Comments of Nokia Siemens Networks US LLC

Nokia Siemens Networks US LLC (“Nokia Siemens Networks” or “NSN”), a global provider of mobile communications network solutions and services for the commercial and public sector markets, hereby submits comments in response to the Notice of Inquiry (NOI) referenced above. Nokia Siemens Networks applauds the Board of Directors of the First Responder Network Authority (“FirstNet”), and NTIA as its agent, for taking this important step of soliciting input from all interested parties on network architecture, deployment and other aspects of the nationwide Public Safety Broadband Network that the U.S. Congress has directed FirstNet to design, build and operate. Nokia Siemens Networks requests consideration of its views expressed herein.

Respectfully submitted,

Bob Fennelly               Chris Stark
Head of Government and Public Safety       Head of Business Development, North America
Robert.Fennelly@nsn.com       Chris.Stark@nsn.com

Derek Khlopin               Brian Hendricks
Head of Government Relations       Head of Global Technology Policy
North America               Brian.Hendricks@nsn.com
Derek.Khlopin@nsn.com

November 8, 2012
Executive Summary

Commercial LTE networks in the United States are some of the most advanced in the world. The coverage and capacity offered by wireless operators is growing rapidly and customer satisfaction metrics are high. Existing commercial LTE networks are built to commercial grade, with high availability and reliability, which could meet the normal day-to-day operational needs of the Public Safety user community (first responders). However, the FirstNet network will be required to continue to operate under exceptional circumstances.
With this context, the FirstNet Board of Directors (“FirstNet Board”) should look at the availability and performance needed by Public Safety users to operate during wide scale natural disasters such as hurricanes or earthquakes as well as potential man made events. Nokia Siemens Networks believes that the true test of the FirstNet network will be measured during such times and first responders, who will be reliant upon this asset, will be the judge of the success of the network.

The FirstNet network needs to be designed for “disaster” level operational capabilities in addition to supporting the day-to-day operational needs of first responders. We believe that defining this disaster level operational capability will drive many important decisions for this network. It is with this in mind that Nokia Siemens Networks urges the board to ensure that the FirstNet network is what the user community (first responders) needs and can depend upon.

Nokia Siemens Networks believes that the inherent tradeoffs between functionality, performance, and cost need to be addressed prior to the commencement of the network build and will ultimately affect the overall design and implementation of the network architecture.

Examples of such tradeoffs include:

- Network restoration times where spares, manpower, redundancy and location are key cost drivers.
- Coverage, where the sparsity of population has made it impractical to establish commercial network infrastructure. Commercial networks are designed to maximize coverage of population and not land mass.
- Survivability, where both redundancy and hardening need to play a part.
Security levels that are engineered into the system design will dictate the usage by different agencies.

These are examples of a potential divergence between the design and performance of commercial networks and the defining characteristics of a truly successful Public Safety network that FirstNet is charged under the law with deploying and operating. Clearly, and for well understood reasons, commercial networks are driven by the economic realities of their commercial subscribers and the tolerance of their end-user base to degraded performance under fault scenarios.

These are not the only factors Nokia Siemens Networks believes that the FirstNet Board should take into account when planning the network. We also see the need for emphasis to be placed on the following areas:

- Applications that will enable users to gain full benefit from the network.
- User profiles, pre-emption, priority access.
- Use cases under which the network will be loaded.

Nokia Siemens Networks shares the FirstNet Board’s view that the deployment planning process should begin quickly and network construction can, and should, commence soon thereafter. To this end, we believe that the expertise needed to plan and drive this process forward can be found in a number of established government contractors or system integrators.
**NSN Recommendations:** Nokia Siemens Networks believes that the optimal path forward consists of a proper blend of leveraging existing Public Safety network assets (towers, backhaul, right of ways, etc.), commercial carrier assets, and dedicated FirstNet assets. Nokia Siemens Networks recommends the following processes:

- Solicit a prime contractor for the overall network, the requirements for which are likely to be met only by entities with large scale systems integration expertise and experience.

