FirstNet Notice of Inquiry Response
Prepared by
NORTHROP GRUMMAN INFORMATION SYSTEMS

NTIA DOCKET #120928505-2505-01

NORTHROP GRUMMAN INFORMATION SYSTEMS, INC.

7575 Colshire Drive
McLean, Virginia 22102
(703) 449-3993

Point of Contact: Royce Kincaid
E-mail: royce.kincaid@ngc.com
Telephone: (571)-313-2114
Mobile: (202)-642-0605

November 1, 2012

Executive Summary

Northrop Grumman Systems Corporation, acting through the Northrop Grumman Information Systems Sector ("Northrop Grumman") is pleased to provide this response to the National Telecommunications & Information Administration's (NTIA's) request for comments on the FirstNet Nationwide Network (FNN) conceptual network design and framework for developing applications. Northrop Grumman is a leading global security company providing innovative systems, products, and solutions in aerospace, electronics, information systems, and technical services to government and commercial customers worldwide. Northrop Grumman has a 40-year heritage in providing trusted, mission-enabling public safety systems and solutions that help first responders and critical decision-makers communicate and collaborate, real-time, across organizational and jurisdictional boundaries, safely and securely. This experience includes building and operating a large scale, multi-agency broadband wireless network in New York City that supports both public safety and public service applications. Northrop Grumman has drawn upon its experience in New York as well as its extensive participation in the development of the National Public Safety Telecommunications Council (NPSTC) Statement of Requirements (SOR) in preparing this response.

The FNN Architecture Should Address Security and Reliability Requirements

The goal of FirstNet is to provide a platform supporting nationwide communications for public safety missions into the future. This goal can only be achieved if first responders have confidence in the security and reliability of the network and make the FNN their primary resource for public safety broadband communications. Wide scale FNN user adoption will be jeopardized unless the network is properly designed and implemented at its inception, overseen by responsible parties at a national level, and maintained to high mission standards of operation. Although the FNN will and should leverage off of commercial networks and municipal assets to the greatest extent possible, these networks cannot inherently be relied upon to provide the needed security and reliability that is required for first responders. Instead, it will be incumbent on the national FNN architecture to provide centralized network security,

cybersecurity, identity management and management of user priorities and quality of service at the outset. These functions must coordinate and interoperate with local capabilities.

The FNN Architecture Should Include a National Enterprise Network Core

The unique security and reliability requirements of the FNN are best met by establishing a Enterprise Network Core (FNN-ENC)[1] which constitutes a "national network core" as a central part of the FNN architecture (Figure 1). The FNN-ENC is a geographically distributed set of functions, isolated from commercial network components in order that FNN data and network traffic can be protected, monitored, managed, and secured separately from network traffic associated with the general public.

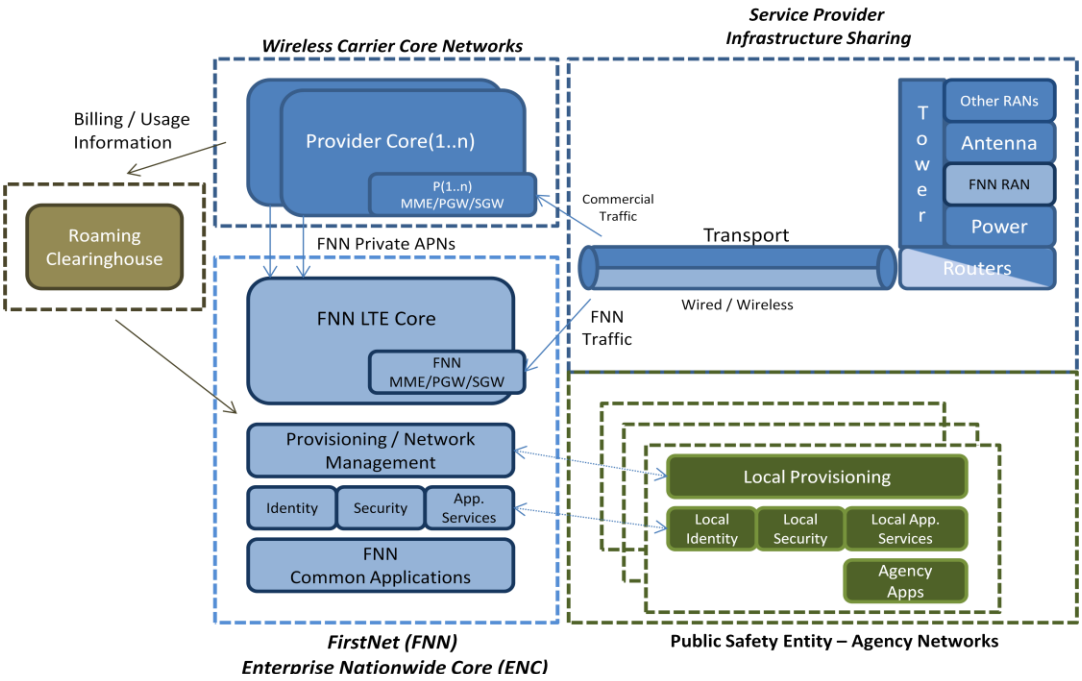

Figure 1 - Northrop Grumman Proposed - FirstNet Nationwide Network (FNN) Architecture

The proposed FNN architecture in Figure 1 allows FirstNet to leverage cost savings and speed to market benefits from existing tower, rooftop, and backhaul assets owned and operated commercially within the regional, state, rural, and local jurisdictions. However, any reuse strategy has to take into account the need for higher levels of security, redundancy, capacity, and must not compromise

[1] Enterprise Network Core (FNN-ENC) is a national network core infrastructure that supports key components needed to support a fully operable nationwide broadband system. Components include: provisioning, network management, identity management, security (cyber, physical, privacy), and applications delivery & certification.

availability during the most extreme conditions. This architecture assures these characteristics through the implementation of an FNN-ENC that supports critical features in security, identity management, and application service delivery while preserving the local control.

