Booz Allen Hamilton’s Response to

National Telecommunications and Information Administration Notice of Inquiry

Development of the Nationwide Interoperable Public Safety Broadband Network

Docket Number: 120928505–2505–01

November 1, 2012

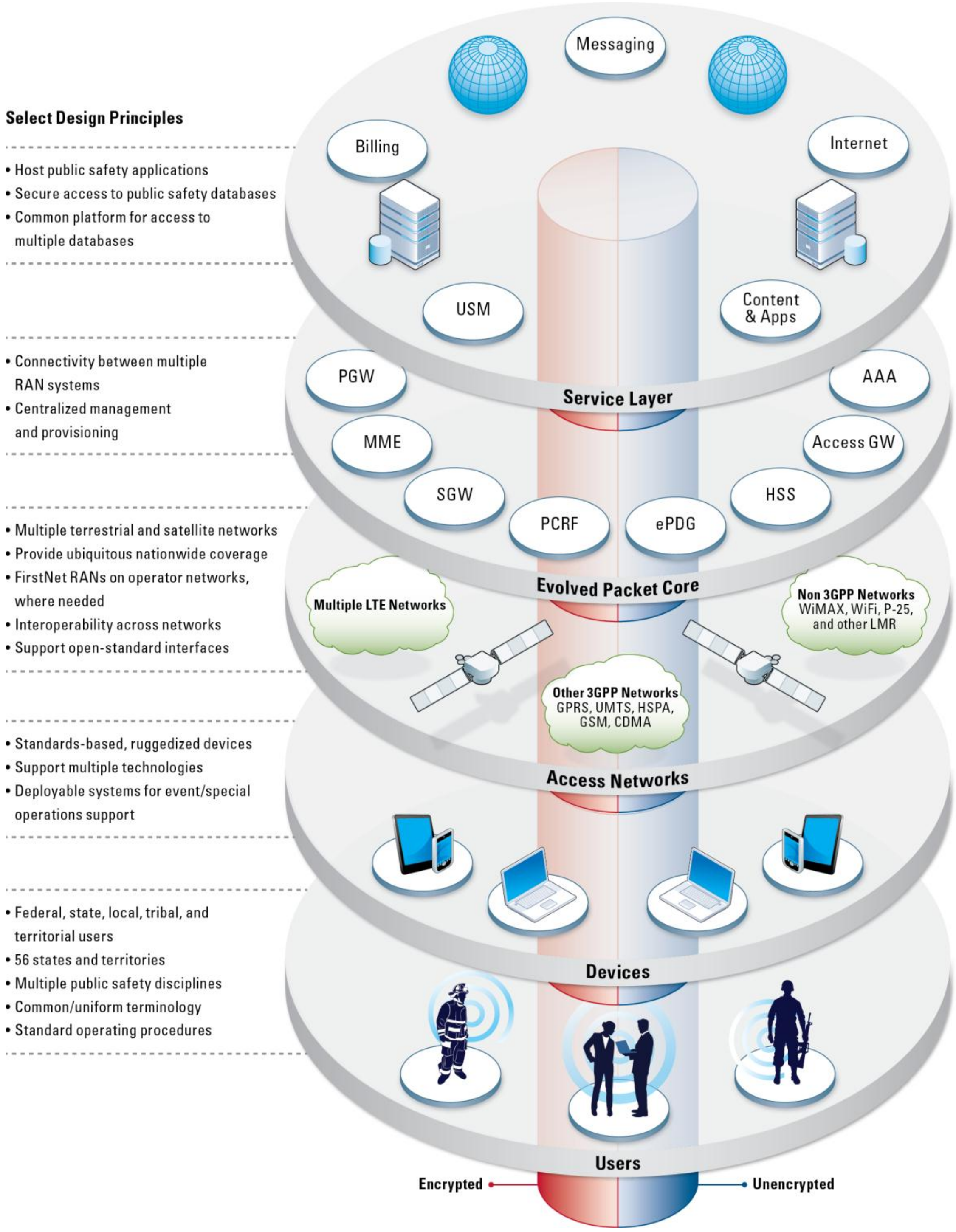
Booz | Allen | Hamilton

Booz Allen Hamilton (Booz Allen) is pleased to submit comments in response to the National Telecommunications and Information Administration's (NTIA) Notice of Inquiry (NOI) regarding the First Responder Network Authority (FirstNet) Conceptual Network Architecture (Docket No: 120928505-2505-01). Booz Allen has been actively involved in public safety communications for nearly two decades—working to modernize public safety networks, tackling the interoperability challenge, and developing deployable solutions for disaster and emergency communications. We believe these experiences provide us insight that can assist NTIA and the FirstNet Board of Directors ("Board") as it develops an interoperable public safety broadband network. We hope our comments will inform FirstNet's architecture development efforts and look forward to continuing this dialogue with NTIA and the FirstNet Board.

1. Response to FirstNet Nationwide Network (FNN) Conceptual Architecture

During its inaugural meeting on September 25, 2012, the FirstNet Board presented the FirstNet Nationwide Network (FNN) conceptual network architecture. The architecture is based on ideas and concepts that have proven successful in the commercial market and emphasizes leveraging the investments of the public sector and wireless industry to the maximum extent possible. We applaud the Board for providing a well thought out starting point at their first meeting. The architecture represents a good point of departure for discussion between the many parties that have passionate beliefs on diverse aspects of the architecture, including spectrum use, the viability of satellite networks to enhance coverage, the affordability of the end user equipment, and the sustainability of the network. Additionally, the Board has put forward an approach that is innovative and encourages progress at the "pace of business." We feel the architecture, as described, will challenge traditional paradigms of public safety communications network deployment and also capitalize on the emerging wireless innovations available in today's marketplace. Exhibit 1 illustrates our interpretation of the high-level FNN architecture and design principles we have inferred in each layer. This framework serves as the organizing structure for the remainder of our response.