- Build a user specification in conjunction with the Public Safety community and the Broadband Working Group of the National Public Safety Telecommunications Council (NPSTC).

- Commence the planning and build for a dedicated core network with built in Public Safety requirements, a platform for applications, and a single subscriber database. Provide early access to this functionality for users through roaming agreements with national/regional/rural carriers.

- Commence the planning and implementation of the radio access network (RAN) after soliciting the proper level of inputs from the States. Start a procurement process that leverages all available network assets in the market (Public Safety/government, utility, carrier) to minimize capital expenditures (CAPEX) and improve speed of deployment with an emphasis on maximizing usage of existing Public Safety sites to minimize operating expenses. Nokia Siemens Networks believes that experienced system integrators are well suited to work with existing assets across the nation in the most efficient and economical approach to building out a secure and effective access method to the Public Safety core network. These procurements should be
run at either a regional or State level and should include design, deployment and operation.
Network equipment procurements should be run separately, although close cooperation between the FirstNet Board and any integrators fulfilling the above role will be critical.

Importantly, as discussed in detail below, Nokia Siemens Networks does not believe it is necessary to “share” the existing radio access network (eNodeB) assets of commercial carriers with the funding provided. Sharing radio network assets will be difficult technically, complicate efforts to provide a secure solution, and in our view conflicts with a core principle of the law, building a separate dedicated network for Public Safety. Nokia Siemens Networks believes that following the foregoing recommendation to utilize a system integrator(s) and a transparent, competitive selection process for the core and radio network elements, while leveraging essential physical infrastructure of commercial carriers, Public Safety, and others, will result in an affordable dedicated network for Public Safety that avoids the concerns of sharing network elements.

I. Introduction

Nokia Siemens Networks is a leading global provider of mobile communications network solutions and services for the commercial and public sector markets. NSN is utilizing its mobile broadband expertise to help network operators in the United States and around the world deploy and operate networks based on 4th Generation Long Term Evolution (LTE) technology. NSN’s leadership is demonstrated through 67 current commercial LTE contract awards. NSN was the first to complete an end-to-end LTE call, and more recently set a new benchmark by demonstrating an LTE-Advanced session connecting at 1.6 gigabits-per-second (Gbps).
Nokia Siemens Networks aspires to leverage our LTE solutions, expertise and real-world network deployment experience to assist in the realization of a nationwide state-of-the-art, dedicated LTE network for first responders. Our investment toward this initiative and our collaboration with the wide range of interested stakeholders has spanned many years as we have eagerly anticipated the scaling up of the deployment of such a network.

The Public Safety community has long and desperately called for mobile broadband in support of its most important mission of saving lives. NSN has been involved every step of the way – helping to match the community’s requirement descriptions with the corresponding technical solutions. NSN advocated alongside the Public Safety community and at the FCC and the Departments of Commerce and Homeland Security for the selection of LTE as the foundational technology that would bring interoperable mobile broadband to first responders for the first time. Moreover, the rapidly blossoming global LTE ecosystem would mean that, so long as its use by Public Safety remained aligned with the global commercial market, Public Safety would receive the enormous benefits being realized on the commercial side – economies of scale that would lead to better prices and a competitive supply of network and terminal equipment that would enable state-of-the-art communications capabilities in the field. The use of LTE will foster a new paradigm of application development for the Public Safety network that will bring new innovative ideas into the fold.

Nokia Siemens Networks is an active partner with the array of government agencies and initiatives underway in this space. NSN sat on the FCC’s Emergency Response Interoperability Center (ERIC) Public Safety Advisory Committee, and co-authored the Interoperability Working Group’s contribution to the committee’s final report. With NIST’s Public Safety Communications Research
Program (PSCR), NSN became the first radio access network (RAN) supplier to pass initial stages of phase 3 interoperability testing and participates in various working groups. NSN also is active in NPSTC and FEMA working groups. NSN has long been an active participant, and in many cases a driver of, standards activities around public safety broadband, including the Third Generation Partnership Project (3GPP), the Alliance for Telecommunications Industry Solutions (ATIS), the Telecommunications Industry Association (TIA), and the MultiService Forum (MSF).