A Logical Sequence of Procurements Preserves the Integrity of the FNN

The inherently complicated nature of this project will be greatly assisted by the expertise of the FirstNet Board ("Board"). Proper sequencing of procurements for the FNN by the Board will assure early program success. The FirstNet Board should first consider issuing a Request for Proposal (RFP) for the Program Management Office (PMO) that is both accountable to the Board and responsible for finalizing requirements that will drive implementation procurements. After defining requirements, the PMO should issue a Request for Proposal (RFP) for the Enterprise Network Core (FNN-ENC). With the FNN-ENC underway, the PMO can then proceed with procurements related to Radio Access Node (RAN) deployments and service leasing arrangements with the wireless carriers. In parallel, FirstNet should establish a framework for the development, certification and delivery of applications which will enhance the utility of the FNN. This logical sequence of procurement activities supports flexible business models while preserving the integrity of a nationwide network.

FirstNet Applications Need a Framework for Certification and Accreditation

The adoption of 4th Generation Long Term Evolution (4G LTE) technology as the "baseline" for the FNN will enable first responders to use new "smart phone" applications in their daily regimen that will result in improved job efficiency and proficiency. Because of the sensitivity of information used and created by these applications, FirstNet should require application certification and accreditation procedures as well as standard applications interfaces. The FirstNet Board should consider designating the National Institute of Standards and Technology (NIST) as the certification/accreditation authority for FNN applications. NIST has done a commendable job with the LTE interoperability testing in Colorado. While NIST would have overall responsibility for this effort, there should be an RFP issued for a contractor to assist NIST with the standardization, certification and implementation of "apps".

Introduction

This document provides to the NTIA FirstNet Notice of Inquiry (NOI) Northrop Grumman's responses to questions raised by the FirstNet Nationwide Network (FNN) Board of Directors related to technology, architecture, business models, and procurement. Our responses are organized as follows:

- **Operability Requirements - Meeting Public Safety Mission Requirements:** Articulates the requirements that should be considered when implementing a Mission Critical network.
- **Network Sharing – Reuse of Service Provider Infrastructure:** Presents the benefits and boundaries of a business case that leverages service provider infrastructure while preserving public safety specific requirements for security and reliability.
- **Operational Efficiency – Reaching FNN Operations Quickly:** Communicates a possible timeline and set of priorities that builds off the establishment of a FNN Enterprise Network Core (FNN-ENC) that could allow the FNN to provide early success and establishes significant nationwide presence.
- **Mission Critical Voice – Enabling Voice Services:** Discusses the transition over time of the public safety administrative and mission voice requirements as technology matures.
- **Mission Support – Creating an Application Framework:** Outlines the timing and priorities in creating a certified delivery and management system for mission applications.

Our primary recommendations are summarized in Table 1 below.

Summary of NOI Recommendations to the FirstNet Board
1. **Security and prioritization requirements are vital to the success of the FNN and must be addressed from day one of the implementation of the FNN. In addition, resiliency against disasters and cyber attacks must be built into the system to preserve continuity of operation in extreme conditions.**
2. **The inclusion of an Enterprise Nationwide Core in the FNN architecture can address security and prioritization requirements and serve as a catalyst for leveraging commercial transport networks. The Enterprise Nationwide Core should be separate from commercial networks and feature increased levels of cybersecurity protections, privacy, and resiliency beyond what is typical of commercial networks.**
3. **The integrity of FirstNet as a single nationwide network can be preserved by a logical sequence of procurements that includes establishing a PMO, standing up the Enterprise Network Core and then proceeding with radio network deployments.**
4. **The sensitivity of information used and created by FNN users dictates that an application certification and accreditation authority be established for FNN users. NIST is a good candidate to serve as that authority.**

Table 1 – Summary of Northrop Grumman's Recommendations to the FirstNet Board

Operability Requirements - Meeting Public Safety Mission Requirements

FNN should seek to balance the benefits of commercial technology and infrastructure sharing while not compromising the critical characteristics that allow the public safety mission to be supported. This section discusses important considerations towards delivering upon mission critical requirements, such as cyber and network security, identity management, priority services, reliability, and redundancy; in a later section we will discuss application delivery and certification.

Network Security and Identity Management

The interests of the public safety community are best served by approaching the security requirements of the FNN in a holistic manner that addresses public safety's fundamental mission of protecting property and saving lives. As a case in point, public safety first responders depend on the 24x7 availability of their communications network to carry out their mission; inextricably linking reliability and security to the public safety networks. Weak and compromised network security undoubtedly reduces reliability and hence, availability. Without the proper security measures in place, no amount of reliability features, such as site hardening and backup power, can assure the highest degree of availability required of the public safety communications networks.

As a dominant global broadband wireless standard, LTE has been identified as the advanced communications platform for establishing a truly interoperable, highly scalable and cost-efficient nationwide public safety broadband network. However, the use of open and globally deployed standards, such as Internet Protocol (IP) that forms the core of the LTE-based public safety broadband wireless networks, considerably increases the vulnerability of these networks to malicious attacks, further underscoring the need for robust security mechanisms to protect these networks. The proof lies in the ever increasing number and sophistication of cyber attacks on ubiquitous IP-based technologies. Equally significant, the requirements of commercial carriers to secure their wireless networks and user communications may not be as stringent as those required by public safety. The implementation of LTE technology over these networks will not address the security and reliability requirements of public safety

emergency communications; hence, the need to integrate additional security and identity capabilities. These features include: network domain security, user domain security and application domain security. Each of these contributes to critical aspects of end-to-end security and, if not implemented properly, may expose the network and public safety users to disruptive and malicious cyber attacks. Even with these additional features, user information is protected only within the domain of the LTE network and not end-to-end from the user device to the public safety network operations and data center. As discussed earlier, additional security solutions would need to be integrated with the LTE technology to enable end-to-end secure communications that complies fully with the security requirements of public safety communications.

