Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20230

	)	
In the Matter of	)	
	)	
Development of the Nationwide	)	Docket No. 120928505–2505–01
Interoperable Public Safety Broadband	)	RIN 0660–XC002
Network	)	
	)	

November 9, 2012

Douglas Booth
Lockheed Martin Corporation
703.216.7810
4350 North Fairfax Dr
Arlington, VA 22203
douglas.e.booth@lmco.com

Michael Grasso
Lockheed Martin Corporation
2121 Crystal Dr
Arlington, VA 22202
703.413.5919
michael.a.grasso@lmco.com

Jennifer Warren
Lockheed Martin Corporation
2121 Crystal Dr
Arlington, VA 22202
703.413.5970jennifer.warren@lmco.com

Table of Contents

Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20230

	)	
In the Matter of	)	
	)	
Development of the Nationwide	)	Docket No. 120928505–2505–01
Interoperable Public Safety Broadband	)	RIN 0660–XC002
Network	)	
	)	

COMMENTS OF LOCKHEED MARTIN CORPORATION

Lockheed Martin hereby responds to the National Telecommunications and Information Administration (NTIA) request for public comment on the conceptual network architecture and the public safety applications identified in the Notice of Inquiry (NOI), Docket No. 120928505-2505-01, RIN 0660-XC002, dated September 28, 2012). To answer specific elements of the NOI, we have organized our response in four sections, as follows:

1. Executive overview of the response;
2. Comments on the FirstNet Conceptual Network Architecture, the FirstNet Nationwide Network (FNN);
3. Other options the FirstNet Board should consider; and,
4. Comments on developing applications for public safety.

Section 1. Executive Overview

We are pleased to respond to this FirstNet NOI and are excited about the ways in which a dedicated nationwide broadband network will offer new capabilities to our police, fire and emergency personnel across the country. FirstNet – with dedicated 700 MHz spectrum, broadband 4G LTE speeds, innovative applications, and instant access to nationwide databases -- provides the opportunity to transform public safety operations in profound ways.

We offer our response as a means to generate further thought, provide ideas and share examples that will assist in architecting this one-of-a-kind, nationwide solution for our country. As the leading IT solutions provider to the United States Government, Lockheed Martin has demonstrated the ability to provide world class services, mission critical architectures and expedited solutions for a variety of our country's national challenges. And, particularly relevant to FirstNet, Lockheed Martin has successfully met the needs of first responders by deploying mission critical architectures and systems in some of the most chaotic, intense and lethal user environments for some of the most complex and risk-rich procurements, of which examples include Army Corps of Engineers, the Federal Bureau of Investigation, and the Coast Guard.

Over the course of our response, there are four (4) major items that we highlight as significant considerations for FirstNet, the FNN conceptual design and the applications concept:

- Security, in all of its forms, will be vital to establish and manage. Given the nature of the inter-networked architecture wanted and needed by public safety, network and cyber security will be atop the list of the most critical security dimensions. The critical dimensions to consider in security are:
    - Secure access to decentralized databases administered by various jurisdictions
    - Usability and reliability for life-critical voice nets
    - Threat monitoring and defense

- Innovative, quick-start use of the FNN by public safety professionals can be achieved through a BYOD (Bring Your Own Device) implementation strategy – which will help all public safety jurisdictions aggressively manage costs of securely and quickly getting on FirstNet's FNN. BYOD means that public safety users across the country will be able to use the devices they have today – to gain access to both an interim network and the long-term FNN network. This will greatly help with end-user costs and the ability for users to quickly get on-net.
- The inherent technical, financial, and operational complexity of FirstNet – driven by its sheer size and scale, along with its unprecedented level of jurisdictional inter-connections, massive infrastructure and ongoing operational costs – will create operations, governance, authentication, business model, and interoperability challenges that will make FirstNet a procurement inherently prone to risks. Along side this level of project complexity, there are the even more challenging aspects of human behavior and policy to be managed. The resulting need: Risk mitigation expertise and processes, accompanied by appropriate business operations, business model and project-delivery assurance structure will be essential to insuring successful and timely deployment and ongoing operation of FirstNet. A single, objective and complexity-proven program manager and systems integrator will be essential to reconciling all of these divergent forces in a cost-effective manner.
- Applications, and their access to them, are a critical motivation for the creation of FirstNet. Apps will be at their best when creating them in a HTML 5, platform-agnostic, web-standards world accompanied by cyber security measures and rigor that will best optimize both security and usability. While an AppStore of the ilk of the Apple App Store or Google Play have had consumer market success and are excellent models from which to draw, the public safety community will require an industrialized, ruggedized and streamlined version of these that addresses both the countless legacy apps and database tools that exist today and their migration and the creation of new, more robust certified apps for the future.