Nokia Siemens Networks meanwhile has forged ahead with the development of products and solutions for the Public Safety broadband market. NSN was the first RAN vendor to make available a 3GPP Band Class 14 eNodeB LTE module. NSN has proceeded to trials and pilots of LTE for Public Safety across the United States, including in Miami/Dade County, Florida; Las Vegas, Nevada; and Dallas-Fort Worth, Texas. A milestone for the entire Public Safety broadband network effort was achieved during the Republican National Convention in Tampa, Florida, when NSN and partners deployed a pilot network that represented the first instance of a truly multi-vendor, interoperable network with live Public Safety users.

Now, as FirstNet moves closer to reaching important milestones in its process, we greatly appreciate this opportunity to provide comment on the initial conceptual network architecture presentation offered at the FirstNet Board meeting on September 25, 2012. Moreover, we are pleased to offer our own recommendations as the NOI invites.

Nokia Siemens Networks holds a number of core beliefs regarding how the new nationwide Public Safety Broadband network should be deployed and operated that completely align with the
statutory provisions of the monumental legislation authorizing the network. After incredible effort by many, Congress passed, and the President signed, a law making clear its intent that, at last, Public Safety would get a dedicated, state-of-the-art LTE mobile broadband network. In addition to the economies of scale that would accrue from the use of the global LTE standard, further efficiencies would be gained by the sensible leveraging of commercial infrastructure where feasible and where Public Safety’s specific requirements could be supported. Congress very importantly also envisioned a dynamic and competitive market for the supply of network equipment, devices and applications for the network, again reflecting an appreciation of the commercial environment and its contrast with the history of the Public Safety equipment market. Taken together, these considerations lead Nokia Siemens Networks to recommend that FirstNet ensure that an independent radio access network is procured and built for Public Safety users, which leverages public and commercial site infrastructure where possible to locate this equipment. Nokia Siemens Networks further elaborates on this recommendation and these important considerations below.

II. Clarifying the Legislative Direction Regarding a Network for Public Safety

Suggestions have been made that a “standalone” network for public safety would be counter to the law, and that legislative direction to leverage existing infrastructure is a requirement to share existing commercial carrier network core and radio network elements. The term standalone network connotes a circumstance in which core and RAN elements separate and distinct from commercial carriers would be deployed and totally separate (from commercial wireless providers) physical infrastructure such as buildings, power supplies, towers, rooftop arrangements, and backhaul would also be constructed. NSN agrees that this framework would run counter to the law, which
provides clear direction to utilize the physical infrastructure of commercial providers and other entities, and would also be unaffordable. NSN believes, however, that the statute does not preclude a core and RAN for Public Safety that is distinct and separate from commercial networks. On the contrary, providing a separate core and RAN for Public Safety is a requirement of the Act, and as NSN points out in the subsequent sections of these comments, is affordable with the funds available.

The Middle Class Tax Relief and Job Creation Act of 2012 (“the Act”) provided that “the First Responder Network Authority (“FirstNet”) shall ensure the establishment of a nationwide, interoperable public safety network.” The Act further detailed that this network would include a network core that includes national and regional data centers and connects to public networks as well as a radio access network (RAN). Far from prohibiting the construction of a separate, dedicated “network” for public safety, the Act actually requires FirstNet to ensure that such a network for public safety is developed. The language is unambiguous in its requirement for a separate core and RAN for public safety. This understanding is consistent with the expectations of the Public Safety community and lawmakers at the time of the Act’s passage. NSN agrees with the comments submitted by RCC Consultants that the statute does not prohibit a dedicated network for Public Safety, or necessitate a “network of networks” approach. In NSN’s opinion, suggestions that both the physical infrastructure of wireless carriers (such as back haul, towers, rights-of-way, conduits, power supplies, etc.) and the actual core and RAN elements of those carrier networks needs to be shared under the statute are incorrect.