While data encryption is an important capability to protect the privacy and integrity of the user information, security for emergency communications must be broader in scope. Equally important are the requirements for strong user and device authentication, protection for data residing on devices, and physical security of the network assets such as communication towers, Network Operations Centers (NOCs) and Security Operations Centers (SOCs). Although these requirements are outside the scope of the LTE specifications, they are critically important for public safety's mission success. We strongly recommend that the FirstNet Board directly or through NIST and NPSTC take an active role in promoting the need to have future 3GPP standards releases address some of these requirements and the FNN be held to the security standards defined by the NPSTC SOR. Furthermore, the FNN architecture should include the integration of a secure Enhanced Nationwide Core (FNN-ENC) to assure network integrity.

Operability – Federated Identity Management

An unauthenticated user on the network would be a serious and an unacceptable security breach. While the LTE standard includes a framework for authentication, including roaming authentication, it applies only to the user device through mutual authentication between the user device and the LTE network. LTE's authentication mechanisms will have to be complemented with robust user authentication

techniques, such as multi-factor authentication, to ensure that only authenticated and authorized users are able to gain access to the FNN. In addition, this user-level authentication would be used to provide access to validated applications and priority services based on role and agency affiliations.

In order to promote and establish a highly operable broadband network across regions and tribal entities, the authentication of all users, whether they are on their home geographical network or visiting other geographical network locations, should be handled by a function best summarized as "Identity Management". The Identity Management function would reside inside a nationally managed and hosted Identity Clearinghouse. This prescribed method is both efficient and scalable, as it does not require technical and administrative arrangements between individual jurisdictions to enable roaming or user movement throughout the system.

A key aspect of the overall success of the FNN will reside in a comprehensive identity management scheme, backed by technology and standards. Devices can be identified on the network via common mechanisms used in industry (such as SIM cards), but extensions are needed to account for validation of the identity of individual users of such devices. Separate user identification allows for public safety officials to share devices, such as across different shifts, while enabling each user to have his/her own permissions related to network functions. The details associated with a user's identity will include information such as credentials, role, access, and clearance levels. By using a common format, nationwide users can be treated by the system across the entirety of the network as verified users, and the system can make decisions about security, Quality of Service (QoS), and access in a straightforward process. Each jurisdiction or agency will then be responsible to connect their existing enterprise to the LTE system using a clearly defined interface for identity and credentialing. Without this mechanism in place, it is hard to see how a truly nationwide interoperable network can be created.

Cybersecurity

In a recent speech to the Council of Foreign Relations in New York City, Secretary of Defense Leon Panetta stated "But the even greater danger – the greater danger facing us in cyberspace goes

beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorists attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation".[2] His comments underscore the absolute certainty that the FNN will be a high profile target creating the imperative that its components and interfaces must be protected, monitored, and threats identified and eliminated in real time. This will require a sophisticated and real-time approach to cyber defense never before anticipated or required for a public safety network.

This point becomes obvious because of the significant role this emerging network will take in providing a comprehensive communications capability to our nation's first responders and government organizations chartered to protect life and property. Protecting this national asset must be a high priority. A comprehensive Security Architecture which includes technology, policies, and procedures to protect the network 24/7 must be implemented. This will ensure the FNN is as protected as possible from malicious attacks in the face of evolving cyber threats and to protect mission information network reliability. To this end, Northrop Grumman recommends the adoption of the security requirements included in the NPSTC SoR (Draft_SoR120725)[3] which identifies three major layers of security that should be provided on the FNN and the devices it serves. These layers include user services, network services and transport services. Security at every layer of the system needs to consider these threats and provide the appropriate protection for the FNN users and infrastructure to reduce the threat to the network and its operations.

Prioritization and Quality of Service

A nationwide public safety broadband network must support prioritization and QoS to give public safety agencies the capability to prioritize network resources based on factors important to their mission operations and during extreme situations. This required support must have the appropriate configuration, management, and dynamic controls and interfaces necessary to ensure that user traffic flows of critical

[2] Transcript of Secretary of State Leon Panetta's Speech to Council on Foreign Relations, Subject: "Cybersecurity", New York City, October 11, 2012

[3] Draft Version of NPSTC Statement of Requirements (SoR), release: Draft_SoR120725, July 2012, Draft created in cooperation between public safety and industry on intended requirements for the future broadband system for public safety.

information related to a time-sensitive emergency event are prioritized. In addition, this prioritization must not only be isolated to the last mile services associated with a given solution, but extend from the user device to the command and control entity requiring the information. Thus, the need to establish priorities based on the application, agency, and responder roles, especially when disaster strikes, becomes even greater as first responders use a multitude of broadband technologies to attach to the FNN and then run applications with varied bandwidth demands and latency requirements.

Prioritization and QoS are two network access control and resource allocation mechanisms that previous 3GPP standards and legacy public safety communications systems did not adequately address. However, LTE supports both prioritization (with pre-emption) and QoS to enable public safety first responders to receive preferential treatment in the access layer through assignment of network resources based on their roles, applications type, end-user device type, geographic location where the request was initiated, and whether the user is on home network or roaming. Implementation of LTE QoS and Priority features as defined in 3GPP Release 9 and above will enable optimal network resource allocation that should strongly enhance the availability and reliability of public safety communications networks in meeting first responders' mission needs. However, this will only address the LTE layers of the system and such features must be extended through the end-to-end network. There is a need to expand the basic implementation of the Prioritization and QoS specifications to address stringent public safety performance requirements for end-to-end communications. It is recommended that the FirstNet Board in building the FNN adopt the NIST-led Public Safety NPSTC Broadband Working Group (BBWG) recommendations that provides for mapping of QoS and prioritization parameters suitable to first responder use case scenarios.

