Comments of

Harris Corporation

to the

National Telecommunications and Information Administration,
U.S. Department Of Commerce,
On Notice of Inquiry on Behalf of the:

First Responder Network Authority

(FirstNet on Conceptual Network Architecture Presentation. Docket No: 120928505-2505-01)

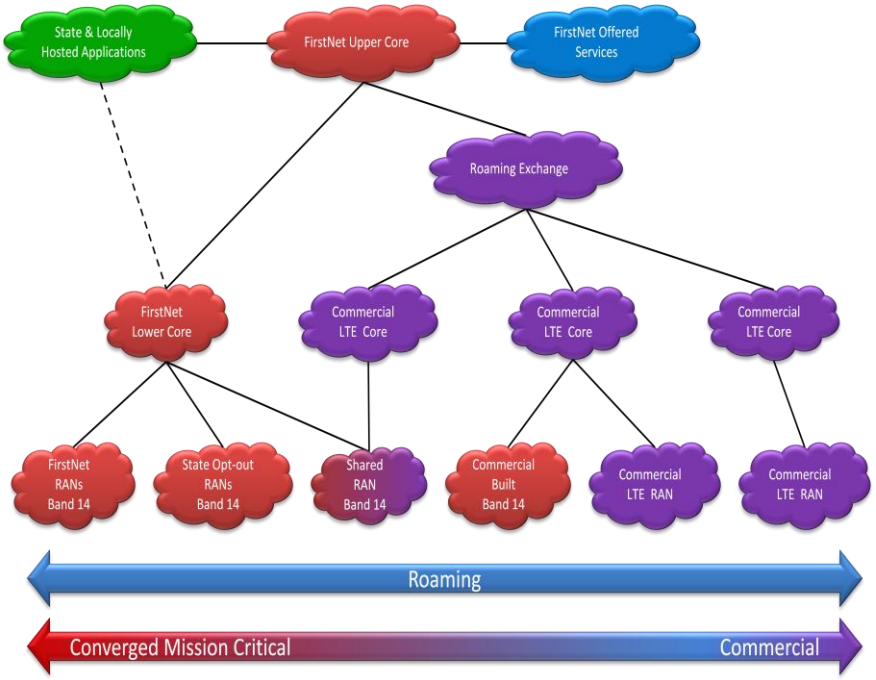
Harris Corporation is pleased to offer the following comments on the NTIA's "FirstNet NOI," which seeks inputs on the FNN Concept network architecture, business models to ensure FirstNet's success, and a path towards delivering broadband applications for first responders. Harris thanks FirstNet and NTIA for their commitment to ensuring the deployment of an interoperable Nationwide Public Safety Broadband Network (NPSBN). Harris is ready to deliver interoperable LTE solutions for first responders across the nation, and is eager to partner with FirstNet to make this happen.

Executive Summary

FirstNet's task, to deliver an interoperable National Public Safety Broadband Network (NPSBN), is enormously complex and vital to First Responders and the citizens they protect. In this context, the FirstNet solution must be executed within an optimal business model that preserves the NPSBN for generations to come. FirstNet must ensure strong collaboration among states and all stakeholders and deploy a network architecture that enables the benefits of network convergence. The NPSBN subscribers will demand open access to applications and user devices supported by superior service value. Harris' recommendations are illustrated in the following tables and network diagram and discussed more fully in the body of these Comments.

I. Success of the NPSBN Requires a Sustainable, Subscribership-Driven Business Plan	
Differentiate service offerings from commercial competitors.	FirstNet should commit to long-term deployment of a dedicated mission-critical network with associated quantifiable performance metrics.
Partner with commercial service providers to expand coverage, lower cost, and simplify the billing process.	FirstNet should define a single commercial service provider for a given geography to provide initial coverage in areas not covered with Band 14 and, in the long term, to serve as a backup to the NPSBN.
Reduce subscription costs for state/local users commensurate with state's contribution to the NPSBN.	FirstNet can work with state, local, and tribal entities to identify assets that could be contributed to the construction of the network. User fees paid to FirstNet would then be reduced in accordance with these capital and monetary contributions to the NPSBN.
Drive revenue generation through secondary users and leased access to excess capacity.	FirstNet should work aggressively to attract secondary users with similar mission-critical requirements.

II. Enhancing State and Local Collaboration Expedites Deployment of the NPSBN	
Work jointly with states and fund their efforts to complete the design efforts for the NPSBN in their state.	Close partnerships with state, local and tribal entities will result in a network that meets the needs of the real users and allow cost benefit trade-offs at the lowest level possible.
Consider allowing states to manage the build-out effort of their approved design.	Collaborating with states on both network design and funding will create significant cost savings and avoid the time penalty likely to occur with state opt-outs.
Take advantage of national negotiating power in awarding cost-effective contracts.	Common RFPs should be issued by FirstNet and awards made on a state or regional basis for network design and construction. A single contract per commercial entity, encompassing several states or regions, will create cost savings and economies of scale.
Drive early deployment of the Evolved Packet Core (EPC).	FirstNet should move quickly to design and deploy a nationwide EPC in conjunction with private industry partners experienced in the design of mission-critical networks.

III. An Effective Architecture Drives Key Attributes of the NPSBN	
Converged, interoperable technology	• Technological convergence with applications that enable access to voice, video and data services tailored to the mission-critical needs of public safety. • NPSBN can evolve without compromising nationwide interoperability. • Economic convergence through investment on a single converged platform, ultimately eliminating the need to invest in multiple divergent technologies and networks.
Long-term financial viability	• Through partnership with state, local and tribal entities, FirstNet can deploy network infrastructure on a large collection of pre-existing public safety hardened facilities. • FirstNet can leverage the same infrastructure commercial service providers have created and/or lease today. • FirstNet can offer mobile broadband service to public safety users where Band 14 Radio Access Networks (RANs) are deployed and on commercial networks that have roaming agreements with FirstNet.
Network that meets public safety mission-critical needs	• Creates dedicated network capable of delivering mission-critical services demanded by the customer base.
The NPSBN supports locally hosted applications and FirstNet-offered services A Roaming Exchange enables independent evolution of the NPSBN and commercial partner networks The dedicated NPSBN EPC enables differentiated service offerings Multiple options exist for Band 14 RAN build-out The NPSBN can deliver converged mission-critical services and enable roaming to commercial networks	

IV. Development of Standards-Based Applications Is Crucial to Network's Success
FirstNet should support formal industry standards to drive interoperable applications.
Establishing essential network services is key to driving open source applications.
FirstNet should develop and publish network management and business systems integration specifications.
FirstNet should publish and maintain a document that describes the underlying security assumptions to guide application developers.