1 See P.L. 112-96 § 6202.
As noted in subsequent sections, Nokia Siemens Networks believes that there are technical and economic challenges related to any effort to share core and RAN assets between commercial providers and public safety. This includes entirely different user expectations about the availability and reliability of the network and associated failure tolerances. Domestic commercial carriers have done an exceptional job deploying best-in-the-world networks, appropriately engineered to meet the threats they face and user expectations. However, past experiences with major storm events and other outages illuminate the biggest challenge in attempting to share network elements. It is in these moments where public safety and the public at large must know that the network will not fail. Even the best commercial networks would require considerable effort and cost to provide the necessary assurance. NSN believes that this is a major reason that Public Safety has consistently expressed the need for a dedicated network, and why Congress provided the directive for FirstNet to plan and deploy such a dedicated network. Consider that the language of the Act authorizes FirstNet to assess and collect fees, for among other things, “access to or use of any equipment or infrastructure, including antennas or towers, constructed or otherwise owned by the First Responder Network Authority. . .”.\(^3\) Congress would not have included this provision if FirstNet were precluded from owning network elements and infrastructure that is independent of commercial provider networks. The need for a dedicated network, the challenges in attempting to share network elements, and the language of the Act make clear that FirstNet can, and indeed should, plan and deploy a separate and dedicated core and RAN for public safety.

\(^3\) P.L. 112-96 § 6208(a)(3).
NSN believes that confusion about the statutory requirements regarding the deployment and ownership of network element assets emanates from numerous provisions directing FirstNet to leverage existing infrastructure. In particular section 6206, at several points, directs FirstNet to “leverage existing commercial wireless infrastructure to speed deployment” and to ensure that proposals “include partnerships with commercial mobile operators to utilize cost effective opportunities to speed deployment in rural areas.” It is important to note that these directives exist against the backdrop of section 6206’s “duty and responsibility to deploy and operate a nationwide network.” The clear implication of the Act’s directives is for FirstNet to seek opportunities to leverage infrastructure (buildings, towers, attachment points, conduits and where available backhaul and power supplies) of commercial providers to reduce the cost of construction and ongoing maintenance and operation of the network. Sharing of these physical infrastructure components allows FirstNet to also speed deployment by locating dedicated public safety equipment at existing physical sites to take advantage of existing tower leasing arrangements, and other structures, of commercial carriers.

NSN agrees with taking full advantage of these resources, and suggests that FirstNet should think as broadly as possible, including the use of utility sites, state, local, tribal and federal infrastructure, and public safety assets in addition to the physical infrastructure of commercial providers. However, that is a wholly separate issue from sharing the physical network elements of the commercial networks; something that NSN believes is neither authorized nor envisioned by the Act.
III. Network Deployment

The deployment by FirstNet of the nationwide Public Safety Broadband network is a complex endeavor that requires a thorough analysis of all options available, the advantages and disadvantages of these options, and their cost implications. The presentation made to the FirstNet Board on September 25th lays out the vision of a FirstNet Nationwide Network (FNN) that is based on leveraging the existing commercial wireless carrier networks to provide ubiquitous, reliable and redundant coverage. NSN sees merit in this vision, but reserves judgment on the ability of this architecture to meet the statutory requirements of a network dedicated to Public Safety. NSN has been a worldwide leader in deploying 3rd generation (UMTS/CDMA) and 4th generation (LTE) mobile broadband technology in both green field (new) and legacy (existing) networks. Utilizing this experience and knowledge base, NSN has put together an analysis of options for FirstNet.

Core Network: Nationwide Distributed Core

Nokia Siemens Networks agrees with the FirstNet Board, and specifically the FNN conceptual presentation, concerning the importance of the core network and an associated Service Delivery Platform. NSN believes that establishing a well designed, distributed core network that is fully under the control of FirstNet or FirstNet’s designated agent will be a key to FirstNet’s success and achieving the interoperability that Public Safety has been waiting so long to achieve.