Because the FNN may interconnect with other commercial networks, there is a need to provide a framework for implementing Prioritization and QoS across commercial roaming networks. It is understood that this functionality may not be available on day one, but an effort must be made to harmonize future roaming agreements with the carriers to allow private Access Point Names (APNs) allocated to public safety to have prioritized treatment when necessary.

The implementation should provide enough flexibility for the regions to "localize" their Prioritization and QoS policies commensurate with their network operational objectives. In defining the requirements for implementing priority rules, Northrop Grumman recommends that more work be performed towards understanding sustainable and efficient methods of network resource allocation and pre-emption that can evolve as public safety applications and user requirements continue to evolve as well. Although the 3GPP Release 9 being planned for deployment by commercial carriers provides a list of attributes such as bandwidth, packet latency, and packet loss that are used to derive QoS parameter settings for various mixes of end-user applications, there are no real world results of optimal QoS parameter settings for incident scenarios with varying network conditions. Thus, the NIST-PSCR lab-based public safety LTE Demonstration Network needs to be replicated in other environments to enable additional tests and optimization of the QoS parameters under extreme conditions of mixed user traffic demand and network loading. Additional research and development (R&D) work is required to investigate methods and solutions that prioritize resource allocation and optimize QoS during emergencies when the need for resources is the greatest.

QoS and Network Security

Northrop Grumman has observed through performing network security operations on a broad range of mission critical networks that certain types of attacks on network security have a significant effect on application performance and QoS. However, it is the mission of QoS to ensure application performance and therefore, the two are inextricably linked. For example, both security and QoS can utilize common access control lists (ACL) for rules on how to treat traffic. Thus, a security mechanism that discovers abnormal traffic patterns could alert a QoS system to treat that traffic according to those rules. Furthermore, incorporating QoS within the network security policies will strengthen the public safety network against potential cyber attacks. Northrop Grumman recommends that additional R&D be directed towards integrating QoS and Security policies and automation to enhance and simplify the implementation of policy-based rules to securely manage network behavior.

Resiliency and Redundancy

A fundamental component of network resiliency is the ability to continue providing service during failures or times of stress on the system. From cyber attacks to natural disasters, critical central system components can be taken offline impacting the ability to communicate and ultimately crippling emergency operations. As a fail-safe mechanism, a survivable core of essential infrastructure should be developed for the FNN. This core needs to provide a small, rigorously isolated set of very basic capabilities on which to rely. There are several approaches to providing a survivable core. One approach is to build and maintain geographically redundant network cores. In the event of a core failure, or, as an example, the need to quarantine the core due to a cyber infiltration, the separate core would be brought on-line to provide minimum interfacing and functionality. A separate survivable core has the advantage of being independent of the operational network and would not be immediately affected by failures. As with any backup system, detailed failover procedural steps must be developed and the process must be exercised regularly in order to assure that it operates when needed.

Another approach is to provide redundancy within the operational core. By distributing key functions throughout the network, a successful cyber attack can be mitigated by removing only the affected section of the network and while still maintaining operational effectiveness. Additionally, using open standards and various vendors can aid in protecting against exploits at the expense of operational complexity. Northrop Grumman proposes having these functionally distributed, secure, operational core components as the most effective way to provide continuing service to users.

Network Sharing – Reuse of Carrier Infrastructure

There are two somewhat opposing factors that need to be considered when looking at "network sharing" agreements with existing tower and infrastructure owners. The two factors are described as follows:

The "Cost Reduction Factor" implies that in order to use existing infrastructure, the FNN should maximize use of existing "carrier" networks in both cities and rural areas that already serve millions of

commercial customers in order to gain cost efficiencies. Taken to an extreme, this could cause the FNN to compromise important special public safety requirements for increased cyber and physical security, reliability, redundancy, QoS, and path isolation (privacy) in an attempt to keep costs in line with commercial business models.

The "Mission Critical Network Factor" implies the need for a private secure and separate network infrastructure for public safety with increased redundancy and reliability built in to assure the network is available during emergencies when it is needed the most. The need to be highly reliable in times of extreme tension or tragedy such as 911 or Hurricane Katrina could drive the need for total separation between the FNN and commercial networks, thereby limiting the cost efficiencies associated with leveraging some aspects of commercial infrastructure.

An effective FNN architecture should balance these two factors. Shared use of network infrastructure between commercial and public safety users can certainly bring a cost-effective approach to the difficult construction challenges of the last mile broadband network infrastructure. Adoption of the worldwide supported broadband technology standard (LTE) by both public safety and large commercial wireless carriers creates significant opportunity for infrastructure and eco-system sharing. Opportunities exist for sharing radio communication tower facilities and equipment, including shelter, power, coaxial cables and antennas, and even connectivity through existing backhaul fiber and wireless components.

However, to meet public safety requirements, the FNN should have an Enterprise Nationwide Core (FNN-ENC) separate from any single existing carrier core assets or commercial infrastructure. The reasons for this are derived from the mission of the FNN to support the protection and safety of the public and those serving to protect it. FNN as a Critical National Infrastructure (CNI) must be a highly reliable and independent network that works at all times and is isolated from the commercial network components in order that it may be protected, monitored, managed, and secured separate from commercial networks serving the general public.