Exhibit 1: Summary FNN Architecture and Assumptions



Select Design Principles

- Host public safety applications
- Secure access to public safety databases
- Common platform for access to multiple databases

- Connectivity between multiple RAN systems
- Centralized management and provisioning

- Multiple terrestrial and satellite networks
- Provide ubiquitous nationwide coverage
- FirstNet RANs on operator networks, where needed
- Interoperability across networks
- Support open-standard interfaces

- Standards-based, ruggedized devices
- Support multiple technologies
- Deployable systems for event/special operations support

- Federal, state, local, tribal, and territorial users
- 56 states and territories
- Multiple public safety disciplines
- Common/uniform terminology
- Standard operating procedures

There are many underlying assumptions of the Board’s thinking that were not explicitly contained in the overview presentation or brief. For the sake of our analysis, we hypothesize that the FNN architecture is based on several important technical, operational, and procedural assumptions identified below.

- FirstNet will make FNN capabilities available as quickly as possible and public safety users will subscribe to them
- Early FNN services will be deployed based on the capabilities of existing commercial Internet Protocol (IP) transport networks (i.e., LTE, satellite)
- Initially, FNN will support data and video service and, over time, provide interoperable voice, data, and video services with the necessary innovations and agreements for mission-critical service
- Existing public safety infrastructure will be made available to support the FNN architecture
- Incentives for commercial network operators to participate are sufficient
- Public safety user requirements are fairly uniform across levels of government, public safety disciplines, and geographies

Generally, these assumptions work well in the development of networks for use by mass markets. However, many of these assumptions warrant reevaluation, further study, and continued monitoring as the FNN becomes more defined. The true measure of success for the FNN architecture will not be based on deployment speed or technological elegance, but rather how well it meets public safety users’ needs in their unique operational environments. FirstNet can deploy all of the FNN segments shown in Exhibit 1, but still fall short of providing the communications capabilities needed to support public safety missions or the expectations set through the Middle Class Tax Relief legislation. For example, this perspective contrasts with commercial models where service interruption or temporary unavailability is an inconvenience to its subscribers, but generally tolerable given day-to-day usage patterns. The FirstNet mission necessarily places the Board in a role of “steward of the commons” where it will be accountable to public safety and taxpayers for meeting unique user requirements (e.g., survivable, accommodates unique public safety devices, data security) and solving FNN problems that present a direct and consequential impact on public safety and those being served. This responsibility will have a direct influence on the architecture and cost/benefit trades the Board must make in its decision making process.

Given that the architecture is in the very early stages, we believe that it is premature to evaluate, in great detail, its ability to effectively meet the high-level FNN objectives the presentation addressed—i.e., ubiquitous, reliable, redundant, interoperable, lower cost, and accelerated availability, as well as other public safety objectives omitted in the presentation such as, security, quality of service, device integration, and subscriber affordability. The architecture concept is detailed enough to ensure interested and passionate parties will react to the architecture and engage in the process to develop solutions to operational, technical, economic, and policy and procedural issues. To help organize this complexity, we have structured our response based on our assessment of the architecture against mission-critical requirements for public safety. Our intent is not to provide an exhaustive listing of key performance parameters, but to offer a framework for characterizing user and stakeholder expectations, our assumptions of how the architecture addresses these expectations and requirements, and any gaps or considerations that should be further explored as the Board continues to flesh out the architecture. We understand there are many more considerations that will impact the architecture, including issues such as core network architecture, the addition of secondary users, commercial spectrum sharing, the unique requirements of specific user communities (e.g., Federal), and existing infrastructure that can be leveraged for FNN deployment. We have largely left these strategic decisions to future comment. Exhibit 2 provides an overall summary of our initial perspectives. Following the Exhibit 2, we discuss these areas in additional detail focusing on public safety mission needs and business considerations.