V. Proposed FNN Concept Creates Subscribership and Technical Challenges
Differentiated services will drive and sustain subscribership.
Hosting several bands in a single handset creates significant implementation challenges, potentially thwarting the goal of leveraging commercial technologies to reduce user device cost and enhance interoperability.
Commercial networks will evolve independently from the NPSBN, creating on-going interoperability challenges.

Harris: A Leader In Development Of Networks, Devices, and Applications to Meet Public Safety's 4G Needs.

- Operates five public safety LTE pilot programs, working with First Responders to demonstrate the power of broadband for our First Responders through cutting-edge networks, applications, tablets, and handheld user devices. pspc.harris.com/media/7846C_harris-lte-brochure_tcm27-17539.pdf
- Recently operated the first nationwide public safety LTE pilot network, linking First Responders in Las Vegas, NV; Rochester, NY; Miami, FL; and Chelmsford, MA pspc.harris.com/Solution/LTE.asp
- Owns, operates and maintains the public safety network for the State of Florida; operates statewide public safety network in Pennsylvania, Maine, and other states. pspc.harris.com/News/aboutPSPC.asp
- Built, operates and maintains a nationwide mission-critical network: The FAA Telecommunications Infrastructure (FTI) govcomm.harris.com/solutions/products/atc/fti-atc.asp

COMMENTS OF HARRIS CORPORATION

I. Success of the NPSBN Requires a Sustainable, Subscribership-Driven Business Plan

The business model FirstNet chooses is arguably the most important consideration that the FirstNet Board must address. The model must ensure long-term sustainability and be able to fund not only its ongoing operation but also future technology refresh cycles. Key to this will be creating revenue generation through capacity leasing, user base expansion, providing mission-critical services superior to commercial alternatives, developing partnerships with commercial service providers, and driving incentives for state and local investment into the building of the NPSBN. Additionally, attracting and retaining NPSBN subscribers is critical to long-term network viability. Today, many First Responders make use of commercial mobile broadband services through monthly subscriptions. In order to be an attractive alternative to this competition, FirstNet must offer greater value than that offered by today's commercial providers while delivering system and network reliability that exceeds commercial-grade reliability. Though a difficult objective, anything less could result in subscribers remaining with their current service and not subscribing to the NPSBN. To avoid the limited subscribership that would hinder the NPSBN, a business model should incorporate the following key elements:

a. Revenue Generation Through Capacity Leasing.

Developing a Shared Access Agreement so that commercial service providers can use excess network capacity when not needed by First Responders would create early and sustainable revenue streams. It will be challenging to balance the long-term needs of commercial service providers with the likely increase in First Responder broadband data usage over time. FirstNet should also expand the user base by aggressively adding secondary users. Critical Infrastructure and Key Resources (CIKR) such as the military, federal law enforcement, department of homeland security, utility companies, and transit agencies should be part of the FirstNet user base.

b. Superior Service.

It is important that FirstNet commits to building a mission-critical NPSBN in order to attract and retain subscribers.[1] The network should deliver converged services for public safety voice, video, and data applications. Further, FirstNet should quantify specific mission-critical grade functionalities and reliability metrics for the future network, particularly noting how these features will exceed those provided by commercial service providers. The minimum level of Band 14 coverage expected to be achieved and an associated timeline to meet that level should be included. To sustain subscribership, this targeted level of coverage should exceed levels normally provided by commercial operators, particularly for in-building coverage, and follow user-established First Responder requirements for mobile and handheld user devices.

c. Partnerships With Commercial Service Providers to Simplify Use and Expand Coverage.

FirstNet should create a business model in which public safety users pay a single monthly fee for broadband services on NPSBN Band 14 (where deployed) and commercial networks (where roaming agreements exist). FirstNet should define a single primary commercial service provider to be used for each geographic area in the short-term for those areas not immediately served by Band 14 and to serve as backup to Band 14 in the long term. FirstNet should solicit competitive bids from commercial service providers, by region, and make awards to a single commercial service provider for each specific area. Negotiating a single contract with each awarded commercial service provider will drive economies of scale through large, multi-region coverage areas. In effect, FirstNet will act as a Mobile Virtual Network Operator (MVNO), using existing network operator transport networks, both prior to and after deployment of the NPSBN Band 14 RAN(s).

Not only would this model drive subscribership by simplifying use and minimizing cost, it will lower the cost of user devices for First Responders. This, in turn, will drive development of the type of user

[1] In determining the broadband communications needs of First Responders, beyond the FCC requirements, Harris collaborated with many stakeholders to develop the National Public Safety Telecommunications Council's Draft "Public Safety Broadband High-Level Statement of Requirements for FirstNet Consideration (Draft Rev C, July 25, 2012)" (NPSTC 7/25/12 SOR). Harris recommends the requirements included in this document for FirstNet's consideration as it determines public safety's needs. These requirements are in addition to and complimentary of the minimum technical requirements as established by the Technical Advisory Board for First Responder Interoperability.

devices for a given area containing Band 14 and the band plan used by the designated commercial service provider. To ensure ubiquitous coverage, some areas may require a cellular service provider and a satellite provider. The service to the user would begin on the FirstNet-designated service provider, but would roam to/from Band 14 as the NPSBN is built out. As FirstNet progresses over time with the build-out of a Band 14 RAN, less commercial airtime would be used and fees paid to commercial service providers would be reduced.

d. User Fees Based Upon Contribution of State/Local Assets.

It makes sense for First Responders to be credited when their state's assets help build the NPSBN. Each state should catalog state and local assets that can be made available during the consultation phase of network design for NPSBN construction (fiber, towers, backhaul, etc.). User fees for all First Responders in that state/region should then be reduced in accordance with the value of the assets contributed by the state/region to the NPSBN build-out. Many publicly-owned tower sites are in use by First Responders today and are, in essence, lease-free. These should be preferred to commercial sites most often leased by commercial service providers from third parties.

II. Enhancing State and Local Collaboration Expedites Deployment of the NPSBN

Securing early and enduring collaboration with state, tribal and local stakeholders will assure an efficient and cost-effective deployment of the NPSBN. In addition to the cost-performance characteristics of the network addressed by the model above, the level of collaboration FirstNet maintains with states, tribal communities, and localities also likely will affect the health of subscribership levels. A procurement and deployment model framework is outlined below that may create significant acceptance and collaboration from these important stakeholders.