The Department of Homeland Security (DHS) considered in the *Communications Sector-Specific Plan – An Annex to the National Infrastructure Protection Plan, 2010* these issues related to emergency

responder use of commercial connectivity: "As the Communications Sector evolves, shared infrastructure could become more vulnerable to disruptions in service due to threats presented by terrorist and other malicious attacks, by natural disasters, and by human failure to adhere to best practices intended to ensure security. During emergencies, the transmission of critical information is often interrupted because of limitations in the amount of radio frequency spectrum over which a wireless service provider can send information, combined with spikes in attempts to access the Internet. The Communications Sector faces a major challenge in managing network resources and educating all users, including emergency responders, regarding the need for diverse access methods to the Internet to ensure that emergency communications are operable. The inability of emergency responders to get information where it is needed is a major concern. Communications Sector representatives from both industry and government are working together to resolve such issues."[4]

This observation by DHS is precisely why the spectrum has been allocated to public safety for the FNN and why the network has to be designed to provide isolation and redundancy with an isolated core network infrastructure. Using commercial infrastructure components can save valuable investment in last mile deployment of the network, but through diversity and separation at the core, the FNN can avoid having too much reliance on the commercial networks. This will avoid the possibility that actions taken either by the public or by adversaries would have negative impact on mission availability. The cyber security footprint, isolation of data paths, and protection of the boundaries of the network are vital to assure that any cyber or other attack on commercial components will not impact the FNN as a whole. It is understood that when sharing infrastructure, portions of the network may be impacted by events either man-made or natural in common with the commercial components; however, the integrity of the FNN and its overall operation is preserved.

In addition, the FirstNet Board has to be cognizant of the fundamental differences that exist between the public safety and commercial requirements with respect to network availability, security,

[4] National Infrastructure Protection Plan, Communications Sector-Specific Annex, Department of Homeland Security (DHS), 2010, pg13

QoS, and user priority and preemption when deciding a path forward. Network infrastructure sharing must not compromise any of the key requirements related to the safety and security of public safety's mission. A public-private partnership will need to address the technical, logistical, and administrative issues as well as the cost implications of addressing any differences that exist between commercial and public safety requirements.

A key business driver for the shared infrastructure approach is to assume that competition comes from multiple sources. The creation of an Enterprise National Core (FNN-ENC) that allows multi-vendor, multi-carrier interfaces at the boundaries gives flexibility at the edges of the network to reduce costs and accelerate network build-out. Whether built at the regional, state, or city level, if the FNN-ENC supports standards-based interfaces for RAN and infrastructure attachment, then the FNN will benefit from lower lease costs and equipment costs. Public safety has for many years been hurt by procurement strategies that are based on individual vendor components that are not interoperable, limiting competition and increasing costs. The selection of LTE for the FNN was intended to avoid this type of situation and must be preserved.

NIST should support research in the areas outlined above to ensure the overall reliability and availability of the public safety network in a shared network infrastructure environment is preserved. This should include considering the impact of an architecture that isolates traffic through the use of multi-vendor capable LTE core components.

Operational Efficiency – Reaching FNN Operations Quickly

For many years the discussions around a public safety broadband network have included the concept that a network of this type could be a "network of networks" whereby individual jurisdictional networks are separately built and eventually interconnected based on limited interface "standards" to create a nationwide interoperable broadband network. This approach can accelerate early deployments, but creates the risk of repeating the failings of Land Mobile Radio (LMR) to create nationwide interoperability. In creating the FNN, Congress mandated the creation of a single nationwide network,

not a spider web of interconnected separate networks. Consistent with that mandate, Northrop Grumman recommends that the FNN architecture include an Enterprise Nationwide Core (FNN-ENC) that serves a set of centralized functions to secure the network, manage users and support applications delivery. An early deployment of the FNN-ENC can serve as a catalyst for initial network deployments while preserving the nationwide network integrity intended for the FNN. Figure 2 summarizes how the FNN-ENC fits within the FNN architecture:

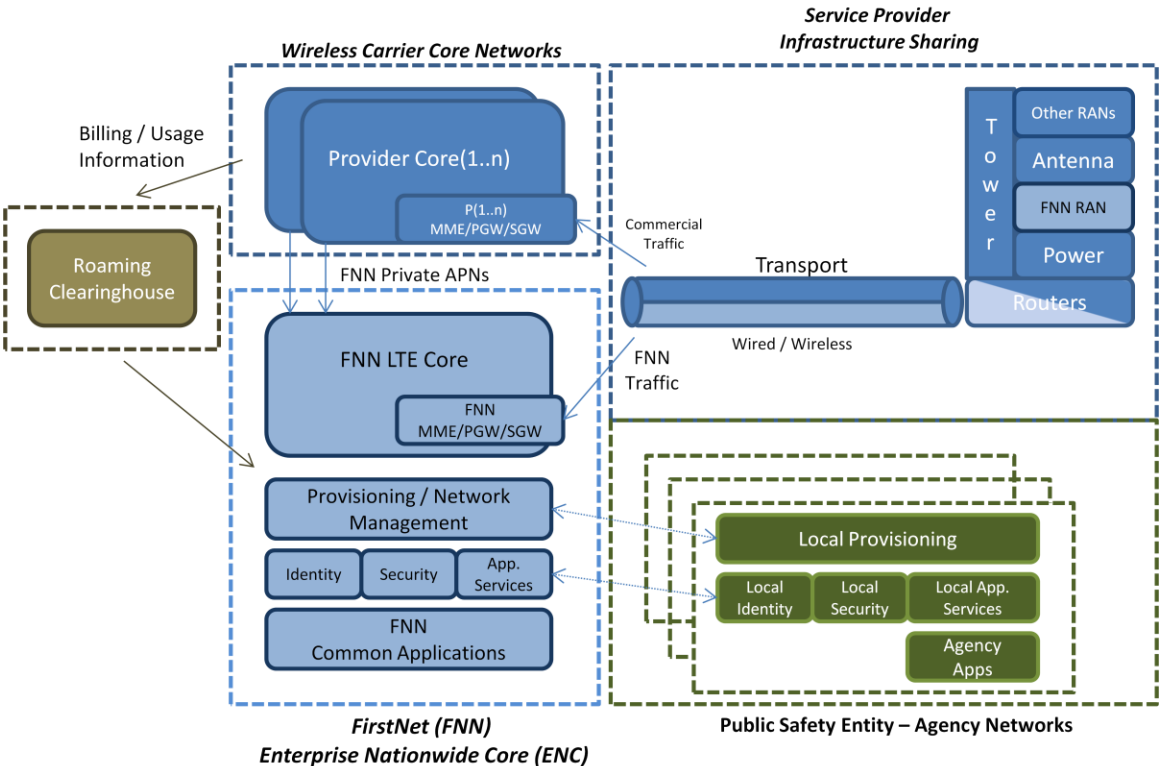

Figure 2 - The Proposed Architecture Contains a FNN Enterprise Nationwide Core (ENC) with Key Characteristics

The FNN-ENC should contain the following characteristics:

1. The FNN-ENC should first and foremost contain the LTE Core network components purchased or leased by the FirstNet Board and be under the direct control of FNN operational personnel. Drawing boundaries around the functions of the Mobility Management Entity (MME)/Packet Data Network (PDN) Gateway (PGW)/Serving Gateway (SGW) and the other network management components of the FNN, enables the ability to design, control and integrate the security, reliability, and redundancy necessary to assure the public safety requirements are met.

2. Critical functions will exist in the FNN-ENC including the public safety User Provisioning system which has extended functionality beyond what traditional service providers require because of the public safety need to do user based authentication, role-based Quality of Service (QoS) support, and additional protection of applications based on user access rights and privileges.
3. The FNN-ENC will provide a Federated Identity Management System (FIDMS) that ties to the provisioning system to allow the local identities to be propagated throughout the network to allow full network operability and access to both "common FNN applications" and "local agency applications" from either devices connected to FNN RAN infrastructure or through private APN connections provided as part of a roaming agreements with multiple and diverse service providers.
4. The FNN-ENC will have the responsibility for the protection of the network, its boundaries, its users (in cooperation with local security teams), and any other agency networks with which the FNN-ENC interfaces. As was discussed earlier, the cybersecurity threat to this network is real. The FNN should be considered Critical National Infrastructure (CNI) and therefore will require sophisticated protection, monitoring, and security response capabilities. The security will be monitored by the FNN Security Operations Center (FNN-SOC) team in collaboration with local Public Safety Entity (PSE)[5] security personnel in assuring FNN security.
5. A Service Delivery Platform (SDP) for FNN Common applications and supported PSE applications should be contained in the FNN-ENC. FirstNet users will use the SDP and an associated application storage facility to access "certified" applications that have been cleared for access based on role, position, and credentials. It is here where the connection between the identity of the user in the FIDMS and the application SDP becomes important because just having a FirstNet device does not necessarily allow one access to all agencies information and even common applications that may be made available by FirstNet and its partners. There must be a coupling between a user's identity and his/her rights on the network.

[5] Public Safety Entity (PSE) refers to the specific public safety organizations and their networks that are connected to the FirstNet (FNN) – Enterprise Nationwide Core (ENC) and contain the local applications, user provisioning, and local security protocols.

The following timeline is proposed to the FirstNet team to efficiently be able to provide nationwide coverage to support operational applications, proper security, and the necessary identity infrastructure, as well as begin edge deployments of 700 MHz D-Block RAN infrastructure:

1. The FirstNet Board should first put in place the program management office (PMO) and technical support team needed to define the procurement and technical specifications of the system.
2. The PMO should immediately define and then procure a FNN-ENC with functionality articulated in our response including network management, a set of private LTE core components distributed regionally and interconnected by diverse highly reliable connectivity, a common Federated Identity Management System (FIDMS), an Applications Service Delivery Platform (SDP), and a Security (FNN-SOC) Operations Center. The formation of this FNN-ENC will allow a smooth transition and clear demarcation of the role and interfaces needed by the local, regional, and/or state procurements of either green-field or shared private-public partnership RAN infrastructure.
3. Upon establishment of the FNN-ENC, the systems integrator responsible for the FNN-ENC should begin immediately integrating the various early adopters (agencies) by on-boarding the appropriate Public Safety Entities (PSE) with the intention of integrating their local Identity Management systems, security operations, and local applications into the SDP.
4. In parallel, while the implementation of the FNN-ENC is occurring, the PMO should work to put into place a set of roaming agreements with multiple wireless providers interested in providing connectivity to FNN users when they do not have 700 MHz Band 14 coverage or infrastructure in place to access to the FNN common applications or their own Public Safety Entity (PSE) local applications. These roaming agreements will provide for the provision of Private-APNs allowed through the FNN-ENC. This will assure secure, reliable access to applications delivered by the SDP to mobile users throughout the country, whether they have Band 14 700 MHz coverage or not.
5. Early deployments of RAN infrastructure should be assembled in parallel with the FNN-ENC by local, state, and regional agencies in an attempt to clearly define the process, technology, and interfaces needed to effectively and cost efficiently build out additional coverage areas.

6. Finally, as all of these activities culminate in a working proven system, additional regions, cities and states can be on-boarded into the FNN system through the interface provided by the FNN-ENC and as funds are made available to build additional Band 14 coverage.