The core should be:

1. Procured by FirstNet, potentially with assistance from a systems integrator selected by FirstNet, through an open and competitive request for proposals (RFP).

2. Geographically distributed and redundant.
3. Based on a single logical subscriber database.

4. Supportive of highly distributed serving & packet gateways to keep local data local and reduce both latency and backhaul costs.

5. Designed to allow local command and control options.

6. Consistent with a high level of security through proper design and continuous monitoring of the entire core network.

7. Based on commercially accepted open standards.

8. Built with an end-to-end Operational Support System (OSS).

9. Independent of (not shared with) a commercial network.

10. Potentially supported by a managed services contract that is renewed periodically, in order to lower operational costs.

Hosted core solutions should also address the following considerations:

1. A single, logical nationwide core is necessary to address interoperability, availability and resiliency.

2. A Public Safety network faces a different class of threats than commercial networks due to the critical nature of its subscriber base. As commercial use of this network is not envisioned, Nokia Siemens Networks encourages the FirstNet Board to fully segregate and firewall the network from as many outside influences as possible.

3. The core infrastructure procurement should adhere to government security guidelines.
System integrators experienced in building and managing secure government communications systems appear to be best suited for this role.

The deployment of the FirstNet core can begin in advance of detailed inputs from states as long as flexibility is built in to the architecture to accommodate state requests for local command and control options. In addition to the security concerns, accessing Public Safety related core equipment by FirstNet personnel or staff associated with the contracted entity (system integrator) to perform maintenance, ensure availability and reliability, and to implement any upgrades or modifications will be necessary. Therefore, NSN believes the most appropriate approach to providing a core capability for Public Safety is to provide a dedicated core rather than attempting to share existing commercial core capability. As indicated, NSN believes that this dedicated public safety core equipment should be procured competitively through a public RFP that is ultimately decided on by the FirstNet board and deployed by the system integrator selected by FirstNet.

**Radio Access Network (RAN) Deployment Options**

Nokia Siemens Networks recommends a blended approach of building an independent FirstNet RAN network, with separate and dedicated equipment for Public Safety, while leveraging existing site infrastructure of public and private entities. While an entirely stand-alone FirstNet network (including independent sites and infrastructure) would provide dedicated access, security and complete control over all assets, it would prove too costly and contravene the direction of Congress to leverage existing infrastructure assets where possible. Meanwhile, offering Public Safety users the services they require by utilizing commercial network(s) not only contravenes the law’s requirement to deploy and operate a dedicated Public Safety Broadband network, active RAN sharing with commercial
networks presents considerable issues that could be detrimental to First Net’s success. As such, an approach between the two extremes that leverages all available physical sites and infrastructure while providing separate, dedicated core and RAN equipment makes technical, economic and legal sense and should be pursued.

A key aspect to be considered in deploying the network is the ongoing operational cost to manage the network. Figure 1 is an estimate of the operations cost of a RAN site under passive site sharing. The operational cost is driven by the site infrastructure used to construct the network. The use of assets owned by State, Local and Tribal entities, LMR towers and utility infrastructure will lower the operational cost of running the network. For this reason, NSN recommends that FirstNet not focus exclusively on the use of carrier sites and physical infrastructure, but instead broaden the focus to include all potential physical infrastructure sharing options: LMR, state and local land and buildings, tribal assets, federal property, utility easements and infrastructure, and the sites and physical infrastructure of commercial carriers. As indicated in Figure 1, this will allow FirstNet to lower deployment costs further than a carrier-only site-sharing model because FirstNet can identify the lowest cost siting option for each deployment area. Identifying appropriate sites across this range of infrastructure ownership, and managing the negotiation, preparation, and roll out of equipment to each of these sites is another reason that NSN recommends that FirstNet hire a system integrator as the primary contractor.