Within each section, there is much detail but the following critical points are key takeaways:

- Section 2: Comments on FNN Conceptual Architecture
    - Network design & interoperability
        - Criticality of Service Level Agreements
        - Analysis of performance considerations for implementation planning
    - Network security and cyber security
        - Tiered approaches can help balance security and usability
        - Active defense will be necessary for meaningful security
- Section 3: Other Options and Aspects the FirstNet Board Should Consider
    - BYOD initial network implementation, followed by full-scale FNN
    - Accountable and objective program manager and systems integrator
- Section 4: Comments on Developing Applications for Public Safety
    - Leverage HTML5 and a secure browser for seamless platform-agnostic delivery
    - Holistic approach to vetting and security that ensures quality applications
    - Context-based application store to improve app discovery

The Lockheed Martin comments regarding the FNN and Applications Concepts are based on and in response to the presentations and discussions that took place at the inaugural FirstNet Board Meeting held on 25 September.

Section 2. Comments on the FirstNet Conceptual Network Architecture

The FirstNet network architecture presented provided an excellent overview of the implementation, roles and responsibilities, and benefits and features of the proposed FNN network. In this section, we comment on the following topics and offer recommendations where appropriate:

- Network Design & Interoperability
- Network Security and Cyber-Security

2.1 NETWORK DESIGN & AND INTEROPERABILITY COMMENTS

Leveraging commercial carrier core networks to deploy FirstNet services offers opportunities for implementation speed and efficiencies, but also risks in its complexity. Moreover, the integration of the FirstNet FNN architecture with established LTE standards and existing LMR systems offers additional challenges. In this section we will highlight key technical areas to consider in the FNN design presented.

2.1.1 FNN's Hybrid Operator Approach and Reliability: Service Level Agreements (SLAs)

LM Comments: When outsourcing network services of any kind the creation of effective SLAs, which are defined when contracting with carriers, demands the coordination and inventorying of the needs of all public safety users of the FNN. Commercial carriers will need to be able to specify what performance level commitments that they will make, and ensure that their systems are capable of having SLA monitoring by FirstNet operators.

- Public safety end-user perspectives need drive the SLA. Today, data and voice service interruptions occur frequently. These disruptions are readily absorbed by the casual mobile user with little or no serious penalty or personal harm. However, for a First Responder, this will be unacceptable. As will be discussed in Section 3, key performance metrics will be needed to ensure the FNN is designed with the necessary level of reliability.
- The FirstNet Board can use SLAs to protect FNN public safety users from consumer traffic sharing the common backhaul hardware.

- SLAs surrounding the performance of carrier networks in the midst of an emergency may require additional stipulations to guarantee quality of service.

2.1.2 FNN's Enhanced Packet Core (EPC) and Backhaul Network

LM Comments: An LTE architecture enables commercial carriers to move certain computational resources from the cell tower location into a separate facility, centralizing the system in a way that can reduce operating costs. A consequence of this approach is that the backhaul links that connect cell towers to the core network will carry more traffic.

- Location selection complexity for EPCs increases significantly with an increase in the number of commercial carriers in a region. Integrating Band 14 towers/operations across a diverse set of carriers will require careful coordination with the carriers to determine the most efficient interconnection, network traffic patterns, VLAN, and routing techniques. This effort will be significant and the outcome will be vital to enabling an efficient network design.
- Number and location of EPCs are also important. Governance, system redundancy and management, and system performance will be general concerns to all First Responder communities. The quantity of jurisdictions grouped together to share an EPC increases the complexity of addressing these concerns while limiting the quantity increases acquisition costs.

2.1.3 Network Architecture: IP Addressing

LM Comments: Regardless of the precise architecture FirstNet deploys, interoperability with existing national and international networks with respect to IP addressing will need to be explicitly designed. Address-planning will be an important design element.

- Coordination of addresses for a network as large as the FNN will likely be a significant activity. Although the threatened exhaustion of public IP addresses has been repeatedly postponed due to creative reuse and recirculation of previously distributed addresses, the size of the FNN may stress or break commercial carrier addressing plans.

- IPv6 vs. IPv4. Even if the FNN were to use IPv6 or IPv4 private addressing with Network Address Translation (NAT), the network's design must determine the optimal techniques to ensure smooth integration with multiple commercial carrier networks. We recommend that this be done in concert with all the participating carriers.

2.1.4 The Value of Public Safety Applications

LM Comments: The value of voice, video and data applications should be quantified using projections based on surveys of public safety system operators and others.

- Establish the application and network demand baseline. Inventory all expected application uses - especially those demanding higher-bandwidth. An evaluation of the public safety user-community demand for real-time video, audio, and applications would be invaluable to properly designing the FNN. This knowledge will also be vital to the development of an effective SLA.
- EPC impacts. As architected, all FNN data will run through the commercial carriers' core networks and FirstNet EPCs. The sizing of EPCs relies upon the quantity of users and the expected data throughput. The EPCs should be deployed and sized based on their ability to support all of the anticipated applications - including eventually voice.
- SLAs help ensure available capacities, but application guidelines will be needed so that the available capacities are not exceeded. We recommend that public safety application developers be required to adhere to guidelines that will help maintain a predictable network demand.