1. FirstNet moves early to procure and deploy a nationwide, distributed Upper Core(s) and associated backbone connectivity, and provides the architectural framework for interconnecting RANs. (See Section III for details)

2. FirstNet defines early in the process the specific funds available to each state for RAN construction and deployment and facilitates the ability for states to use other sources of funding to accelerate or supplement the RAN build-out.

3. Each state designs the NPSBN in its geography, in accordance with FirstNet guidelines, including site locations, network topology, coverage areas, etc. FirstNet provides State and Local Implementation Grant Program funding to the states for this purpose. FirstNet allows states the option of partnering with neighboring states in a 'regional' effort.

4. Once the design is approved, FirstNet executes an RFP for each state/region build-out using a common template and LTE equipment approved for use on the NPSBN.

5. FirstNet makes awards for each state/region, negotiating one contract per awardee, leveraging large contract awards to reduce costs. FirstNet considers allowing the state to act as the primary manager in executing the build-out of the approved network design. FirstNet provides funds to support this management as it would for any build-out oversight.

6. Using service and leasing fees, FirstNet contracts for Operations, Administration, and Maintenance (OAM) on a state-by-state, regional, or national basis.

This model must carefully balance state needs with overall FirstNet governance, as required in H.R. 3630. It positions the states and FirstNet as partners and could eliminate more than a year from the development cycle, compared to a model that relies on centralized planning and management of opt-outs. It also minimizes the likelihood that states will opt out of the NPSBN and reduces the potential deployment delay. In this process, FirstNet funds the states to design and manage the implementation of the NPSBN in their state, eliminating the 20% opt-out match requirement and maintaining economies of scale by retaining contract negotiation and management at the national level.

The Board's decision on September 25, 2012 to engage NTIA "to examine [BTOP] projects and provide input to NTIA as to whether and how these projects can support the development of the nationwide, interoperable public safety network" provides a unique opportunity to emphasize key principles of FirstNet. Harris recommends that unspent BTOP funds be used, in conjunction with H.R. 3630 designated funding, to foster early deployment through a competitive procurement process executed in collaboration with State/Local governments and pursuant to the RFP process detailed in H.R. 3630. Harris recommends that this, and all NPSBN infrastructure deployment, require multi-vendor participation with associated certification and demonstration of appropriate interoperability. By doing so, the requirements of H.R. 3630 to ensure an interoperable, multi-vendor driven build out can be achieved, potentially on an accelerated timeline.

III. An Effective Architecture Drives Key Attributes of the NPSBN

Developing an effective network architecture is a significant part of a successful business plan for FirstNet. The NPSBN network architecture must serve as a blueprint that drives the network along a cohesive evolution trajectory to ensure nationwide interoperability, while allowing for substantive participation at the state, local, and tribal level in design, construction, and maintenance of the network.

a. Network Architecture Assumptions.

In examining the FNN Concept and alternatives to the NPSBN architecture, Harris makes the following assumptions:

1) The NPSBN will support nationwide roaming of public safety users, enabling their mobile user devices to access hosted applications: (1) in their home jurisdiction; (2) in the serving network into which they roam; and (3) in the Service Delivery Platform available nationwide and hosted by FirstNet.

2) Public safety users will be "homed" on the NPSBN EPC and will be authenticated by that EPC in accordance with a FirstNet-defined security policy. This would be true even for public safety users operating in an area served by a commercial FirstNet roaming partner that provides coverage where no Band 14 service is available.

3) FirstNet may have multiple strategic commercial wireless operator partners.
   i. There is potential for FirstNet to implement multiple business models.
   ii. Commercial networks will evolve independently from FirstNet.

4) Secondary users will have access to excess Band 14 network capacity; public safety users have priority.

5) The NPSBN will evolve with technological advances through incremental investment. This evolution will ultimately enable the NPSBN to support converged mission-critical voice, data and video services to public safety users.

6) FirstNet will endorse the potential for state, local, and tribal investment in the construction and operation of the network

7) FirstNet will create an architecture enabling interoperability with legacy Land Mobile Radio (LMR) systems in use today by First Responders.

b. Existing Challenges or Obstacles.

The FirstNet Board will confront several key challenges as it further develops the network architecture of the NPSBN as part of its overall business plan:

1) How to ensure long term financial viability;

2) How to ensure that the NPSBN meets the mission-critical needs of public safety;

3) How to ensure that the NPSBN can evolve without compromising nationwide interoperability;

4) How to ensure cyber security from the very beginning and throughout the lifetime of the NPSBN;

5) How to ensure user devices will exist that meet the unique needs of public safety.

FirstNet – A Converged Mission-Critical Network for Public Safety

It is essential that FirstNet implements the NPSBN consistent with its core goal: construct a network that offers public safety users capabilities that are aligned with their mission-critical needs and are interoperable on a nationwide basis. While it is important for FirstNet to leverage commercial technologies, infrastructure, and business practices, FirstNet should not implement a commercial-like network that simply offers capabilities that are available from commercial networks now and in the future. The following table summarizes some of the distinct characteristic of public safety networks, the NPSBN, and commercial broadband networks.

Existing Public Safety Networks	NPSBN	Commercial Broadband Networks
RF Sites are located to provide required jurisdictional coverage (e.g., 95% land area).	Cell density and location are driven by the need for geographic coverage.	Cell density and location are driven by the need for population-centric capacity.
Capacity constraints require implementation of priority and preemption capabilities to ensure the highest priority calls are given priority access to network resources.	Public safety usage model requires priority and preemption capabilities with responsive local control.	Commercial networks offer best-effort service to customers.
Mission-critical needs drive Grade of Service requirements for resiliency, reliability and security.	Mission-critical needs drive Grade of Service requirements for resiliency, reliability and security.	Consumer and market-driven concerns drive Grade of Service requirements.

a. Architecting for Financial Viability

Network architecture is an integral part of the FirstNet business plan and the financial outlook of the NPSBN. FirstNet must ensure that the NPSBN architecture enables a variety of options within the context of a nationwide framework, thereby enhancing its ability to address financial challenges. H.R. 3630 provides for build-out funding tied to spectrum auctions and contains provisions for permanent self funding through user fees, secondary leasing and leased access to equipment and infrastructure that FirstNet owns. In addition, a close partnership between FirstNet and state, local, and tribal entities is called for to enable these organizations to participate in constructing and maintaining the NPSBN. Further, a close partnership will encourage states to utilize the NPSBN rather than engage in the opt-out procedure or remain with a commercial service provider.

b. Evolution of Public Safety Networks

Two principles are key to successful evolution in a commercial network. First, ensure *backward compatibility through interoperability* - a graceful migration from the current network/technology to the new network/technology. Second, phase in *new capabilities* offered by the new network/technology. For public safety, a key to evolution is migration from current commercial broadband networks to the NPSBN and from narrowband LMR networks to a fully converged voice/video/data network. These evolution steps are depicted in Figure 1.