The system integrator can identify appropriate sites, negotiate arrangements with the owners for location of Public Safety’s independent core and radio network elements, negotiate
payment, and facilitate necessary roaming arrangements with commercial carriers to provide important coverage and redundancy.

<table>
<thead>
<tr>
<th>Site Sharing LMR/ State/ Local / Tribal / Utility</th>
<th>Site Sharing Commercial Networks / Tower Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Site Operations cost per year</strong></td>
<td><strong>$24,200</strong></td>
</tr>
<tr>
<td>Site Rental per year*</td>
<td><strong>$12,000</strong></td>
</tr>
<tr>
<td>O&amp;M per year</td>
<td><strong>$8,100</strong></td>
</tr>
<tr>
<td>Utilities</td>
<td><strong>$700</strong></td>
</tr>
<tr>
<td>Personnel (Field, RF and operations)</td>
<td><strong>$3,400</strong></td>
</tr>
<tr>
<td><strong>Monthly Operating Cost per User</strong></td>
<td><strong>$29</strong></td>
</tr>
</tbody>
</table>

* Site rental to be used to subsidize “user fee” paid by local public safety entities

**70 users per site based on 3M users on 44K Sites

**Figure 1: Operational Cost per Site**

An independent FirstNet RAN network deployed on infrastructure that is owned by a blend of State, Federal, Local and Tribal entities, commercial carriers, utilities, and which utilizes existing LMR sites and assets provides significant advantages in lowering cost and speeding up the deployment timeline. The use of LMR tower sites and state owned buildings for site location will result in a lower monthly site rental fee. The site rental fee paid by FirstNet to local entities could also subsidize the “user fee” paid by local Public Safety to access FirstNet. Reuse of existing backhaul, power, generators and lower site hardening requirements will further lower deployment costs.

Assumptions

Personnel
- Network Operations - 100 eNodeB per person
- Field Engineers - 75 eNodeB per person
- Admin & Management -100 eNodeB per person
- Annual average cost per personnel - $100K

OA&M - Includes HW and Swmaintenance including software support and new releases

Source : (Refer to Appendix for details)
2. Minnesota Department of Public Safety, Public Safety Wireless Data Network Requirements Project - Televate LLC March 2012
4. Nokia Siemens Networks - Internal Analysis
Appropriate infrastructure to leverage under this approach would include towers, buildings, rooftop sites, conduits, rights-of-way, power supplies, and backhaul, but would not include the sharing of existing commercial carrier radio network elements. The section that follows identifies the considerable technical challenges as well as the security concerns that sharing commercial carrier radio assets creates. For these reasons, NSN believes it is important to instead procure and deploy independent radio network elements dedicated to Public Safety at all of the physical infrastructure sites identified above.

For existing commercial carrier sites this would entail co-locating the Public Safety equipment at these sites and connecting to existing power supplies and transport while potentially improving those items to account for additional power consumption and improved security for the transport necessary to meet Public Safety needs. As in all cases, NSN believes that promoting a vibrant and competitive equipment ecosystem will further lower costs to FirstNet. To accomplish this, NSN recommends that FirstNet decouple the selection of RAN equipment from the selection of a system integrator and the involvement of commercial carriers. A public RFP process for equipment selection ultimately decided upon by the FirstNet board will provide FirstNet tremendous flexibility to define the desired functionality and obtain a highly competitive price for the equipment.
Issues with active RAN sharing with commercial networks

Nokia Siemens Networks fully appreciates that in some cases RAN sharing between commercial carriers has its benefits. However the requirements of a Public Safety network differ from those of commercial networks and sharing infrastructure with commercial carriers raises a number of concerns. Careful consideration must be given to issues such as the following:

1. Public Safety Features on Commercial Networks. Public Safety has a well-understood but poor quality of experience on commercial networks during times of disaster and other incidents that create high network demand. Over the past several years, concepts like priority and quality of service have been described to Public Safety as methods to improve their quality of experience on either a commercial or private network. In our experience, Public Safety may require a more robust implementation of Quality of Service than currently implemented on commercial carrier networks due to the extreme conditions that this network must continue to function under.