2.1.5 FNN System Provisioning Controls and Authentication

LM Comments: Administrative control over provisioning and revocation of authentication and user-associated Quality of Service (QoS) parameters will need to be addressed early in the FNN design.

- Authentication systems spanning multiple jurisdictions should be designed and configured to support multiple administrators. Enabling public safety users to have maximum control within their jurisdiction with optional ability to delegate or share that control with other jurisdictions provides a strong platform to build trust among state and local agencies.
- Authentication systems should generate a secured audit trail. An audit trail of all authentication-related administrative tasks helps maintain the integrity of the FNN.

2.1.6 Land Mobile Radio (LMR) and Voice Interoperability

LM Comments: We recognize that first responders currently rely on LMR networks for their critical communications needs. Additionally, the market offers a myriad of reliable solutions to support the interoperability of mobile devices with LMR systems. These solutions, or “consoles”, which currently provide emergency services operators the ability to 'patch' disparate voice systems to their agency's LMR system, are part of the foundation of emergency services communications today.

- We recommend that FirstNet inventory the console population. Analysis of the national inventory of fielded solutions will be an invaluable source of data from which a clearer picture of costs and schedule needs can emerge for how LMR systems might be integrated into the FNN.
- Understanding how LMR, consoles, and Voice-over-IP (VoIP) would be used by first responders will be critical. In our experience, application and network design is improved significantly when the process is driven by in-depth analysis of ‘concept of operations’. It is unlikely that a 'drop-in' module to satisfy public safety user needs can be introduced at a date in the future without any disruption of functioning network components.

2.1.7 Deployed Systems: Cell On Wheels (COWs)

LM Comments: Cell on Wheels solutions are relatively easy to configure and deploy for closed or isolated, stand-alone networks. However, COWs which need to be integrated into a multi-jurisdictional network and/or require reach-back access to authentication services demand stronger pre-planning and provisioning design in order to ensure their availability for rapid deployment.

- Security will be needed for network access. Certain emergencies, such as natural disasters, offer minimal concern for system security. Devices may be automatically authenticated by default. However, other disasters or special event situations will demand use of system security functionality. For security to work, authentication data for all possible responding agencies must be synchronized in all COW systems - or an adequately sized satellite backhaul must be available to perform the sync during crisis or to handle all authentication remotely.
- Service Delivery Platforms (SDPs) should be pre-provisioned into COWs. Local and state application configurations would need to be pre-provisioned or automatically provisioned so that any infrastructure components that have been lost (e.g. failure at an SDP site) are restored. The applications may be restored with the COWs or at some facility to which the COWs provide backhaul connectivity.

2.2 NETWORK SECURITY AND CYBER-SECURITY COMMENTS

The Technical Advisory Board for First Responder Interoperability provided a comprehensive framework for FNN security in Section 4.8 of the document *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, dated 22 May 2012. Protecting the network from attacks, and public safety databases from compromise, are critical issues that must be addressed from the beginning of the FNN design.

2.2.1 Achieving Network Security, Usability and Reliability

LM Comments: Life-critical communications for police, fire and EMS personnel cannot be hampered by cumbersome security protocols. The challenge will be to provide usability and reliability while simultaneously protecting the FNN from network and cyber threats.

- Tiered security levels for FNN voice nets could provide different security/usability set-points, whereby emergency responders would have device-only authentication requirements (via USIM), requiring minimal user-device interactions.
- Other voice nets facing greater interception threats would require different levels of user authentication, including passwords and random-number tokens.

2.2.2 Network Security in the Hybrid FNN Architecture

LM Comments: Within a network of multiple carriers with IP connectivity, implementing the necessary security solutions are significantly more challenging than in a self-contained network.

- Peering with commercial carriers may mean that SDPs are exposed to all commercial mobile subscribers unless traffic is tunneled and firewalled effectively. The FNN security architecture will need to be developed with thorough consideration of the implications of utilizing the core networks of commercial carriers.
- Ensure integrity of software running on network components. An ongoing program to review code for, and verify the authenticity of, firmware to be installed on operational devices on the network will be critical to assuring users of the reliability, stability, and integrity of the FNN as a whole. For example, EPCs that can be remotely shutdown via malware originating from a manufacturer or a foreign nation would pose a serious risk to public safety.

2.2.3 Threat Monitoring and Defense

LM Comments: As with most large corporate and government networks, the FNN will be exposed to a full spectrum of targeted and evolving adversarial cyber threats. This threat is compounded by the connection to thousands of jurisdictions, a shared commercial/FirstNet network backbone, and requirement to provide access to nationwide databases.

- LTE security standards alone will not provide the scope of security features needed to counteract the threats. A comprehensive FirstNet "enterprise hardening" process will be needed – involving not only technology, but also people and processes.
- Real-time threat monitoring by cyber security analysts will be required to respond to all sorts of security incidents, from lost user devices to network intrusions and large-scale cyber attacks.
- The architectural (and budgetary) "hooks" for threat monitoring and defense must be embedded in the design from the beginning.