Mission Critical Voice – Enabling Voice Services

Commercial LTE networks in operation today provide high-speed data services, but cellular voice services are provided through the commercial carrier's separate 3G networks. As LTE standards and deployed LTE elements evolve to support voice services, the mobile network operators will transition to a state where voice and high-speed data services are provided over one integrated LTE-based network. While cellular voice service is expected, the unique features of Push-To-Talk services may not be provided by future commercial LTE networks. The public safety community also has unique requirements for Mission Critical Voice (MCV) with direct talk-around service between local users in cases where network connectivity is not available (commercial or FNN). FirstNet's plans to enable public safety voice services while leveraging commercial network infrastructure should recognize these factors and should provide a phased approach to support cellular telephony, push-to-talk (PTT) services, and a long term solution that meets all MCV requirements.

MCV refers to the communication features and capabilities that support public safety to accomplish their mission successfully regardless of the status of the communications infrastructure. The features and capabilities include direct talk-around, PTT, a full duplex voice system, group call, talker identification, emergency alerting, audio quality, priority access, and preemption. According to the NPSTC, MCV communications entails the provisioning of all the aforementioned features and capabilities across the network and between users of the network.

It is widely recognized that all the features associated with public safety MCV cannot be delivered over currently-specified LTE standards. However, the capability exists to deliver many, if not most, of the features associated with MCV via alternative solutions application based services that supports LTE. The definition of these features and their priority by the public safety community needs to

be articulated and refined in relation to FNN future voice services. As an integrator of technology, Northrop Grumman continues to watch for guidance from federal authorities and the public safety communities on a broadly accepted definition for "MCV services" and on the prioritization scheme that might best serve public safety needs. Absent clear long-term direction, significant technical differences are likely to emerge between local, state, and/or regional public safety implementations that may jeopardize the goals for interoperability of the FNN. Like any technology, investment needs to be made to further the development of MCV. Unfortunately, commercial network operators have not placed a priority on MCV as a mode of operation; therefore it is important that the FNN through NIST and other industry investment seek to develop next generation voice over broadband capabilities. In addition, new modes of communication (e.g., full duplex always live communications) need to be considered as part of the future of operational voice. Military organizations are researching and even deploying alternative methods of communications that seek to improve traditional PTT using more sophisticated packet-based delivery systems and LTE may provide opportunity to do similar things in the public sector environment.

A phased approach to MCV implementation provides the service delivery flexibility best suited to this application. For example, an initial deployment could involve a suite of non-MCV capabilities (while offering both voice, data, and PTT services that align to important, but non-critical, operational needs). As MCV standards are established and delivery methods proven, existing systems could be augmented to provide MCV service levels for PTT voice.

Mission Support – Creating an Application Framework

Wireless broadband data services and open frameworks for application development to take advantage of those services have dramatically changed the way users' access information in a mobile world. Through common operating systems and user interface (UI) functions presented through those operating systems and the fact that the functionality provided by these applications are independent of the wireless network operator, application developers have developed literally millions of applications (apps) designed to improve the daily lives of the app users through access to information that has not previously

been accessible from a mobile environment.

While the FNN may seek to replicate the thriving development and delivery environments of today's commercial mobile broadband "apps", a critical difference that cannot be overlooked, minimized or trivialized is the explicit sensitivity of information that can now be accessed, used, and shared. The types of data that will become accessible over the FNN will be significantly different on many layers. The level of security controls that must be implemented to ensure network and data integrity must be taken into account in both the development of applications and potentially even more importantly, the hosting of those apps in a common application delivery environment for the FNN user community.

In the sections that follow, we will provide recommendations on application categories that would benefit public safety, describe the interface requirements that should be used, detail specific requirements for FirstNet's application certification process, outline security requirements public safety needs in its applications, provide recommendations on how the applications process should be structured organizationally, and describe possible delivery models for a FNN "app" store.

Recommendations That Would Benefit Public Safety: What Type of Applications Would Public Safety Users Like to See?

Over a period of several months, NPSTC hosted the development of the NPSTC Statement of Requirements (SoR) which identified the need for users to be able to access applications hosted from within the FNN, as well as applications hosted from within regional public safety networks. While each public safety entity has unique needs and associated unique applications, there are many common application types across the FNN community. FirstNet should prepare a candidate list of common FNN-Hosted Applications utilizing the NPSTC SoR as the guiding framework and present them for discussion in an open user forum at the earliest possible convenience.

The following types of applications are proposed for the FNN as either being included within the base connectivity service offering or as separate value-added services:

1. Mobile Virtual Private Network (MVPN) applications that allow the FNN user community to safely and securely access both the FNN and the applications/data that will now be made available. While

many system users will already have these types of applications, many will not or what they do have may not meet the security and encryption levels required for use on the FNN.

2. User-centric geospatial information that captures where users are, what equipment do they have access to, what skills they may have that can be brought to bear in emergency response, what is their current state "on/off duty", etc.
3. Common network "presence" or situational awareness information which can be graphically presented in the mobile environment via different layers to deliver, incident response areas, critical containment and resource distribution information (blockades, street closures, strategically and tactically deployed resources) both physical information (building types, power and water access, etc.) and environmental information (weather, flooding, hazard material contamination zones, etc.).
4. Traditional public safety-centric emergency management applications such as 911 Call Center Exchange services which would include Computer Aided Dispatch (CAD), Records Management Systems (RMS), and Logging and Recording functions. While these may not be used by larger municipalities as they already have standalone systems, the FNN community will include a significant number of smaller entities that could greatly benefit from being provided Tier 1 level emergency management systems. Along with those services come significant benefits in mutual aid, situational awareness and dispatch capabilities extended to a larger regionalized community.