2. Service Fees and Affordability. In our discussions with Public Safety officials, NSN has encountered a number of jurisdictions whose communications budgets do not allow them to use commercial wireless services today. They express concern that they will not be able to use FirstNet services due to limited budgets. Nokia Siemens Networks encourages FirstNet to take jurisdictions like this into account when designing the network and its business model. Nokia Siemens Networks is also concerned that the statute only authorizes FirstNet to assess fees for access to infrastructure and elements it owns. It is possible that a shared RAN model would compromise FirstNet’s legal ability to assess and collect important user and access fees to pay for ongoing management and upgrade of the network.
3. Network Management. In the scenario outlined in the FNN conceptual presentation, specifically a FirstNet core network connected to multiple carrier RANs, FirstNet would need to pay special attention to how each individual carrier RAN is maintained and operated. Even though 3GPP specifications ensure compatibility and interoperability between releases, interfaces and functions, there is a greater burden to manage and verify compatibility between equipment vendors’ software updates for FirstNet. Timing of feature and software releases between RAN vendors would need to be managed and harmonized for FirstNet required features to ensure timely upgrades. FirstNet would need to be extremely vigilant in its network configuration management and that of its partner networks.

4. Public Safety Grade Networks. There is no common definition of public safety grade equivalent to carrier grade which is commonly understood to be 99.999% network availability. The attributes of a public safety grade network are plant hardening, high levels of power redundancy, fast restoration, and a level of security that enables federal users to have secure access. FirstNet could overcome some of these issues by stacking network coverage as described in the presentation to the FirstNet Board, but in areas where several carriers may not be available, FirstNet would need to ensure that the RAN meets the attributes required by the Public Safety community.

5. Nokia Siemens Networks believes that “Securing the Radio Access Network (RAN)” consists of three very distinct and critical components that should be part of a minimum security specification for FirstNet: User Access Security, Transport Security, and Trusted Environment (found internal to the eNodeB). All three of these components are required to reach a
minimum acceptable level of security. Properly implemented transport security includes support of PKI, secure device identity (found internal to the eNodeB), operator identity management (PKI), IPSec, management protocols that are secure and secure file transfer for the management planes, and firewalls. Secure Device identity is critical in protecting from such issues as cloning and actual radio infrastructure. Thus minimizing risks by requiring authenticated and integrity protected code (Signed Software) and ensuring a process that ensures radios can only boot in a secure boot mode and are booting genuine and verified vendor code would need to be a minimal requirement.

The carrier networks do not implement all of the above components uniformly on existing infrastructures. For example, some networks may lack:

- A single PKI Infrastructure in place managing operator identity and devices.
- A uniform transport security implementation between eNodeB interfaces and core network (Security Gateways) for a traffic plane.
- A system in place to ensure integrity of code on radio units, that those radios will only boot in protected mode, and that the radios allowed on the network are only those authenticated radios.

A lack of appropriate levels of security in the architecture of FirstNet puts FirstNet and its user community of first responders at risk of eavesdropping (e.g., Foreign Nation Intelligence Units), unauthorized access of sensitive first responder data (e.g., Criminal Elements) or worse, infrastructure attacks by terrorist or other elements that could result in failure of key network components and a loss of use of the network by first responders at a
critical time (e.g., during a terrorist attack). Nokia Siemens Networks recommends that FirstNet develop strong security specifications in the short term that address, at a minimum, User Access, Transport and Trusted Environment Security in a manner that is consistent with industry groups (e.g., 3GPP)\textsuperscript{4} and U.S. Government standards being currently developed within the Department of Defense (DoD) and apply those specifications to any decisions taken with regard to the architecture taken by FirstNet. Further elaboration of these points is available in a document submitted by Nokia Siemens Networks to the Technical Advisory Board for First Responder Interoperability at the Federal Communications Commission (FCC).\textsuperscript{5}