2.2.4 Public Safety Access to Decentralized Databases

LM Comments: It is envisioned that existing public safety data services will remain under their current jurisdictional control, and will not be migrated to a centralized SDP within the FNN.

- Since the public safety data services are decentralized and administered by many different jurisdictions, FirstNet's role might be two-fold:
    1. To provide a common centralized directory of data services, enabling public safety users to request access to existing decentralized data services. These data services would then use their existing security methods to provide access to authorized users.
    2. To provide a single access control/authentication service to simplify access to data services for authorized users.

2.2.5 User Device Security

LM Comments: When first responders lose custody of an LMR device, it is often cause for concern due to the possibility that the tool can fall into the hands of malicious parties. Loss of devices that have the ability to access data bases on the FNN increase the risk of potential harm to the public safety users.

- Custody-loss presents the potential for a major security breach. FNN applications should be designed with this consideration. Applications running on mobile or laptop devices should run in a "secured container" or leverage configuration management tools appropriate for the platform.

- Unattended connectivity to the FNN, like 'standard' cell phones, should not be encouraged. Devices which automatically connect and whose chain of custody can be broken provide easy network access for malicious parties.
- Device specifications may need to consider a 'remote zeroize' feature. Devices that have been contaminated or whose chain of custody has been broken should optimally permit remote administrators to control or 'zeroize' the device in order to minimize the risk of system attack.

Section 3. Other options the FirstNet Board should consider

- ***Speed network deployment through a two phase approach*** *– Deploy innovative Bring-Your-Own-Device (BYOD) data mobility services, followed by the full-scale FNN.*

- ***Accountable and objective Program Manager and System Integrator (PMSI) role will be required*** *– FNN faces complex technical, business model and programmatic challenges.*

We believe that any FNN implementation approach must satisfy four criteria that will lead to widespread adoption:

1. Be reliable in normal and large-scale stressed operations.
2. Be affordable in both its initial deployment and on a continual basis.
3. Offer compelling services not available with the current public safety communications systems in place today.
4. Be deployable quickly to provide enhanced services to fire, police and emergency medical services (EMS) personnel.

Implementing the FNN will be a large and complex undertaking regardless of the network architecture selected. As recognized, the challenges will include the creation of complex business relationships and new implementation of existing technologies. Multiple vendors will need to cooperate at a deeper level than exists in the commercial network operator world today. The operation of the FNN core must also appear and feel seamless to the First Responder user, regardless of the transport mechanism. Much system engineering and integration will need to be conducted in order to address these challenges and the inevitable unknowns in order to meet the reliability, affordability and service criteria for the FNN. We therefore urge the FirstNet Board to consider a two phase approach that would speed initial deployment:

- Phase 1: A data-only (no voice or FNN LTE) mobility service that rides atop of the commercial infrastructure and provides access to data services critical to police, fire and EMS personnel using a "bring-your-own-device" (BYOD) business model.
- Phase 2: A 4G LTE service to provide full-scale FNN capabilities.

The paragraphs below describe the path forward for each of these phases.

3.1 PHASE 1: FIRSTNET BYOD MOBILITY SERVICE

LM Comments: Phase 1 consists of data services and applications that engage FirstNet stakeholders and form the core of the full FNN that follows. This early deployment would form the basis of the Service Delivery Platform (SDP) described in the 9/25 briefing. Technologies for cloud-based data and application servers are already well established. FirstNet could leverage these technologies, as well as existing and new software applications for public safety use. FirstNet could host these applications or provide a single, secure method for local users to access existing data warehouses.

The Phase 1 deployment would speed the development of the SDP, engage stakeholders in FirstNet environment, build a core of public safety applications, and help drive business relationships with carriers and service providers. In this phase, capital expenditures would be minimized by a BYOD approach, whereby public safety users would employ their existing smartphone or laptop with a limited selection of key applications. This phase would also include the analytics for performance and usage studies and projections performed by an objective Program Manager and System Integrator (PMSI). In this manner, the larger capital expenditures will be correctly sized and avoid potential waste in the next phase. This Phase 1 service would co-exist with legacy LMR systems dedicated to voice traffic, and would focus on non-mission-critical services.

The BYOD approach would be augmented with a Mobile Device Management (MDM) system to provide security and data integrity. MDM systems are readily available and well-vetted solutions. Several major vendors and can provide assistance with selection and integration. Furthermore, these systems often include tools for developing secure applications that run within a “sandboxed” environment, provide encryption capabilities, and can support multiple mobile operating systems such as Android and iOS in limited capacity.

Near the end of Phase 1, FirstNet would transition BYOD users to a lighter-weight Mobile Application Management (MAM) system as more vendors begin to support this model. MAM allows a reduced footprint on personal devices while providing strong security and improved cross-platform access.