Exhibit 2: Key Mission Needs and Business Considerations

Trade Space	Considerations	FNN Architecture Assumptions	Key Challenges	Considerations
Key Mission Needs	Coverage	• LTE using multiple carriers • Supplement LTE with satellite and deployable networks • Seamless roaming across networks	• Coverage in unique operational scenarios (e.g., canyons, air-to-ground) • Extensive use of satellite can be cost prohibitive • Roaming across networks and disparate technologies • Seamless coverage using multiple carriers and satellite networks • Participation of carriers to support coverage objectives	• Optimize satellite integration to minimize delay • Use-case scenarios to define unique operational environments • Coverage analysis to quantify % land area unserved by LTE • Roaming and service level agreements for hand-off across networks • Expand existing deployable assets for operation on FNN • RAN aggregation and network core sharing models (e.g., 3GPP – TS 23.251)
	Interoperability	• Connect networks via RAN • Devices operate on multiple networks	• Unknown access to public safety infrastructure • Communication across multiple LTE networks and technologies (satellite) • Distributed databases and information sources across networks • Too much interoperability can increase cost and complexity	• Standards-based interfaces between terrestrial/satellite RANs and core network • Parameters/agreements for roaming across networks (LTE, CDMA, HSPA, P25) • Rigorous compliance assessment prior to release (mixed vendor mode) • Information sharing permissions/rules for access to data across multiple networks
	Availability, Reliability, & Survivability	• Reliability/redundancy through network diversity • Distributed, hardened core network elements	• Reliability of commercial networks less than public safety requirement • Consistent survivability measures across wide range of networks • Continuity of communications using terrestrial (commercial, public safety), satellite, and deployable networks	• FNN meets minimum redundancy and equipment MTBF standards • Hardening measures across FNN networks (e.g., backup power, TIA 222-G/F) • Integrate Federal Emergency Management Agency (FEMA) and National Guard Bureau (NGB) deployable systems
	Quality of Service (QoS)/Priority Access	• Public safety grade QoS • Common QoS for all users	• Commercial networks do not provide needed QoS (e.g., low latency, jitter) • Latency/performance of satellite limits use across missions • QoS needs differ across missions and user communities • Priority scheme to balance and accommodate mission needs	• Optimize satellite integration to minimize delay • SLAs for public safety QoS with commercial providers • Design schema to retain QoS parameters during network transitions • Models for managing/dynamically modifying priority and QoS parameters
	Security	• Not specified	• Commercial networks do not meet security requirements for public safety • Requirements and certifications differ by user communities (i.e., Federal) • Consistent security measures across multiple networks/owners	• Implement cyber security program for FNN architecture (i.e., devices, applications) • Validate security requirements prior to deployment • Standardize and implement security measures and risk response across networks
	Device Integration	• Standards-based, ruggedized devices • Support multiple technologies • Centralized management and provisioning • ~100M devices to scale	• Some devices potentially unavailable for up to 5-7 years • Proprietary influence in device development • Affordable devices capable of operating on multiple networks • Economies of scale while supporting needs for customization • Authorized devices adhere to open standards and rigorous requirements	• "Core" devices to maintain economies of scale • Customize devices based on operational needs (e.g., mission, rural vs. urban) • Rigorous compliance/interoperability assessment prior to release • Accessories tailored for unique use (e.g., ruggedized cases, battery packs)
Business Considerations	Deployment Schedule	• Leverage existing commercial/public safety networks • Accelerate FNN availability (2013-2014)	• Meet public safety requirements through commercial deployment model • Participation of multiple carriers/agencies to support FNN build out • Ability to coordinate and manage the host of activities and milestones that must be met to successfully commence implementation in 2013-2014	• Phased approach to introduce broadband to users and evolve over time • Pilot FNN architecture in different regions to test architecture concepts and understand regional requirements, gaps, and expectations • Manage FNN rollout schedule and the portfolio of activities required to meet accelerated timelines
	Affordability	• Lower CAPEX and OPEX • Global economies of scale • Leverage existing infrastructure	• Unclear secondary user base (e.g., transportation, hospitals, utilities) • Unknown ability to leverage existing public safety infrastructure • Unknown willingness of terrestrial operators to support FNN • Public safety budget for FNN costs with limited understanding of business model and subscription or device costs	• Define FNN user community and existing infrastructure that could be leveraged • Cost implications of including secondary users • Right-size QoS scheme to mission needs to manage costs • Lease spectrum to incentivize carriers to provide QoS at a reasonable price

1.1 Coverage

A key FNN objective is to provide ubiquitous wireless coverage across all 50 States and 6 territories for federal, state, tribal and local government organizations. The proposed FNN approach will leverage available terrestrial, satellite, and deployable infrastructure by aggregating the coverage from each of the respective networks to create a nationwide footprint. This footprint must accommodate a number of operational environments, many of which are unique to public safety. For example, many rural public safety agencies operate in remote and sparsely populated areas, such as deserts, heavily wooded areas, dense mountainous regions, canyons, and parks, where infrastructure often does not exist due to a limited commercial user base. Urban public safety agencies also conduct operations in areas that present physical coverage challenges, including the interior of buildings and tunnels. The unplanned nature of many public safety missions, the typical lack of coverage from existing networks, and the criticality of wireless communications to both mission success and safety, necessitate that coverage be available in these areas to the extent that it is feasible and affordable. In many of these areas, satellite technology is often seen as the logical solution for areas uncovered by terrestrial networks; however, the characteristics of satellite technology do not fulfill some public safety operational needs. The FirstNet Board will need to engage the public safety community collectively and individually to understand these unique needs in un-/underserved and challenging coverage areas before committing to satellite coverage as a universal solution for uncovered areas.

By developing a thorough understanding of minimum user requirements and priorities, FirstNet can make business decisions regarding the extent and type (e.g., LTE, satellite) of coverage that can be afforded. Additionally, support for research and development (R&D) of solutions for integrating disparate networks and technologies will allow FirstNet to maximize coverage through the use of the best available solution in a given area based on cost, schedule, and performance factors.

1.2 Interoperability

The convergence of public safety onto a shared network presents a tremendous opportunity to significantly improve interoperability across jurisdictions and levels of government. While this convergence does much to address some of the key technical challenges (e.g., proprietary technology) that have plagued legacy communications systems, a number of non-technical issues must still be addressed to realize interoperability. For example, agreements and operational procedures must be established to enable interoperability between agencies. These agreements must provide not only authorization for establishing interoperability, but must harmonize policies such as security mandates, software updates, encryption key management, and communications protocols. Additionally, capabilities and procedures must be identified to enable roaming across networks using a universal device. This requires not only agreements among public safety organizations, but also between FirstNet and commercial service providers to allow access to commercial networks using devices that are subscribers on multiple networks. The interoperability of data systems will also be critical to enable access to applications and common services across agencies when desired. Technical and policy issues associated with data formats, access and security protocols, and storage must also be considered to enable seamless data sharing across platforms and networks.