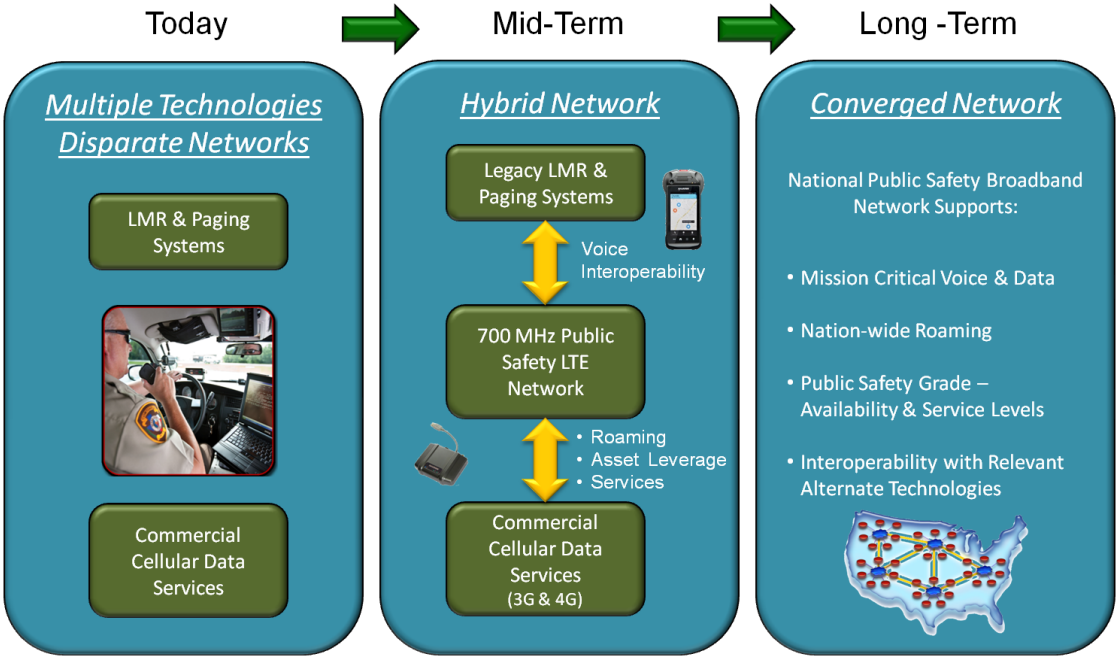


Figure 1: Evolution of Public Safety Networks

FirstNet must also consider how to evolve the NPSBN through subsequent LTE releases, particularly considering that the total solution is comprised of Applications, User Devices, Network Services, the Core Network (or EPC) and the RANs. Interoperability across all these layers requires specific attention to the implications of each phase of evolution to backward compatibility and future capability. Figure 2 depicts a notional evolution framework for FirstNet to consider as it plans this facet of the NPSBN.

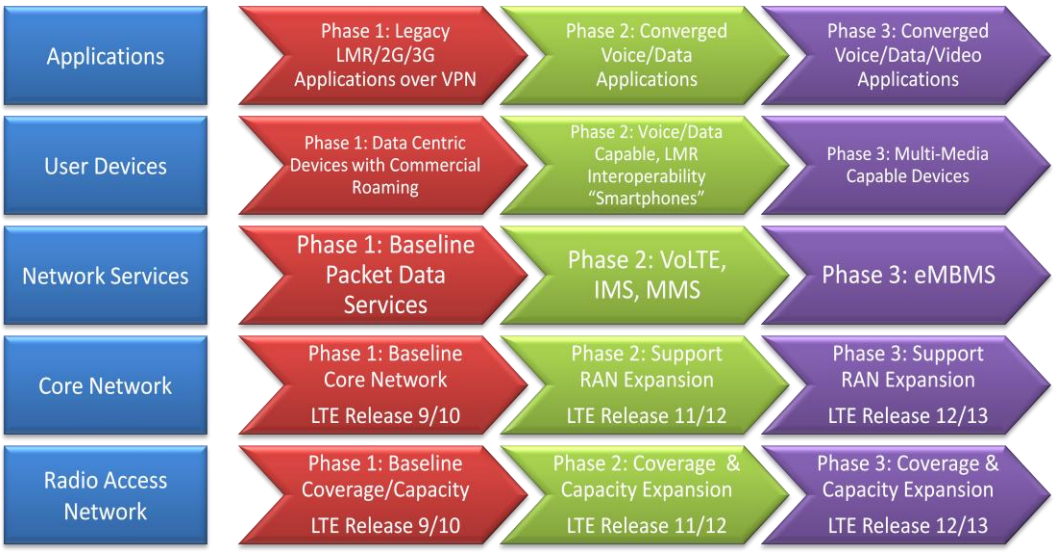


Figure 2: Notional Evolution Framework

c. Cyber Security

H.R. 3630 places particular responsibilities on FirstNet to ensure the protection of the NPSBN from cyber threats, specifically to "ensure the safety, security and resiliency of the network, including requirements for protecting and monitoring the network to protect against cyber attack" – §6206(b)(2)(A). From the outset, cyber security components must be fundamental to the architecture and continue through the life of the network. Harris supports and contributes to ongoing work within DHS as part of the Cyber Security Risk Assessment initiative and recommends that the FirstNet Board consider creation of a dedicated committee focused on this key requirement. Indeed, cyber security was also addressed by the Technical Advisory Board for First Responder Interoperability in its recommended minimum technical requirements to ensure nationwide interoperability for the NPSBN.

d. User Devices

As commercial 700 MHz LTE networks continue to be deployed in the U.S., key discussion among industry regulators and policy makers is focused on interoperability. In this context, interoperability refers to two things: 1) the interconnection of these networks to enable roaming between commercial service providers, and 2) availability of user devices that support multiple commercial frequency bands. In commercial practice, development of user devices is driven by service providers as part of their business plans to evolve their networks. There is a flow down of requirements from these service providers through user device OEMs (Original Equipment Manufacturers) and onto chipset providers. In the current ecosystem, nothing naturally drives interoperability across commercial networks.