3.2 PHASE 2: FIRSTNET FULL-SCALE DEPLOYMENT

LM Comments: Phase 2 further increases the need for a strong, objective Program Manager & System Integrator (PMSI) team to help bring this complex system together.

Meeting the reliability, affordability and service criteria for the use by first responders in life-critical situations will require a strong program management and system engineering team. We recommend that the FirstNet Board build a strong, objective PMSI team to help manage the FNN deployment. The PMSI team would provide system engineering leadership for the program, working for the FirstNet program management team and in collaboration with NTIA, NIST, commercial operators, and others.

3.3 ACCOUNTABLE AND OBJECTIVE PROGRAM MANAGER AND SYSTEM INTEGRATOR

LM Comments: We highlight how several of the most critical PMSI activities will influence the outcome of the FNN development. System engineering and integration of large complex systems relies on a number of processes, which if executed well, help ensure that the completed system will operate as intended and in a timely manner. For communications programs as vast as the FNN, there is a subset of activities that will be vital to the success of the system. Below is a description of these activities and how they could be used in the FNN development.

3.3.1 Public Safety User Needs Development

LM Comments: Local fire, police and EMS needs as well as state and federal needs will have to be synthesized into a cohesive architecture and requirements set. First responder user needs will come from local, county, state, tribal area, territorial and national jurisdictions. Local first-responder needs will focus on critical voice services, that is, conference nets to replace existing LMR networks. Data services and operational administration of the FNN resources will also be important. At the state and federal levels, the critical needs will likely focus on nationwide connectivity, access to large-scale databases, and an overarching security framework. User needs across all levels will need to be understood, prioritized, and de-conflicted in order to develop a common operating concept that drives the architecture.

3.3.2 Network Architecture Development and Requirements Definition

LM Comments: Much of the FNN architecture is not covered by the 4G LTE standards, and will need to be developed. Public safety user needs, FirstNet business model and FNN operating concept will lead into a detailed architecture development phase. Although the commercial, single-carrier, 4G LTE architecture is defined by the 3GPP standards, the unique characteristics of FNN will demand a significant advancement in architecture definition. For instance, the proposed hybrid FNN/commercial infrastructure and the common FirstNet EPC/SDP impose a set of interfaces and functionality not currently part of the 4G LTE standard. We anticipate that a large set of architecture threads will be needed. These threads define the precise functions and interfaces required for every function not directly called out in the 4G LTE standard. For instance, security architecture threads will describe in detail how a voice net is sustained as First Responder users traverse carriers, all the while maintaining secure connections through the voice server. FNN architecture threads will cover not only user operations but network management, user provisioning, backup operations, and a myriad of other architectural elements. The results of these threads will be distilled into requirements and interface documents, and serve as the basis for verification.

3.3.3 Technical and Business-Model Analyses

LM Comments: Comprehensive and validated models will form the basis for predicting affordability and reliability. Both technical and business-model decision analyses will complement the architecture development activities described above. Many far-reaching decisions will need to be made early in the FirstNet program. Financial constraints of First Responder users and cost recovery of the carriers and equipment providers will likely drive important architectural decisions. The basis for these decisions will likely be in the form of cost models that seek to assess both initial deployment and ongoing operational costs of the network. The FirstNet Board will be able to use these models to help increase the value to public safety users of the FNN as compared with the users' legacy radio networks. In addition to cost models, a number of large-scale technical analyses will be needed to predict performance and to properly allocate requirements. Of course, geographic coverage is a critical technical analysis since Band 14 equipment will be widely deployed by multiple carriers. Additionally, analyses related to voice call setup times, data backhaul capacity and various measures of system reliability all will be critical to FNN definition and First Responder satisfaction.

3.3.4 Service Level and Performance Metric Development

LM Comments: Values of key metrics, like link margins and coverage reliability, will directly affect how well the FNN serves emergency responders in life-critical situations. A system-wide metric for coverage area signal reliability will be needed, and will drive the number of cell towers and hence the performance and overall system cost. A similar parameter, link margin for building penetration, will also have a large affect on performance. Other standards will involve user devices, applications, and required capacity margins. In most cases, the technical analyses will only be the first part of the sizable effort required to gain adoption of the metrics by the FirstNet stakeholders. Transparent processes will need to be developed so that proposed metrics can be commented upon, updated, and implemented.

3.3.5 FNN Verification and Validation

LM Comments: We recommend a confidence-building test program consisting of early interface tests, pilot implementations, and formal tests/certifications. Due to the critical nature of the communications going over the FNN, both verification (test against the requirements) and validation (test in an operational environment) will be a very critical activity. It is anticipated that a comprehensive crawl-before-you-walk test strategy will be employed to assess new technological capabilities that extend the 4G LTE standards – such as the security overlay and voice networking architectures. It is anticipated that the NIST labs will play an important role in these early verification events, with the need for a large-scale testbed probably required to test wide-scale FNN functionality and performance. Pilot implementations, such as the existing county-wide LTE deployments, might also be engaged to test FNN capabilities on a non-interference basis if possible. Additionally, after the initial FNN deployment, an ongoing verification program will be needed for technology upgrades. The verification program will extend to type-certification of user devices that vendors are expected to develop for the large FirstNet user base. The verification program must also handle how changes within commercial carrier infrastructures will be evaluated for effects on system performance. The integrity of the verification program will be a key driver in building stakeholder confidence that every FirstNet deployment will operate reliably and as intended.