The FNN will be deployed using a phased approach, requiring interoperability with legacy systems in some areas until the FNN is fully implemented. Technical (e.g., interoperability gateways) and operational (e.g., policies, procedures, protocols) solutions will be needed to ensure FNN designs and agreements—both among government agencies and with commercial service providers—will enable interoperability. Additionally, understanding the policies, formats, interfaces, and protocols associated with existing agency data systems and services will enable FirstNet to develop standards, guidance, and agreements necessary for interoperability.

1.3 Availability, Reliability, and Survivability

The FNN architecture represents a significant shift in the way public safety communications deliver the required availability and reliability for users. The mission-critical nature of public safety communications necessitates that capabilities be readily accessible and reliable regardless of the environment or situation. This challenge is exacerbated by the reality that public safety communications capabilities is often at its peak during and after catastrophic incidents that threaten to damage or disable communications infrastructure either directly, or by impacting critical services such as electric power or commercial telecommunications. When systems are damaged, safety hazards, blocked roads, and high demand for restoration services can result in sustained outages throughout the time when capabilities are needed most.

Traditionally, public safety agencies have achieved reliability through stringent design of private networks. The FNN will leverage multiple systems, such as government-owned networks, commercial cellular networks, and satellite networks to provide the robustness and redundancy needed to achieve the high levels of availability, reliability, and survivability required by public safety. However, particularly in areas where multiple networks are not available, the FNN architecture model must exceed those of typical commercial carriers in a number of ways. For example, the tolerance for dead spots and dropped calls is much lower for public safety users compared to commercial users, and could require additional sites to improve coverage reliability. Minimum levels of audio quality and error rate must also be achieved to ensure urgent messages are clearly and fully received. Additionally, the FNN must be designed to withstand natural disasters and intentional attacks. Measures such as hardening infrastructure and network elements, building redundant communications paths, and supplying backup power must be considered to ensure continuity of communications for FNN users.

The availability, reliability, and survivability designed into a system will have a direct impact on cost. Understanding the minimum needs of FNN users will be necessary for FirstNet to assess various design tradeoffs. Failure to meet these needs can result in stakeholders choosing not to adopt the system, or worse, putting lives, property and mission success at risk. Addressing these needs early in the system development process, and ensuring R&D and commercial coordination efforts account for these needs, will help FirstNet to identify and leverage solutions that best balance cost with network performance.

1.4 QoS/Priority Access

To meet the needs of public safety users, the FNN must provide a high QoS (e.g., low latency, packet loss), especially for communications deemed critical to the protection of life or property. One of the critical decisions not included in the current FNN architecture concept is its support for mission-critical voice communications. If the architecture is intended to support mission-critical voice, it will need to be made much more robust to provide the required QoS. Push-to-talk voice communications are generally considered critical by most public safety agencies, and various dial-to-talk, data, and video communications may also be considered critical depending on the information being communicated, the user, or the situation. The QoS provided by a typical public safety land mobile radio (LMR) system today can serve as a good benchmark for the QoS public safety users will likely expect from the FNN for these critical communications.

Although LTE technology promises to deliver high data rates by today’s standards, large user populations and the use of bandwidth-intensive applications (e.g., video, large file transfer) could quickly saturate FNN resources—especially during major incidents when network traffic may be abnormally high or when network resources are reduced due to damage or scheduled downtime—resulting in reduced QoS. Further, today's commercial cellular and satellite networks, which the FNN is envisioned to leverage for expanded coverage and capacity, are not designed to provide public safety QoS. These circumstances require careful planning and agreements among stakeholders with regards to the prioritization of FNN traffic based on a variety of factors, including the application used, type of user, and situation, to ensure QoS meets user needs and expectations. In addition, FirstNet must carefully design the FNN priority access schema to balance differing, and sometimes conflicting, requirements for access to network resources across user communities.

FirstNet can support public safety QoS by developing SLAs with commercial providers to best meet those needs. As part of the SLAs, carriers should model their QoS metrics, such as usage, call blocking, dropped calls, average frame error rates, average throughput, delay, jitter, and customer complaints as part of their vendor qualification process, so that QoS issues can be adjudicated against public safety expectations before carrier selection. FirstNet can then work with developers, commercial providers, and public safety users to research and develop solutions for optimizing bandwidth usage for both systems and applications. Additionally, SOPs and permissions (i.e., the ability for a specific user to access a particular application) for application usage should be established to help ensure proper balancing of system resources.

1.5 Security

The FNN architecture concept is largely silent on the issue of security and what elements would need to be included in the architecture to secure what will surely be one of the nation's critical infrastructures. The nation is facing more frequent and sophisticated threats to the cyber security and resiliency of its networks. The prevalence of IP-based architectures dictates the need for robust cyber security measures to effectively respond to risks. The FNN, subscriber devices, and data at rest or in transit must be protected from both malicious and unintended attacks (e.g., denial of service, message modification) that could reduce network performance or the integrity of important information. Additionally, information communicated by public safety can often be considered sensitive and must be secured in accordance with applicable security requirements and agency policies. As the FNN provides public safety with opportunities to leverage new and more robust applications, the amount of sensitive information, such as personally identifiable information (PII) and agent/officer locations, residing on devices and traveling over the network will continue to increase.