6. Shared Infrastructure – Nokia Siemens Networks believes that sharing wireless carrier infrastructure like towers and backhaul facilities makes sound economic sense in situations where the carriers actually own that infrastructure. A number of wireless carriers have sold their tower assets to companies like Crown Castle or American Tower Corporation over the past decade as a way reducing cost and creating revenue. This complicates asset-sharing arrangements between FirstNet and the commercial carriers because they are often tenants on someone else’s tower. A very good example of this is the recent agreement between Crown Castle International and T-Mobile, which allows Crown Castle to operate 7,200 towers in exchange for $2.4 Billion. Large systems integrators are best positioned to acquire RF design expertise and negotiate agreements with the large number of state, local, carrier, utility and third party tower owners to match that network design.

\textsuperscript{4} 3GPP Technical Standards concerning Radio Access Security (TS 32.301, TS 33.210, and TS 33.401).
\textsuperscript{5} FCC TAB Input: Public Safety Networks and LTE Security Considerations (dated May 2, 2012).
7. Complex Device Ecosystem – Nokia Siemens Networks is concerned that both eNodeB sharing and layering of commercial carrier spectrum to achieve high levels of availability will create a very complex device ecosystem. The need to support multiple carriers, technologies, and spectrum may lead to very expensive devices. One of the primary tenants of adopting commercial standardized technology for public safety is to leverage scale and the significant amount of research and development (R&D) dollars pumped into the ecosystem today. If single device types become all things to all people we will simply end up creating unique Public Safety devices that miss on scale and competitiveness. To avoid potential interoperability issues when roaming outside a home region, FirstNet should consider defining a baseline frequency and technology that all devices employ. FirstNet should pay special attention to these issues to ensure that they are transparent to Public Safety.

Nokia Siemens Networks believes that these considerable issues with RAN Sharing could be detrimental to FirstNet’s success. Separate, dedicated core and RAN equipment for Public Safety avoids most of these challenges. Nokia Siemens Networks thus recommends a blended approach of building an independent FirstNet RAN network, with separate, dedicated equipment for public safety while leveraging site infrastructure of public and private entities.

Network Operations Model

The management and operation of the network is critical to the success of FirstNet. A “user fee” paid by FirstNet users is to support the operations, maintenance and upgrade of the network. To lower operational costs, a managed service contract awarded to System Integrator(s) selected in a competitive bid process that is renewed periodically should be considered.
IV. Application Framework

NSN fully supports FirstNet’s view that it should deploy a Service Delivery Platform. Commercial Network operators have developed their Service Delivery Platforms and capabilities over a number of years and that knowledge and experience should be leveraged to the fullest extent possible.

A Service Delivery Platform helps to create an application development ecosystem that enables application developers from Public Safety’s ranks to large corporations and even individuals to provide their applications and services to FirstNet subscribers. Nokia Siemens Networks believes that this will create vibrant and diverse ecosystem for Public Safety.

V. Devices

Devices allowed to operate on the FirstNet LTE network need to meet minimum criteria:

- Compliance to 3GPP and other applicable open standards as specified by FirstNet.

- Minimum 3GPP Band 14 support and a limited set of bands/radio technologies as specified by FirstNet which match to commercially available capabilities.

- Ability to support multiple advanced applications – advanced video solutions, push-to-talk voice, etc.


A device management system will be required to provision, secure, manage and provide over-the-air software updates. FirstNet should maintain a list of devices which comply with the
requirements of the network and institute IMEI checking to ensure that rogue or non-compliant devices cannot access the network.

VI. BTOP Grants for FirstNet Pilots

Nokia Siemens Networks recommends that FirstNet redeploy BTOP grant funding for FirstNet pilots in 2013 to support PSCR activities related to FirstNet with test beds for equipment and applications and Pilots to demonstrate Interoperability and deployment scenarios including hosted core solutions.

Appendix: References

The following sources were referenced to develop the operating cost model shown in Figure 1.

   Federal Communications Commission May 2010


4. Nokia Siemens Networks - Internal Analysis