3.3.6 FNN Program Planning

LM Comments: We recommend an integrated and transparent program planning across government, commercial carrier and equipment vendors, under supervision of a strong program management organization. Tight coordination of the activities described above – and many other related activities – will result in a timely deployment of FNN capabilities. Activities of device vendors, commercial carriers, state and local government agencies, public safety users, and others must be pre-planned and then executed using sound approaches and frequent checkpoints. Policy agreements between and among government stakeholders will need to be included in the project plan so that critical elements, such as security requirements, can be driven into the FNN implementation in a timely and cost-effective manner. A series of outreach events will also likely be required to vet requirements with various first responder users and drive their needs back into the baseline. In addition, program planning for the initial deployment, program planning for the transition of the 3000+ U.S. counties and other areas will also need to be managed. Thus, a continuous transition activity will be a fundamental part of FirstNet, along with the accompanying technology insertion and system capability upgrades.

3.4 HOW PMSI ACTIVITIES ADDRESS SPECIFIC CHALLENGES

LM Comments: Table 3-1 provides a representative sample of key challenges and the PMSI activities that can be employed for successful FNN implementation.

Table 3-1. PMSI Activities in Addressing Important FNN Challenges

FNN Challenges	PMSI Activities
Business Model	
Cost estimation for development, recurring operations, and technology insertion/refresh.	• Detailed cost model development • Cost modeling working group • Key performance parameter trade studies
Commercial carrier costs and billing	• Concept of ops for user roaming among carriers • Concept of operations for usage metering and billing
Deployment of public safety applications	• Apps store billing model • App certification requirements
Customer service and user provisioning.	• Service management trades and requirements
Programmatic	
Timely deployment of the system	• Schedule tracking across all activities • Transparent risk management program
Integration of commercial MNOs providing FirstNet B14 and backup services.	• Early interface tests • Load-testing of commercial backhaul networks
Implementation across 3000+ US counties, as well as states, tribal areas and territories.	• Standardized/streamlined transition plans • Transition support to localities • Provision for local control of FNN resources
Controlled access to secure databases and other information sources.	• Inter-agency agreements • Security requirements for applications, user devices
Buy-in by stakeholders and public safety users having strict budgetary and reliability requirements.	• Key Performance Metrics reporting • Solid technical baseline – minimize req'ts. creep
FNN/Commercial priority and pre-emption policies	• MOAs with commercial carriers • FNN-wide policy statements
Technical	
Detailed FNN architecture development and specification.	• Detailed architectural/conops threads • Interface definition across FNN elements • Requirements flowdown to carriers, eqmt. vendors
Coordination of Band 14 operations where more than one MNO services the same geographic area.	• Nationwide coverage modeling • Process for B14 sharing among MNOs.
Development of cost-effective user equipment – ruggedized/non-ruggedized, multi-band, and satcom capable.	• Value engineering • Cost-conscious requirements definition • Early integration tests to ensure compatibility • Type-certification in collaboration with NIST.
Implementation of voice nets over the FNN and interfaces to legacy radio systems	• Call flow architecture development • SDP sizing analysis • Early compatibility demonstrations

FNN Challenges	PMSI Activities
FNN network management with real-time insight into commercial network status and issues.	• Network management interface requirements • Specification of FNN network operations center
Incorporation of 4G TLE technology improvements.	• Representation at 3GPP standards body • Technology roadmaps in insertion plans
Coordination of security and privacy while leveraging an all-IP network	• Security framework for access to databases • User authentication architecture • Definition of security enclaves, VPNs, etc. • Threat monitoring requirements
Deployment of public safety applications	• Bandwidth usage constraints for apps • Stringent acceptance tests of life-critical apps

3.5. FULFILLING THE FIRSTNET PMSI ROLE

LM Comments: An able, accountable, and objective PMSI capability should be one of the highest priorities of the FirstNet Board. The FNN PMSI organization will serve as an extension of the FirstNet Board and program management office. As such, the PMSI organization will always need to operate in the best interests on the overall FNN system. The PMSI organization will help drive the most cost-efficient and reliable system implementation. We recommend that the FNN PMSI organization possess the following characteristics:

1. Proven track-record of system engineering and integration successes on large programs. Timely deployment of the FNN will demand that the PMSI organization have the institutional knowledge about how to plan and architect large complex systems. The organization should have the breadth of system engineering skills – planning and scheduling, architecture development, requirements management, modeling and simulation, etc. – that can be employed in an integrated manner.