FirstNet will face the challenge of interoperability as well, perhaps to a greater degree because of the smaller user base to be addressed by the NPSBN. It is difficult to imagine that user devices will exist that support Band 14 and more than one commercial band plan. In fact, it will be practical to source user devices that support Band 14 and the band plan of one commercial service provider – but no more– in a cost-effective user device. It is conceivable that multiple user devices will be offered on the market, each targeted at a different FirstNet roaming partner.

e. Proposed Network Architecture

Harris proposes that FirstNet consider a layered network architecture that supports multiple business models. The layers of this network are depicted in Figure 3. FirstNet may implement all components of this architecture, or a subset, based on the business model it selects and the relationships it establishes with commercial partners. This architecture reflects key provisions of H.R. 3630:

1) The NPSBN will initially consist of an EPC, and multiple RANs – §6202(b). FirstNet may enter into agreements with commercial, federal, state, tribal and local entities to leverage existing infrastructure as it constructs the network – §6202(c)(3). States can implement RANs in accordance with an opt-out process – §6302(e)(2). These network components are depicted in **Red.**

2) FirstNet may enter into roaming agreements with commercial network providers – §6202(c)(5). These components are depicted in **Purple**.

3) FirstNet may enter into covered leasing agreements resulting from public-private partnerships to allow access to network capacity on a secondary basis – §6208(a)(2). These components are depicted in the combined **Red** and **Purple**.

4) The NPSBN will provide support for state and locally hosted applications, specifically to promote integration of the network with public safety answering points – §6206(b)(2)(C). These components are depicted in **Green**.

5) FirstNet may provide connectivity to the public Internet and public switched network – §6202(b)(1)(B). These components are depicted in **Blue**.

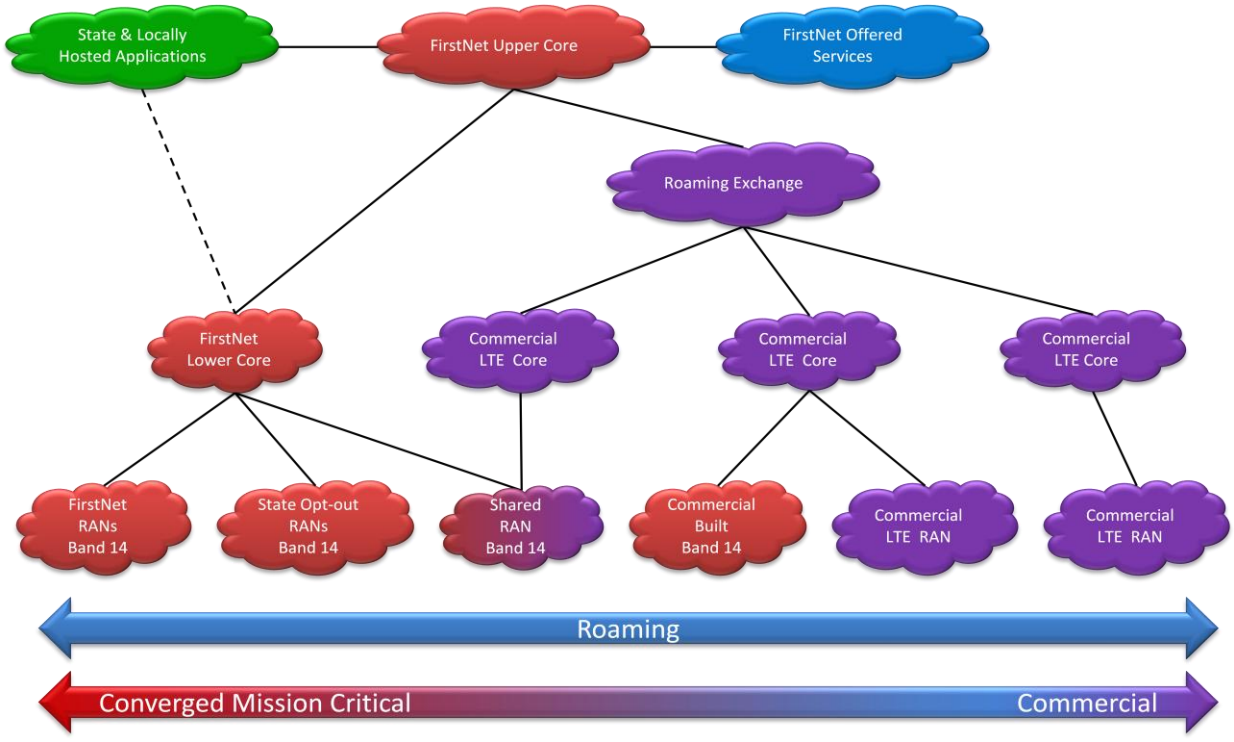


Figure 3: Layered Network Architecture

The components of this single nationwide network architecture include:

FirstNet Upper Core	In the LTE architecture, an Upper Core provides subscriber and business system services, which are implemented in the Home Subscriber Server (HSS) and Policy and Charging Rule Function (PCRF). It can also include Packet Data Gateway (P-GW) functions that anchor packet data services in the Home Network.
FirstNet Lower Core	In the LTE architecture, a Lower Core provides control plane and data plane services, which are implemented in the Mobility Management Entity (MME) and Serving Gateway (S-GW). Local breakout functions can be provided through locally implemented P-GWs.
FirstNet Radio Access Networks (RAN) (Band 14)	Band 14 RANs are implemented in the eNBs (Evolved Node B) located at the cell sites. These sites can be any combination of commercial and state/locally owned sites. FirstNet can implement commercially sited RANs through leasing agreements with commercial cell/tower providers in the same manner as is common business practice with commercial wireless operators. Through the State Planning Grant process, public safety sites owned by state/local governments should be given priority for use in constructing the Band 14 RAN.
State Opt-out RANs (Band 14)	State Opt-out RANs are implemented by states that successfully execute an opt-out process. FirstNet should also consider the possibility that these states implement some or all portions of a Lower Core.
Commercial Built RANs (Band 14)	If FirstNet enters into partnerships with commercial wireless operators, these service providers would implement Band 14 RANs, presumably co-located with their own commercial RANs, and possibly sharing backbone/backhaul networks.
Shared RANs (Band 14)	If FirstNet enters into shared leasing agreements with commercial entities to utilize excess capacity, these entities would implement shared RANs, in which each eNB is connected both to the FirstNet Core and the commercial operator's core such that public safety traffic is routed through the FirstNet core and commercial traffic is routed through the commercial core.
Commercial LTE Core Networks	Commercial LTE Core Networks implement both Upper and Lower Core functions within a commercial wireless operator's network.
Roaming Exchange	In keeping with commercial practice, one or more Roaming Exchanges would be used to interconnect the NPSBN to the wireless service providers with which FirstNet enters roaming agreements. Roaming exchanges enable decoupling of these networks, permitting non-synchronous evolution of these networks.
State and Locally-Hosted Applications	State, local and tribal public safety entities implement a variety of jurisdictional-specific applications, typically in their owned/operated data centers. A primary business function of FirstNet is to provide mobile access to these hosted applications.
FirstNet Offered Services	As depicted in the FNN, FirstNet may implement a variety of network services in the Service Delivery Platform.