Interface Requirements for FirstNet Applications

There are two interface functions that should be considered relative to FNN application development. The first is relatively straightforward and well understood by the application developer community. Utilizing the operating systems of the devices, applications need to have a common set of User Interface (UI) features and controls, much like the UI standards presented in both Android's and Apple's multi-gesture controls. This will greatly reduce the learning curve requirements of the FNN user community ensuring effectiveness in high-stress environments. In broad summary, these requirements would be:

- Consistent ways of starting, pausing, and stopping applications
- Consistent actions for pinch and or swipe functions
- Consistent behavior of applications "back grounding" when other applications are started

However, where the real complexity resides and where the application development community requires a paradigm shift, is in how the available data sources are accessed. As brought forward in the introduction of this section, the data that will be available for use on the FNN is significantly more sensitive than what would be available to the commercial community. As such, FirstNet should not allow open access to all data sources in a "free for all" approach but must ensure certain controls are in place to protect both the network and data integrity.

FirstNet, through the FNN, must provide a virtual data access layer that on one side has access to all of the data sources and on the other, presents an application programming interface (API) to allow access to those data sources via common data calls. At the same time, FirstNet must validate the data access request to ensure both at the user level and the data owner repository level, that the access request is authorized. It is unrealistic and detrimental to expect both an application developer and a data repository owner to code or allow literally thousands of connections to both locally and nationally significant data sources. Potential data sources may include:

- ***Local Public Safety Communications Gateway services*** – FNN should provide an application interface that manages the gateway services to regional and local public safety communication networks and the necessary protocol conversions.
- ***Federal Systems Gateway services*** – FNN should provide approved network interfaces and services to federal systems such as Criminal Justice Information System (CJIS), National Fire Incident Reporting Service (NFIRS), law enforcement information exchange networks such as LInX, or Center for Disease Control (CDC) data.

- ***Commercial Mobile Alerting Service (CMAS) gateway service*** – FNN should provide network interfaces and services to the CMAS system and allow public alerts to be announced across multiple regions as required.

Certification Requirements for FirstNet Applications

When an FNN user downloads an application from a hosted environment, he/she needs assurances that the application will function as advertised and that the application does not contain any malicious code that will either impede their public safety mission or compromise the network and data integrity as the application is utilized to provide its requisite functionality. There must be a process in place where applications are submitted to a Certification Authority for verification and approval prior to delivery to the FNN user community. This approval process ensures both consistent quality of application and that applications do not contain harmful code that would, at best degrade handset performance and at worst, compromise the network and data integrity of the FNN at critical moments potentially affecting both the safety of the public and the public safety professional.

Finally, application developers need to be given clear guidance on what network services are available from FirstNet so that they can develop the necessary applications to meet mission functions. This is best done by implementing open and standard protocols whenever possible but that are managed and monitored by an independent, respected, integrity-driven organization. It is our strong position that the NIST should be this authority. By taking on this mission, NIST should set standards for code quality to include:

- Ensure no malicious code is contained within an application
- Ensure that an application does not significantly reduce battery life of a device
- Ensure that applications are free from memory leaks that could degrade overall performance
- Ensure that applications only use approved APIs and library calls
- Ensure required network resources are used properly via proper QoS integration
- Ensure applications do not put unneeded strain on network resources and services.

Security Requirements Public Safety Needs in its Applications

Applications and their developers need to understand their specific security requirements in terms of confidentiality, integrity, and availability with respect to the specific mission requirements that the application is fulfilling. Many of these can be published by NIST in an interface document for use by the development community. This document should contain the core functions of defining requirements around ensuring the data the application is sending and receiving is getting to the appropriate, authorized recipients, can be trusted when it arrives, and that can be secured from access by others. There will be great challenges to meet these requirements but by no means can they be trivialized and unequivocally must be recognized and respected. The more security requirements FNN can support, the easier it is for application developers; however, it is unreasonable to have FNN support all required security features as use of these applications will be both on the FNN and, through roaming agreements, commercial systems. This again requires that the applications are fully verified, vetted, and certified to ensure their security posture is maintained in a mixed access environment. NIST, with proper direction, support, and funding, will be uniquely suited to support this mission. Further, NIST must be given the appropriate authority to both grant and deny the publishing of applications to the FNN hosted environment.

Organizational Framework for Applications Development

As stated above, it is recommended that NIST should have overall responsibility for the applications for the FNN. NIST has done an exemplary job with public safety broadband LTE interoperability testing and is well qualified to also lead the "apps" effort for FNN. In spearheading this effort, we recommend that NIST do the following:

- Hold an "apps" conference in the first quarter of 2013 to address the interface standards for FNN
- Establish an industry/end user working group to develop the interface standards for "apps"
- The working group will define the interface requirements for any applications put on the FNN
- The working group will define the certification and authentication process for any applications

- The working group will publish and release a document that defines the interface standards, defines, the certification and authentication process for “apps”
- NIST will define the standards for an “apps store” that would be hosted in a secure FNN environment and contain all of the “apps” much like today’s commercial “app” store
- Issue an RFP for a contractor to support the “apps” efforts for NIST
- As part of the FNN-ENC procurement, include the requirements for the contractor to deploy and operate an applications service delivery platform. This delivery model will support applications access, security, and certification.

Conclusion

Northrop Grumman would like to thank the NTIA and the FirstNet Board for soliciting the public safety user community and the industry for inputs on the implementation of the FirstNet Nationwide Network. Northrop Grumman is looking forward to further engagement with the NTIA on FirstNet. We recommend that NIST identify areas of study related to network architecture that seek to define quickly the key FNN-ENC elements we have defined in our response including: security, identity management, and application delivery. In addition, NIST should identify a strategy and timeline for the integration of voice into the network, which should include research and development efforts to identify new innovative ways to deliver Mission Critical Voice (MCV) using the LTE technology. As stated earlier in this document, it is recommended that NIST should have overall responsibility for the applications for the FNN. NIST has done an exemplary job with public safety broadband LTE interoperability testing and is well qualified to also lead the “apps” effort for FNN, and Northrop Grumman stands ready to support the development efforts needed to assure success for the FNN. Finally, NIST should continue their work with public safety, federal agencies, and industry in defining the technical requirements and standards for the FNN.