2. No conflict of interest with other segments of the FNN. The top level network architectures presented on 9/25 have significant business implications. There will also be many other technical and programmatic activities that have direct bearing on the degree to which different entities participate in the FirstNet operation. In order to conduct these activities in an objective manner, we recommend that the PMSI organization not be a FNN service provider or equipment vendor.

3. Domain expertise in mobile systems, networking, applications governance, and cyber security. The initial challenges facing the FNN development involve generating the architectural foundation and critical standards. These drivers of reliability and affordability will be critical to stakeholder

acceptance of the FNN. As such, the PMSI organization will need technical depth in the core technology domains in order to help the FNN management team make the right long term decisions.

4. Ability to tailor system engineering processes/activities to meet the timeline and performance needs of the FNN deployment. Unlike some large system developments, the FNN is based on continually progressing commercial standards. The PMSI organization will need to have sufficient maturity to know how to adapt the development process to ongoing changes in technology. The result will be a FNN that matures from 4G LTE Rel. 8 to Rel. 9 and Rel. 10 in a timely and cost-effective manner.

5. Expertise in monitoring, measuring and managing performance / mitigating risks. Achieving reliable oversight and management of such a complex deployment will be the highest objective of FirstNet's Board and Management. The many different network operators, device manufacturers, LTE core network providers and applications developers, amongst other value-chain parties, will need to be managed and held accountable to ensure program success. This means putting in place an agreed dashboard of metrics to rigorously manage and mitigate risks in service delivery, deployment, operation, service levels, availability, security, interoperability and a host of other dimensions.

Section 4. Comments on developing applications for public safety

4.1 SUGGESTIONS FOR APPLICATIONS THAT WOULD BENEFIT PUBLIC SAFETY USERS

LM Response: We recommend the development of an application strategy comprised of two distinct categories. The first category should contain applications that deliver fundamental and universally applicable FirstNet services. The second application category should be comprised of all non-universal or market specific applications such as the CPR Certification list mentioned during the FirstNet kick-off briefing. Application suggestions are provided in the tables below.

Table 4-1. Suggestions for Core FirstNet Applications

Core Applications
Secure email
Secure calendar
Secure contacts
Personnel tracking map – layers
Emergency map layers – police, fire, hospital, etc.
Secure photo capture
Secure video capture

Secure audio capture
Secure notepad with web sync
Encrypted VoIP w/Push-To-Talk
Encrypted messaging
Interactive medical database

Table 4-2. Suggestions for Market-Specific FirstNet Applications

Market Specific Applications
Interface to medical sensors
Interface to sensors (i.e., weather, traffic, etc.)
Fire Fighter navigation system
Waypoint mapping
Emergency procedures documentation
Interactive instruction manuals for gear
Medical records database
Hospital capacity dashboard
Vehicle location tracking
Electronic ticketing w/email ticket option
Public safety camera feeds
Building blueprints & maps

4.2 INTERFACE REQUIREMENTS & ASPECTS NEEDED IN AN OPEN APPS ENVIRONMENT

LM Response: FirstNet should consider the following requirements for application development:

- ***Platform Agnostic*** *– enables "write once, deploy anywhere"*
- ***Web Standards*** *– well-vetted framework for security, communications, and interfaces*
- ***HTML5 Presentation*** *– leverages previous points to deliver a fluid user experience*
- ***Secure Browser*** *– allows HTML5 apps to access device hardware and enhances security*

Developing applications for mobile devices may appear simple at first glance. However, mobile software development is not an insignificant effort when meeting the needs of large public safety user bases spread across multiple device platforms. In this scenario the proliferation of applications and the total cost of ownership (TCO) can increase exponentially as a direct result of incompatible hardware/software combined with the rapid pace of mobile product evolution. Based on these factors and the specialized needs of FirstNet users, we recommend that FirstNet consider a platform agnostic application strategy to control costs and simplify the interface requirements. The core components of this strategy, listed above, provide a method for securely delivering quality web applications and circumnavigating vendor dependencies.

4.3 ADDRESS WHAT SPECIFIC SECURITY REQUIREMENTS PUBLIC SAFETY NEEDS IN ITS APPLICATIONS

LM Response: To mitigate cyber threats FirstNet will require server, client, and device level security. The following requirements deliver strong security while minimizing the impact on user experience:

- ***Data-at-rest encryption*** *– minimum FIPS 140-2 certified AES 128 SHA-1 algorithms.*
- ***Data-in-transit encryption*** *– minimum FIPS 140-2 certified AES 128 SHA-1 algorithms*
- ***Encryption key management*** *– mitigates risk of brute force and physical hacking*
- ***Data policy management*** *– enforces on-device data storage rules for apps*
- ***Multi-factor authentication*** *– delivers rapid and secure access with biometrics or CAC*
- ***Single-Sign-On*** *– enables fluid transition between applications*
- ***Encryption hardware acceleration*** *– increases computational speed & performance*
- ***Application permission control*** *– isolates applications from critical resources*
- ***Device integrity validation*** *– prevents compromised devices from accessing data*
- ***Physical access control –*** *whitelist approved device ID and user certificate*