Figure 3 reflects key realities that FirstNet will face:

1) Commercial networks will not evolve in synchrony with the NPSBN; it is necessary to decouple these networks from the NPSBN, as depicted here, through a Roaming Exchange.

2) Grade of service (including coverage, priority, QoS, and preemption) offered in commercial networks may not meet the same functional or performance levels as provided by the combination of the paired FirstNet Core/Band 14 RAN.

3) Security levels available from commercial networks may not meet the same criteria as provided by the combination of the paired FirstNet Core/Band 14 RAN.

4) There is a practical limit on how many commercial bands (in addition to Band 14) can be included in user devices.

f. Backbone Considerations.

It is worthwhile to consider the backbone that interconnects the elements of a distributed EPC. The backbone, which connects distributed elements of the EPC to ensure nationwide service, is distinct from the backhaul, which connects the RAN sites to the EPC. In addition to the design and planning that will occur in consultation with state, local and tribal entities, there is need for design and planning for handling interstate connectivity. Possibly little to none of the backbone will be constructed by FirstNet. Rather, it will be sourced much in the same manner as is currently commonplace for many commercial service providers. Harris urges that in developing the network architecture, FirstNet evaluate commercial backbone offerings that are suitable for mission-critical networks, for example, the Harris Trusted Enterprise Network (H-TEN) that is specifically designed for nationwide mission-critical applications (Figure 4).

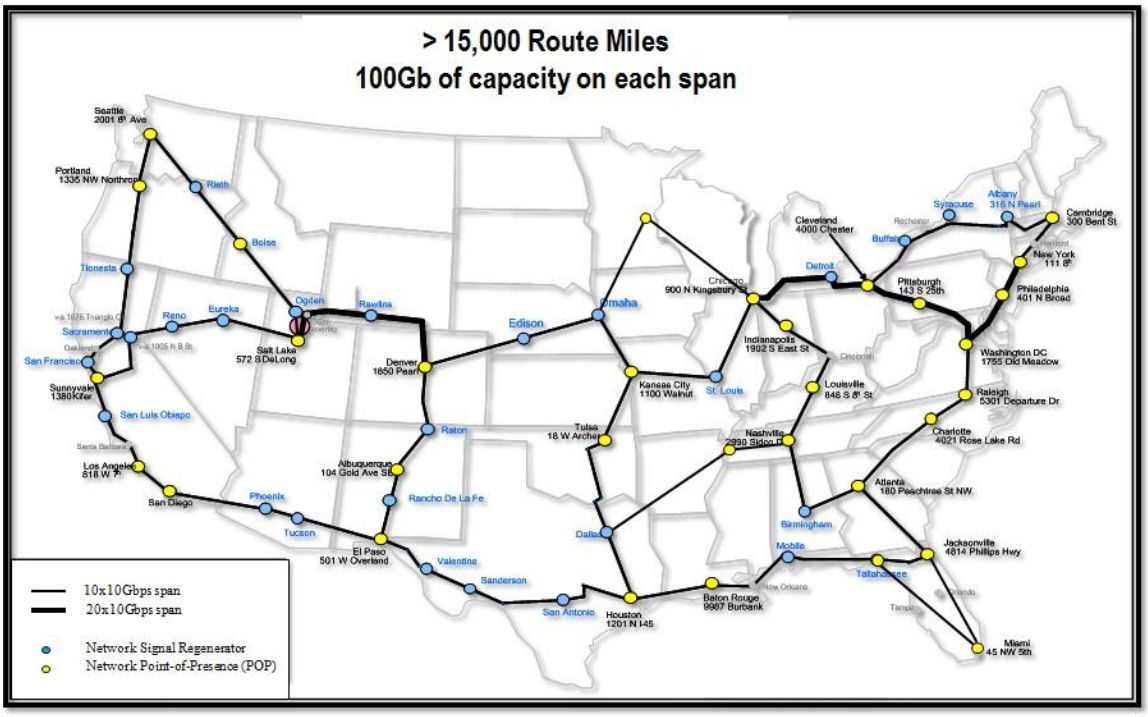


Figure 4: Harris Mission-Critical Backbone

Opportunities and Benefits

The layered network model described in preceding sections addresses important challenges that FirstNet will face, and correspondingly provides multiple opportunities for success as well as key benefits. These are summarized in the following table:

Financial Viability	FirstNet is positioned to benefit from two important conditions. First, through partnership with state, local and tribal entities, FirstNet can deploy network infrastructure on a large collection of pre-existing public-safety hardened facilities. In addition, many cities and counties have made significant investment in fiber infrastructure that can be brought to bear to ensure both a cost effective up-front CapEx investment and a manageable long term OpEx outlay. Second, FirstNet can today leverage the vast ecosystem that commercial mobile operators have created. Commercial mobile operators focus on a business model in which the majority of their cell sites are on leased facilities (in some cases all their sites are leased). FirstNet will have direct access to these same sites, both on a stand-alone basis through direct leasing, and in connection with potential partnerships with one or more commercial service providers.
Compliance with Statutes	The NPSBN differs from commercial mobile broadband networks in that its structure and requirements are defined by statutes and not by a purely commercial business plan that targets return on investment. As depicted, the layered architecture mirrors the key statutory requirements, and therefore endows FirstNet with significant discretion to implement its business model in compliance with these statutes.
Responsive to public safety needs	The NPSBN also differs from commercial broadband networks in its particular user base. It is important therefore that FirstNet focus on the unique needs of public safety and resist implementing a network that offers no significant benefit over what is available from commercial networks. These high value-add capabilities that meet unique public safety needs could support an average fee per user that is attractive to public safety entities, albeit probably higher than a less-capable commercial offering. As noted below, the full benefit of this proposition will be realized through convergence.
Convergence	In the long term, FirstNet and the NPSBN will help bring about two types of convergence. First is technological convergence: having a converged network and related applications that enable access to voice, video and data services tailored to the mission-critical needs of public safety. Second, as converged mission-critical capabilities are realized, economic convergence will enable a focused investment on a single converged platform, ultimately eliminating the need to invest in multiple divergent technologies and networks. Therefore, over time, there may be a reduction in funding for the construction of new LMR systems and a reduction of subscription to commercial network services, and the total outlay by public safety for communication would focus on the NPSBN and its continued deployment and evolution.