Often, the policies, statues, and guidelines that govern communications security vary among different user groups and levels of government. For example, all wireless federal law enforcement communications is considered to be, at a minimum, “sensitive-but-unclassified,” and therefore must be protected using Advance Encryption Standard (AES) encryption or higher, and all cryptographic modules must be Federal Information Processing Standard (FIPS) 140-2 certified. Also, federal communications devices are subject to stringent management and security guidelines, such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and DoD 8500.2, and many agencies are beginning to require two-factor authentication that conforms to FIPS 201-1 and Homeland Security Presidential Directive (HSPD)-12 requirements. Conversely, most state agencies are not required to use encryption for routine law enforcement communications and cities and counties generally follow individual state or local guidelines. Although they vary across agencies, ensuring individual security requirements are met will be essential to promoting and enabling adoption of the FNN at all levels of government.

FirstNet should engage its stakeholders and standards bodies (e.g., NIST) to develop and prioritize security requirements for various user groups, applications, and operational situations. Working with these groups and service providers, FirstNet should also conduct a thorough risk analysis to identify threats and vulnerabilities to the various system elements (e.g., networks, devices, applications). FNN solutions will need to address these risks, as well as specific challenges—such as achieving interoperability among agencies with different security policies and ensuring minimum security requirements across interconnected systems—associated with a network involving multiple agencies, jurisdictions, and owners. FirstNet should also develop comprehensive security plans that define how security solutions will be implemented and maintained by FNN solution provider(s), and tested, certified and monitored by the cognizant government authority.

1.6 Device Integration

The FNN architecture makes some significant assumptions about the devices that can be used on the network. Most notably, the architecture will require a device that can potentially work across multiple bands and technologies (e.g., LTE, satellite, existing public safety systems). Such devices are not currently available to public safety. Further, due to their varying mission, roles, and operational environments, public safety users have a diverse set of needs with regards to the capabilities and form factor of their wireless communications devices. For example, firefighters require a ruggedized device that can be operated with gloves, while undercover law enforcement agents require devices that look like typical civilian cellular devices. Some police cruisers require a universal serial bus (USB) adapter to connect to their mobile data terminals, while air and marine personnel require devices that can be installed and certified for use in aircraft and marine vessels. Most public safety users require the ability to communicate directly with other users within a localized area, independent of network infrastructure if the network is unavailable due to damage or coverage limitations. Additionally, seamless roaming among disparate systems and seamless interoperability with legacy devices requires that user devices have the ability to operate across multiple networks and technologies.

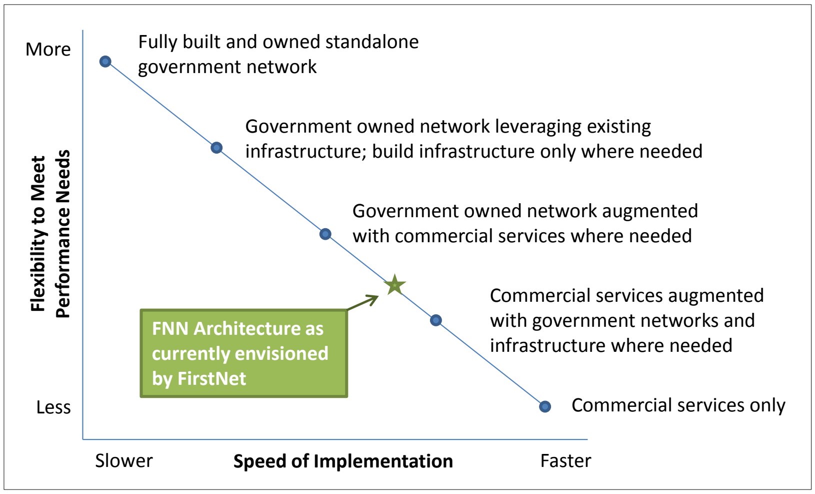
Developing affordable devices that meet the unique and diverse needs of public safety users will be a challenge due to current technology limitations (e.g., providing the requisite power for direct device-to-device communications in a commercial-like device) and limited economies of scale when compared to the civilian commercial market. Discussion at the Board meeting indicated the possibility of approximately 100 million devices on FNN. We believe this number to be high, but may be the volume required to make devices affordable. Further, to keep pace with latest technologies, public safety will need to adopt typical commercial device technology refresh rates of 2-4 years rather than the 5-10 year rates of most legacy public safety devices. This necessarily becomes a jurisdiction-specific affordability issue that will affect overall subscriber and device break-even assumptions of the FNN architecture and deployment roll-out schedule.

1.7 Deployment Schedule

The Board's objective of accelerated deployment dictates an architecture and deployment approach that is largely unfamiliar to the public safety community. Traditional government-led LMR network development adheres to what could be considered lengthy systems engineering lifecycle processes that focus heavily on collecting, dissecting, and validating operational requirements and designs to ensure initial deployment fully supports user needs. Accelerated FNN availability assumes a phased or rapid-prototyping approach that incorporates unique geographical and user requirements over time. This shift from a traditional, customized requirements-based architecture, to an architecture that addresses requirements iteratively and re-purposes existing assets to minimize development costs and accelerate availability requires that FirstNet carefully manage stakeholder expectations and understand minimum performance requirements to enable public safety use of the network.

The concept of accelerated availability is based on a number of key architecture assumptions that could ultimately influence the FNN deployment approach. Exhibit 3 presents a continuum of deployment approaches ranging from traditional, government-owned networks to the sole use of commercial services.