A comprehensive security framework is paramount to protecting mission-critical FirstNet infrastructure. However, a careful balance must be maintained between security and usability since most security measures adversely impact usability. The core components of the security strategy must include data encryption (both at-rest and in-transit), authentication mechanisms, network & services permissions, and data storage management. These tools should be augmented with a holistic application and developer certification process discussed in Section 4.5. We strongly recommend that FirstNet consider instituting all the requirements listed above and can provide additional guidance regarding implementation.

4.4 FRAMEWORK OR ORGANIZATIONAL FACTORS THAT WOULD ALLOW FOR DEVELOPMENT OF THE GREATEST NUMBER OF QUALITY APPS

LM Response: We recommend the following framework and organizational factors to enable quality apps and developer flexibility:

- ***Web signup*** *– web system to post app needs & connect with developers*
- ***Simple registration*** *– quick & easy means for developers to be screened*
- ***No-fee registration*** *– no barriers to de-incentivize signup*
- ***Contract execution*** *– streamlined process for quick turnaround*
- ***Integration guidelines*** *– streamlined guides for security & infrastructure integration*
- ***Limited design restrictions*** *– provides flexibility and creativity for developer*
- ***Code signing*** *– verify application authenticity*
- ***Code reviews*** *– protects against malicious code*
- ***Secure browser*** *– enhanced app functionality and device hardware interaction*
- ***Open source environment*** *– easy integration and application hosting*

As previously mentioned**,** we recommend web applications to control cost and facilitate cross platform interoperability. However, steps must be taken to provide developer flexibility while delivering both security and functionality. Flexibility is necessary to incentivize application development and entice the greatest number of developers to consider working on public safety applications. The requirements listed above and will help minimize restrictions and build a strong talent base.

4.5 SUGGESTIONS FOR APP CERTIFICATION REQUIREMENTS

LM Response: We recommend FirstNet consider a holistic approach to application certification:

- ***Background checks*** *– ensures developers have clean records & good track record*
- ***Digital certificates*** *– allows code signing to verify application authenticity*
- ***Code reviews/vulnerability analysis*** *– mitigates malicious code*
- ***Application vetting –*** *ensures quality apps and avoids trial-and-error*

Deploying a large-scale digital network such as FirstNet introduces a myriad of security concerns. While simple and well-vetted solutions can be instituted for encryption and management it is imperative that developers and software be screened. The requirements above highlight an approach modeled after the well-vetted Apple Computer App Store, which has been successful at mitigating threats according to industry leading security experts. Augmenting this model with a vetting process would eliminate the trial-and-error commonly encountered when downloading applications from public app stores, whereby users are presented with multiple applications that handle the same task, but only a small subset of those applications actually perform and deliver the intended result.

4.6 SUGGESTIONS FOR APP DELIVERY METHODS (E.G., APP STORE MODELS) UNDER THE FNN CONCEPTUAL ARCHITECTURE MODEL

LM Response:

- ***Web application store*** *– allows browsing and searching of platform-agnostic applications*
- ***Secure browser*** *– allows HTML5 applications to interact with hardware & improves security*
- ***Pre-loaded web applications*** *– essential services without the need to search & install*
- ***Contextual application discovery*** *– discover relevant apps based on role and location*

Applications should be hosted and accessed via a web-portal, with essential applications pre-registered in the device's secure browser. The web-portal can be similar to Google Play or the Apple App Store, but should employ contextual services to improve application discoverability, thus delivering a focused approach to ensure police, fire, EMS, and others can readily identify and download necessary applications rather than browsing expansive lists. User profiles could be combined with location-based services to automatically display the most relevant applications for a given user and location. For example, police officers in Los Angeles would automatically be presented with applications designed for Los Angeles upon accessing the application store. Additionally, users would be presented with location-relevant apps when travelling to new areas.

4.7 COMMENTS ON OTHER ISSUES THAT FIRSTNET SHOULD CONSIDER IN FACILITATING DEVELOPMENT OF PUBLIC SAFETY APPS

- FirstNet should consider developing quality applications rather than focusing on quantity. Deploying fewer and more functional applications with tightly integrated feature-sets and a focus on performance will yield an optimal First Responder user experience.

- FirstNet should consider the scalability of application hosting environments and their associated databases or resources. An elastic and seamlessly scalable approach is recommended to support high availability and heavy user loading.
- A large-scale application store modeled after Google Play or Apple’s App Store may not be necessary for the immediate phases of the program. We recommend that FirstNet begin with a more focused application delivery model, such as pre-loaded applications, and expand the capability over time.

Doug Booth
Lockheed Martin
IS&GS Defense, Advanced Programs
Business Development Director