IV. The Development of Standards-Based Applications Is Crucial to the Network's Success

a. Framework/Organization Factors for Large Numbers of Quality Applications.

In considering an application framework, it is important to ensure that the quality of the applications is high while aspiring to the greatest number of applications possible. Applications are easiest to

develop, and therefore will proliferate, in an unconstrained environment with low barriers to entry and many potential customers. The Android™ marketplace, for example, has very few restrictions and millions of potential customers; hundreds of thousands of applications have been developed that meet a plethora of individual needs. However, few, if any, of these "apps" interoperate in any meaningful way and many have been developed to essentially supplant web browsers as a means of accessing commercial information.

Therefore, FirstNet's goal should be to ensure development of the maximum number of "quality" public safety applications that: 1) meet a need; 2) encourage interoperability; 3) provide security to the user; and 4) maintain the security of the network. The challenge for FirstNet will be the need to balance appropriate controls while not inhibiting substantive innovation.

b. Applications Furthering Public Safety's Mission.

The NPSBN could drive the development of a vast array of powerful, mission-specific and mission-critical, interoperable applications. To ensure this, FirstNet should enable interoperable applications by supporting formal industry standards for communications services and information elements and encouraging their use for all applications, rather than pre-selecting particular applications for deployment within the NPSBN.

Figure 5 illustrates this idea. For example, a situational awareness application for a law enforcement officer can be thought of as combining information received from several information sources and fusing and presenting that information in a manner that is optimized for a particular mission.

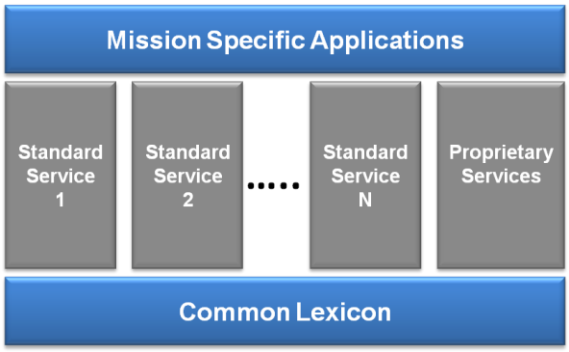


Figure 5

If the information services (e.g., Location Reporting services) and communications services (e.g., messaging) that underpin applications are largely standardized, different developers with specialized knowledge or value-added technologies can develop differentiated applications that interoperate.

This concept of interoperable, standardized applications is gaining industry traction. The Telecommunications Industry Association (TIA) Broadband Data Standards subcommittee initiated a project to develop a set of services and information elements that follow this model. This work will include both invention and the adoption of existing standards and commonly used forms. For example, the use of FIPS location codes could represent geopolitical areas, WGS-84 representations of geologic information, and perhaps adoption of Topologically Integrated Geographic Encoding and Referencing (TIGER) "shapefile" data elements for the representation of shapes. Harris believes that practitioner and industry cooperation in the establishment of these standards is critical to their success.

c. Interface Requirements And Other Information For Developers

To efficiently and rapidly develop applications in an open environment, commonly needed services must be well documented and supported. The 7/25/12 NPSTC SOR provides several examples of necessary network services, which include:

1) Location services that provide suitably authorized services and applications with the ability to determine the geographic location of users;
2) An Identity framework that allows public safety entities to manage the roles and identities of their users, and facilitates authentication of those users by other public safety organizations;
3) Authentication and Authorization services associated with those managed identities;
4) A collection of fundamental network services (e.g., Domain Name System (DNS));
5) Device management services that provide public safety organizations the ability to manage their user devices and applications.

Using these services as a baseline, FirstNet can enable the development of First Responder applications that are standards-based and operating system-agnostic. To further accelerate application design and deployment cycles, FirstNet also should develop network management and business systems integration standards and publish a network management interface standard that identifies an extensible framework with common underlying data types. This will support public safety's expressed need for real-time visibility into availability and status of applications and infrastructure supporting their various missions. The establishment of standard services is necessary, but not sufficient, for the establishment of a rapidly evolving ecosystem of secure public safety applications developers.

Because the NPSBN will be a critical national security resource, it is important that application developers have a clear understanding of the security assumptions under which the network was deployed, and clear guidelines for security implementation. Harris believes that FirstNet should, at a minimum, publish and maintain a document that describes the underlying security assumptions that application developers can assume in developing their own secure applications. This would include a compendium of application security requirements (see below) and documents describing best practices for secure services and peer-to-peer networking. Finally, since no information network or service infrastructure can be perfect from day one, Harris believes that FirstNet should manage a moderated, limited access, online developer forum to encourage the exchange of information about the "quirks" that undoubtedly will be found in deployed services and infrastructure.

d. Application Security Requirements.

Understanding user needs is critical in determining the specific security requirements for public safety applications. The 7/25/12 NPSTC SOR provides preliminary guidance in this area; however, it is important to recognize that different public safety missions require different levels of security. For example, applications and services that process criminal justice information typically are required to meet requirements established in the CJIS Security Policy (CJISD-ITS-DOC-08140-5.0), and applications and services that process personal health information must comply with HIPAA privacy and data security requirements. In addition, real-time communications services traditionally have supported optional end-to-end encryption. While only a subset of missions require this level of real-time security, often they are ones in which the lives of First Responders are most at risk.

e. Certification Requirements

Application certification is important and should focus on: 1) network impact; 2) compliance with network security requirements; and 3) compliance with adapted interoperability standards (e.g., use of the identity framework, etc). Without this focus, certification requirements could raise unneeded barriers to entry and cripple public safety application innovation. FirstNet should consider the application certification model employed for the Federal Communications Commission type

certification in which suitable "certification houses" validate products against established standards and report findings to a certification body.

In ensuring that public safety has the applications that it needs, a certification regime must allow existing over-the-top applications to be temporarily "grandfathered," providing public safety with time to replace their existing applications as part of the normal upgrade lifecycle. Moreover, whatever applications delivery framework is adopted, individual public safety entities must be able to continue to host and operate their own specialized application services to satisfy their diverse needs.

In the applications space, FirstNet has a unique opportunity to foster innovation by providing a stable, secure, well-defined applications infrastructure, and by facilitating cooperation among practitioners, FirstNet, and industry to continuously evolve the infrastructure itself to meet public safety's evolving needs. Throughout this process, public safety's special mission and need for local control of their mission, visibility into the network, best in class security, and other unique requirements, must be embraced as the first principal guiding applications development.

