations may be used to keep a reasonable cost.

It might seem like a reasonable requirement to have a target data rate to the first wall. However, within complex buildings meeting such criteria beyond the first walls may be impossible. Additional indoor coverage solution (permanent or temporal) may be required in some cases even if this criteria is met. Advanced technology like relays and directive antennas could be deployed specifically for incidents.

6. Operation of Fixed Stations and Complimentary Use of Fixed Broadband Spectrum

The Commission tentatively concludes that it should allow public safety to operate fixed services in this band on an ancillary basis.[37] Nokia Siemens Networks believes that is reasonable that fixed services may co-exist if planned for in a limited use scale with high directional beams being deployed. The actual amount of interference will reduce the quality and coverage of the public safety user's experience especially at the cell edge. Nokia Siemens Networks would not recommend ancillary use other than in a coordinated fashion as with LTE relays. However, fixed stations as complimentary users of an existing LTE network are not expected to create potential interference issues.

8. Public Safety Broadband and Next-Generation 911 Networks[38]

Nokia Siemens Networks believes that interconnection between public safety and NG911 networks would be a natural progression of moving to an all-IP based system. Cooperation between ATIS (Alliance for Telecommunications Industry Solutions), NENA (National Emergency Number Association) and public safety organizations should be encouraged in order to create an interoperability environment to connect 3GPP based networks with NG911 and public safety systems.

---

[37] *Id.,* ¶129.

[38] *Id.,* ¶133.

F. Section 337 Eligible Users [39]

Nokia Siemens Networks agrees with the Commission that it should pursue the goal of allowing such appropriate secondary users access to the interoperable public safety broadband network. There are secondary users with mission critical communication needs. They may be first responders in some emergencies and must have interoperability with public safety officials in order to "protect the safety of life, health or property." Moreover, through expansion of the user base, even on a secondary basis, there are significant advantages that would accrue to public safety. The expanded user base will enable a more diverse user equipment ecosystem, greater access to financial resources to build and operate the network and a larger set of services that can be utilized on the network.

In terms of the Commission's questions around limiting secondary use and priority of access, Nokia Siemens Networks encourages the Commission to require the use of the features and functionalities in 3GPP Release 8 which provides a robust set of QoS control, preemption and prioritization features. These features will ensure that the network can automatically provide control of secondary users.

The Home Subscriber Server in 3GPP Release 8 compliant network controls who is an authorized to attach to and utilize the network. If the user does not have a valid subscription, they cannot use the network. In roaming scenarios, the user must have a subscription in an HSS and a roaming agreement must exist between the visited and home network. This network functionality ensures that the network owner has control of who is authorized to use the network.

Secondary users should only be considered as a tenant or user on an existing Public Safety Broadband Network rather than a user of spectrum on a secondary basis. In situations where the secondary user would fund and deploy a Public Safety Broadband network and therefor be the defacto owner of the network, they will do so with the understanding and requirement that their users are

[39] *Id.*, ¶¶134-140.

secondary on the network.

The public safety broadband network is going to have ongoing and substantial operating cost requirements. The public safety community and many policy makers share concerns over how these obligations will be met. There are possibilities to assist in this process enabled by secondary users. For example, a monthly fee for service is a tried and true business model even for current public safety communications systems as well as the use of a commercial network for public safety. We would expect the primary users on these networks to continue to help defray the operational costs through monthly fees in jurisdictions that decide to use this model. Secondary users should be held to the same standards for cost recovery. If the set of secondary users are well defined and the general public is not considered as a valid secondary user then the fees should be deemed as acceptable. Any funds received should be for the support and enhancement of the public safety broadband network.

Secondary users should only be considered as a tenant or user on an existing Public Safety Broadband Network rather than a user of spectrum on a secondary basis. In situations where the secondary user would fund and deploy a public safety broadband network and therefore be the *de facto* owner of the network, they will do so with the understanding and requirement that their users are secondary on the network.

III. CONCLUSION

As the Commission continues its exhaustive effort to ensure the realization of a nationwide, interoperable public safety broadband network, Nokia Siemens Networks respectfully requests consideration of its views expressed above. Nokia Siemens Networks applauds the Commission for driving an open standards, industry driven approach to making the network a reality. The Commission should work to finalize the principles and guidelines that will establish the framework, and then continue in an oversight role as the public safety community and telecommunications network suppliers roll out the networks that will help improve the safety and well-being of all Americans.

Respectfully Submitted,

Nokia Siemens Networks US LLC

/S/ Derek Khlopin

_____

Derek Khlopin
Head of Government Relations
North America

Brian Kassa
Head of Technology, Public Safety Broadband

Ajit Kahaduwe
Head of Industry Environment
North America

Nokia Siemens Networks
1401 K Street, NW
Suite 450
Washington, DC 20005

April 11, 2011