Exhibit 3: FNN Deployment Approach Continuum



The FNN architecture is based on several assumptions that attempt to balance the tradeoff between speed of implementation and network performance, including the ability to leverage public safety and commercial infrastructure, adapt LTE networks for mission-critical use, and integrate and roam across networks. Should any of these assumptions prove invalid, the deployment approach begins to shift towards the government-owned network and schedule slows. If, in some cases, public safety elects not to participate or make infrastructure available for FNN deployment, the approach begins to rely more heavily on commercial services, reducing the flexibility to meet mission-critical performance needs of public safety. Validating assumptions early will help ensure FNN continues to move towards a target architecture that appropriately balances deployment schedule and performance objectives.

1.8 Affordability

Public safety agencies across all levels of government are facing fiscal constraints and rising costs of operating and maintaining legacy communications networks. The state of existing technology dictates that public safety agencies continue to support existing networks for mission-critical voice until FNN provides integrated voice and data capabilities. As a result, near-term FNN service offerings and subscription costs present an increased cost to state and local municipalities strapped with deficits and/or limited budgets. The near- and long-term FNN affordability proposition for public safety remains unclear based on a number of highly variable factors such as inclusion of secondary users, the ability to leverage existing infrastructure, and a sufficient understanding of operational requirements to determine the trade space in cost and performance.

Exhibit 4 provides an initial characterization of the affordability trade space between user-driven performance requirements and key enablers that will help drive down costs and improve affordability for FNN users. These factors are categorized using the major cost areas that will ultimately impact FNN affordability: capital expenditures (CAPEX), operational expenditures (OPEX), and the cost of user devices.

Exhibit 4: Factors Impacting Affordability Trade Space

Capability Area	Example Applications	Key User Benefit
Network CAPEX	• Extent existing infrastructure can be leveraged • Ability for commercial networks to meet availability, reliability, and QoS requirements • Ability to provide seamless integration across networks	• Coverage • Capacity • Interoperability • Availability, reliability, and survivability • QoS • Security

Capability Area	Example Applications	Key User Benefit
Network OPEX	• Extent commercial services are utilized • Ability to enhance business case for commercial service providers • Ability to minimize maintenance costs on government infrastructure • Speed at which FNN can meet all critical requirements to enable transition off legacy systems	• Availability, reliability, and QoS requirements on commercial networks • User traffic loads on commercial networks • User acceptance of FNN enabling transition off legacy systems
User Devices	• Extent commercially available devices can be leveraged or modified • Ability to develop standard devices that can be "accessorized" to meet unique needs • Ability to develop universal devices that can access multiple network types • Device upgradability	• Diversity of device form and functionality requirements • Extent the use of the most modern technologies must be maintained in the future

Overall affordability across each cost area will be largely driven by minimum acceptable performance requirements, and the extent to which existing infrastructure, commercial services, and standard user devices can be leveraged to meet these needs. For example, the need for significant expansion of existing infrastructure to meet coverage requirements will likely increase costs, while the ability for existing commercial services to meet QoS needs will likely decrease costs. We offer several considerations below to help manage FNN affordability.

- ***Define minimum acceptable requirements for user adoption***. FirstNet should work with the user stakeholder community to understand the criticality and priority of user requirements. Based on this understanding, FirstNet can baseline the cost of providing the minimum performance required for user adoption of the network, and conduct tradeoff analyses on requirements above the minimum to determine solutions that will provide the optimal mix of cost, schedule, and performance.
- ***Partner with industry to manage affordability.*** Due to the relatively low number of public safety users compared to commercial users, recurring user fees would need to be very high to support a commercial business case for meeting certain priority requirements specific to public safety (e.g., priority access, coverage in unpopulated areas) on existing commercial networks. FirstNet should work with industry to offset

these costs through partnership agreements, such as providing carriers secondary access to public safety spectrum and infrastructure.

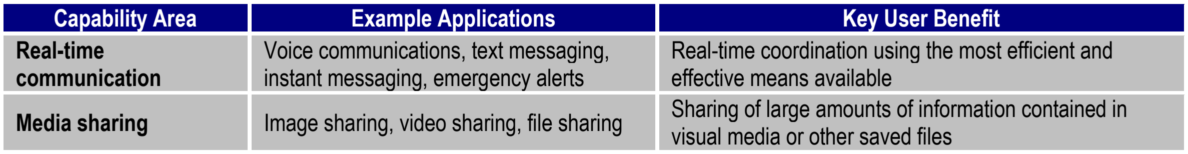
- ***Drive towards standardized equipment.*** The cost of equipment will be driven largely by economies of scale. Therefore, standardization of equipment across the FNN and particularly the ability to leverage or modify commercially available equipment for public safety use could help manage costs to FirstNet and its users. This is particularly true for user devices, of which certain models are produced by the millions to serve a large commercial user base. However, the unique and diverse needs of public safety users present a challenge to using "off-the-shelf" equipment designed and configured for use by a commercial user on a single network. FirstNet should work with its stakeholders and industry to enable—(1) R&D of standardized equipment that utilizes commercially available equipment to the extent possible, and (2) R&D on potential accessories that could be used to customize or enhance the capability of this standardized equipment.
- ***Leverage SOPs to manage network usage.*** Many costs associated with the FNN may be driven by predicted and actual and usage of the network. In some areas, FirstNet may need to build new infrastructure to handle predicted network traffic that exceeds the capacity of existing infrastructure. Inefficient or excessive use of the network for non-critical communications could result in high user fees. FirstNet should work with the user community to develop SOPs for use of the network, particularly for the use of bandwidth intensive applications and those that receive priority access to minimize excessive usage. FirstNet should also develop strong training programs to ensure SOPs are clearly understood and implemented.