V. Proposed FNN Concept Creates Subscribership and Technical Challenges

As discussed above, FirstNet's network architecture and business model will determine the success of the NPSBN. With an architecture capable of delivering the truly interoperable services required by public safety in a way that is economically and technically optimal at the network, user device, and service levels, FirstNet will be empowered to deliver a network as prescribed by H.R. 3630. In this context, and while embracing many of the goals of the FNN Concept, Harris notes several issues that are raised by this proposal.

a. Service Levels Will Drive Subscribership.

Based upon extensive experience owning, building, operating and maintaining major mission-critical networks, Harris proposes a threshold principle essential to FirstNet's success: The NPSBN must deliver service level value that will drive and sustain subscribership. Given that this network is statutorily dedicated to providing service to First Responders with unique communications needs, it is

vital that its architecture provides mission-critical services and simultaneously delivers local control aligned with a national policy framework.

Some aspects of the FNN Concept may raise issues about desirable service levels from the subscriber perspective. For example, the FNN Concept appears to offer exclusively commercial grade service and reliability. While leveraging multiple commercial networks may increase network reliability in some circumstances, it is questionable whether in times of emergency that access to multiple commercial networks, all of which often are overloaded during crisis, will provide First Responders the broadband services they need. Moreover, the commercial infrastructure that most commercial carriers share (towers, fiber routings, etc) is not designed specifically to ensure mutual redundancy and minimization of single points of failure. [2] To deliver high availability, commercial service providers will be required to provide priority, preemption and quality of service capabilities to First Responders. To date, this has not been offered beyond Wireless Priority Services, and is the primary reason why FirstNet has the mission to create a dedicated nationwide interoperable broadband network for First Responders.

b. Service Cost Model Viability.

In designing, building, and operating statewide public safety networks, Harris has learned that a public safety service provider must clearly demonstrate to the customer the service to be provided, the cost of that service, and how it will meet public safety's unique state, tribal, and local needs. Currently, First Responders have access to LTE broadband services, provided by commercial service providers at commercial/consumer grade. FirstNet will need to differentiate the value of the NPSBN from competitive commercial offerings. If FirstNet does not offer enhanced services at good value, First Responders could opt to not participate in the NPSBN and continue to rely on commercial services.

[2] *See, e.g.*, David Goldman, "Sandy Knocks Out 25% of Cell Service in its Path," CNN Money, Oct. 31, 2012, available at: http://money.cnn.com/2012/10/31/technology/mobile/sandy-cell-service-outages/index.html?iid=Lead (stating that, "Wireless carriers reported to the Federal Communications Commission that 25% of cell sites in the core area affected by the storm -- 158 counties across 10 states, from Virginia all the way up to Massachusetts -- remained non-operational.").

From this perspective, the FNN Concept raises concerns regarding cost and differentiated service. The proposed diverse network, relying upon a hierarchy of several commercial services could suggest that each First Responder may incur multiple subscription and/or roaming fees from the diverse service providers. This could result in a cost and payment system that is complex, and could ultimately result in a high level of aggregate costs for access to many different networks. Additionally, it does not appear that this service will provide differentiation that could with certainty justify the complexity and expense associated with choosing FirstNet over commercial competitors.

c. User Device Cost Viability.

Harris congratulates the FirstNet Board for developing the FNN Concept as "a starting point for further discussions"[3] on how to ensure that FirstNet succeeds in its vital mission. In evaluating how this network architecture corresponds to FirstNet's duties under H.R. 3630, it is imperative that emphasis be placed upon how the network can deliver the services that subscribers demand on devices they can afford and readily use. Harris is confident that FirstNet will provide network architecture options that can deliver this opportunity to First Responders.

The FNN Concept suggests that the user devices operating on the NPSBN should operate on Band 14, four to five commercial bands, and a satellite band. Hosting this many bands in a single user device may create significant technical and implementation challenges. Moreover, manufacturers would be forced to create a dedicated set of devices at very low volume, and consequently very high cost, thwarting the goal of leveraging commercial technologies to reduce cost and enhance interoperability. Indeed, under the FNN Concept, using a ruggedized smartphone with mission-critical features and applications may not be possible.

[3] FirstNet NOI at 5.

VI. Further Research and Development

Harris suggests FirstNet focus research and development on the following key areas:

Cyber Security	In its Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the NPSBN, the Interoperability Board made four recommendations for consideration by FirstNet: • FirstNet should consider supporting implementation of a national framework for user identity management. • FirstNet should consider supporting implementation of a national framework for user identity federation to enable user interoperability across administrative domains within the NPSBN, where authorized. • Implementation of the national framework for user identity management and federation should include a set of guidelines and rules for applications to participate in the national identity management framework. • The agency, organization or entity that utilizes the NPSBN Identity Management framework should be responsible for enforcing authorization constraints on access to information as per their own security policy.
User Devices	FirstNet should engage in activities that foster the development of Band 14 user devices that meet the mission-critical needs of public safety and support the FirstNet business plan. These development activities should seek to maximize the leverage of commercial ecosystems and to identify and help fill gaps that are unique to a Band 14 public safety network.
Applications and Network Services	In the FNN Concept, a notable capability is the Service Delivery Platform. A key area for research and development is to foster the development of a layered solution that drives interoperability beyond just the transport network. Building the network on LTE standards will drive interoperability in the transport network. Significant effort is required to drive interoperability through network services and into applications.
Standards	LTE and other standards that are used to construct the NPSBN will continue to evolve. HR 3630 authorizes FirstNet to represent the interests of public safety in standards development activities, in consultation with the director of NIST, the FCC and the public safety advisory committee – §6206(c) (7). In commercial practice, participation in Standards development is aligned to research and development activities. FirstNet should mirror this relevant business practice, with the notable difference that the actual R&D activities would be performed by commercial entities that supply products and services to FirstNet.

VII. Conclusion.

Harris is eager to partner with FirstNet and all stakeholders in making the NPSBN a reality. To ensure the long-term viability of the NPSBN, FirstNet must choose network architectures and business models that drive subscribership, foster a converged network and services, and welcome states as key partners in designing and building the NPSBN. We thank NTIA and FirstNet for the opportunity to provide insight into models that will drive success, and look forward to detailing our proposals in the future.

Respectfully Submitted,

HARRIS CORPORATION

221 Jefferson Ridge Parkway
Lynchburg, VA 24501

Charles Shaughnessy
Vice President, Public Safety LTE

November 9, 2012