2. FNN Applications

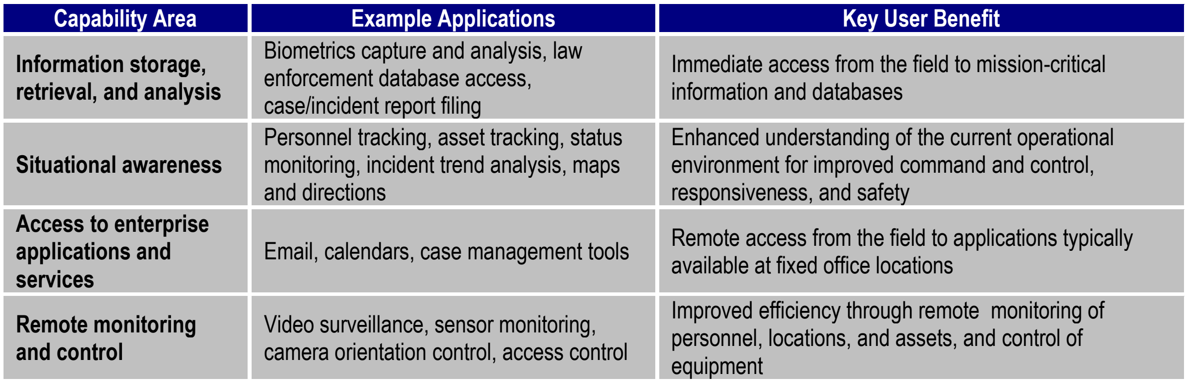
The proliferation of mobile applications is expected to bring significant enhancements and change to the public safety communications culture and user experience. Applications will enable greater responsiveness for users and provide the ability to access and exchange information in ways not possible using today's predominate public safety technologies. For example, real-time access to information contained in criminal databases, video, emergency alerts, and images will improve situational awareness and facilitate more effective, timelier decisions. Remote monitoring, control, and access to enterprise services will improve efficiency by reducing the need to travel to fixed office locations. With the power of this capability comes the responsibility to identify and manage new security risks to ensure neither public safety enterprise infrastructure nor mission-critical data is compromised.

Applications for Public Safety. Applications are generally developed to meet a specific task or function that is identified based on the collection and aggregation of information access and exchange needs. For FNN, the range of functions performed by public safety users will likely drive the development of numerous applications. For example, during routine traffic stops users may access a variety of databases (e.g., Department of Motor Vehicles, National Crime Information Center) to collect information. During border interdiction operations, users require access to images to identify suspects. Similar user needs should be collected early in the planning process and used to inform application development, including technical design and level of customization needed for unique operational scenarios (e.g., fire response). Exhibit 5 highlights capabilities often desired by users, examples of applications, and benefits.

Exhibit 5: Example Public Safety Applications



Capability Area	Example Applications	Key User Benefit
Real-time communication	Voice communications, text messaging, instant messaging, emergency alerts	Real-time coordination using the most efficient and effective means available
Media sharing	Image sharing, video sharing, file sharing	Sharing of large amounts of information contained in visual media or other saved files



Capability Area	Example Applications	Key User Benefit
Information storage, retrieval, and analysis	Biometrics capture and analysis, law enforcement database access, case/incident report filing	Immediate access from the field to mission-critical information and databases
Situational awareness	Personnel tracking, asset tracking, status monitoring, incident trend analysis, maps and directions	Enhanced understanding of the current operational environment for improved command and control, responsiveness, and safety
Access to enterprise applications and services	Email, calendars, case management tools	Remote access from the field to applications typically available at fixed office locations
Remote monitoring and control	Video surveillance, sensor monitoring, camera orientation control, access control	Improved efficiency through remote monitoring of personnel, locations, and assets, and control of equipment

Application Delivery Methods. A number of delivery methods exist for enabling public safety access to mobile applications. Today, the predominate method for the aggregation and delivery of commercial mobile applications is the ***application store***, which provides direct access to consumers via a variety of access methods, including smartphones, tablets, laptops, and other devices. Traditionally, a number of models have been used to establish application stores, including device manufacturer (e.g., Apple, Blackberry), operating system (OS) developer (e.g., Android, Windows Mobile), mobile network operator (e.g., Verizon), and multi-platform development (i.e., support multiple OSs and devices). Key factors that restrict access to applications in the device, OS, and mobile network operator models are brand of device, service provider, or proprietary nature of the software in use. In contrast, a multi-platform model is not dependent on these factors and could be dedicated for a particular function or user base. For example, several Federal Government organizations have initiated efforts to build private application stores. Specifically, the Defense Information Systems Agency (DISA) is developing an application store that will collect all relevant Apple iOS, Android, and BlackBerry applications into a single portal. The store is planned to contain both commercial and custom applications for Department of Defense (DoD) users and accessible with the DoD infrastructure to ensure applications are controlled and secure for smartphone users.

There are a numbers of key considerations for determining the appropriate model for providing public safety users access to applications, including the ability to—

- Control applications available to users
- Control the application distribution mechanism
- Manage applications from multiple sources and address updates
- Explore non-traditional methods for loading applications onto devices
- Balance limitations or requirements levied by commercial application stores
- Support multiple OS platforms and operate on multiple devices
- Control features such as access control, push notifications, and over-the-air updates
- Control security mechanisms, including certification and incident response
- Develop, prototype, and test applications in a controlled environment to ensure quality and security prior to release.

Interface Requirements. Open development enables the flexibility, market competition, and compatibility required to create an array of affordable applications that are both customized to the needs of specific user communities and accessible across organizations. However, for applications to operate on the FNN architecture, be compatible with other applications, and comply with FNN and agency policies, FirstNet needs to consider the target audience, type of technical features the applications must support, long-term prospects of the mobile platform being considered, required level of security, and types of devices supported.

- **Mobile platforms.** Today’s broadband devices typically leverage one of a variety of mobile platforms, including Android, Blackberry, Windows Mobile, Apple iOS, Symbian, Qualcomm BREW, and Sun J2ME. Public safety requirements extend beyond what any one platform can satisfy. Thus, FirstNet should consider promoting the development of multi-platform (develop once, deploy anywhere) applications.

There are several multi-platform developer tools in the market today, including RhoMobile, PhoneGap, Appcelerator, MoSync, WidgetPad, and Whoop. Building a mobile device agnostic solution will help reduce development time and operations and maintenance costs associated with supporting various operating systems.

- **Device/user/personal information permissions.** Many applications rely on access to PII, device information, user location information, and other potentially sensitive information to authorize network access or provide information needed for field users (e.g., locate responders closest to an incident, use of GPS to track personnel or assets). Developers should understand specific agency policies for accessing, storing, transmitting, and modifying sensitive information for applications and ensure security measures align with these policies.
- **Enterprise security protocols.** Public safety users require varying levels of enterprise-level security depending on several factors, including their mission and organization, and the information stored, received, or transmitted from their device. Developers should understand these requirements at the application, device, and system levels to comply with agency policies and ensure applications successfully interface with the security systems and protocols of FNN.
- **Enterprise services platforms.** Many applications will rely on access to existing or planned enterprise applications and services that may reside on the FNN or other public safety networks. Developers must understand enterprise-level protocols and interface requirements to ensure applications will work as intended.

Application Security Considerations. Due to the missions of public safety, any interface into the system containing or controlling records is likely to be subject to various types of threats. Terrorists may wish to access the system to access security details, and other sensitive information to plan their attacks or leverage the information to avoid being captured.

Hackers may wish to attack the system simply to embarrass the government in an attempt to make a political statement. Consequently, it is paramount that any mobile application and supporting infrastructure built for public safety ensures the security of the data and the system. The applications, especially as they proliferate, could become an adversary's first point of entry to the network. There are three approaches adversarial threats may use to attack applications to compromise the network. They will attack:

- Data at rest (stored indefinitely within the mobile device)
- Data in process (stored temporarily while handling a user request),
- Data in transit (between the device and the public data infrastructure).

It is essential to consider each of these potential vulnerabilities when designing the application, device data storage mechanism, and the interface to public safety servers. Typically, mobile devices may also be connected to other consumer devices, such as personal computers, that may themselves provide other attack vectors into the device file system. Additional applications may also be loaded onto the device which may attempt to access public safety data, either directly in the file system or through specially crafted function call registrations. Traffic transmitted between the device and public safety servers may be monitored in flight at many points along the network path, especially when using unsecured WiFi network capabilities built into the mobile devices. For public safety infrastructure, any interfaces opened to allow mobile traffic could be compromised to access systems that are within the network.

These attack vectors can be mitigated with a robust end-to-end approach to addressing security. The most effective way to avoid many of these attacks is to not store data on or transmit to the device unless absolutely necessary. For all data that must be stored, whether temporarily or indefinitely, the application must apply strong encryption, especially if the data represents PII or greater sensitivity. Increased care must be taken to ensure data is not inadvertently leaked within the device by using best security practices in the design of inter-application function calls. Any data sent over cellular, WiFi, Bluetooth, or other interfaces, must be encrypted to prevent tampering or viewing the data in flight. Firewalls and servers must be configured to only allow appropriate traffic into the system, with enterprise security software monitoring the system for unauthorized access and ensuring proper patch levels on all system components. The best protection against intruders gaining system access and doing serious damage is to not build such capabilities into the application and isolate servers from those being used for public safety mobile traffic. With proper consideration of security, mobile applications can help lead to improved mission effectiveness and agent/officer safety.

3. Conclusion

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. The firm provides services primarily to the U.S. government, and to major corporations, institutions, and not-for-profit organizations. Booz Allen offers clients deep functional knowledge spanning strategy, organization, engineering, operations, technology, and analytics. Specifically, Booz Allen has over 20 years of experience supporting public safety communications. Our broad experience working together with homeland security and public safety agencies across levels of government to modernize national and regional networks, provide technical assistance to state and local agencies, develop deployable solutions for disaster and emergency communications, improve communications planning and coordination nationally and regionally, and plan and execute grant programs to get critical resources to states has afforded unique insights into the challenges faced by this community. We have a legacy of working with and supporting commercial telecommunications companies and have considerable wireless engineering expertise. In addition, Booz Allen has supported the Department of

Commerce for more than a decade, including the last three years supporting NTIA’s largest and most complex programs ever— the Broadband Technology Opportunities Program (BTOP).

The envisioned FNN presents great potential to transform public safety communications. Achieving this potential will require careful navigation through complex operational, technical, and economic challenges that have plagued public safety communications for decades. Our years of experience with these challenges, as well as the diverse and, at times, passionate stakeholder perspectives, enables Booz Allen to effectively “work within the seams”—meaning the ability to objectively balance trades with respect to stakeholder perspectives, business considerations, and FNN performance objectives. This attribute will become increasingly important as the Board continues to evolve the FNN architecture from concept to deployment. We appreciate the opportunity to comment on the FNN conceptual architecture and applications framework, and look forward to continuing this dialogue with NTIA and the FirstNet Board.