High performance. Delivered.

National Telecommunications and Information Administration

Development of the Nationwide Interoperable Public Safety Broadband Network

Notice of Inquiry

Docket No: 120928505-2505-01
RIN: 0660-XC002

November 1, 2012

Submitted To:
FirstNet
First Responder Network Authority
firstnetnoi@ntia.doc.gov

Submitted By:
Christopher Smith
Chief Technology and Innovation Officer
christopher.l.smith@accenture.com
+1 703-947-3409

Robert Casselman
Public Safety Broadband Lead
robert.c.casselman@accenture.com
+1 917 452-4484

Accenture Federal Services LLC
800 North Glebe Road
Arlington VA 22203

• Consulting • Technology • Outsourcing

NOTICE OF INQUIRY
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Docket No: 120928505-2505-01, RIN: 0660-XC002
DEVELOPMENT OF THE NATIONWIDE INTEROPERABLE PUBLIC SAFETY BROADBAND NETWORK

Introduction

Accenture Federal Services, LLC (Accenture) hereby submits the following comments in response to the Notice of Inquiry (NOI) issued by the National Telecommunications and Information Administration (NTIA) on September 28th, 2012 regarding the Development of the Nationwide Interoperable Public Safety Broadband Network.

In the following sections, Accenture wishes to provide its perspective on a range of opportunities, challenges, and potential solutions that will be important as FirstNet proceeds through the process of planning, designing, building, and ultimately managing a nationwide broadband network for public safety. While this response is by no means intended to be fully comprehensive, Accenture has endeavored to focus on a few specific areas of interest that it believes to be especially relevant to the future success of the FirstNet program. These areas include:

- Overview on Public Safety Communications
- Governance (including organizational approach and process for decision-making)
- Public Private Partnerships (including government partnership with both carriers and utilities)
- 4G / LTE Network Strategy (including economic modeling and business case planning)
- 4G / LTE Network Sharing (including approach for deployment and ongoing operations)
- Mobile Application Strategy for Public Safety (including design, development, and support)

Accenture hopes that insight on these topics will be gained through the process of initial public comment and then further refined during the course of future deliberation amongst key stakeholders for FirstNet. It is for this reason that Accenture has aimed to structure its comments in the manner of best practices with a view towards future refinement and specificity.

I. Overview on Public Safety Communications

One of the greatest tests for any government is crafting an effective, coordinated response to emergencies. With lives often at stake, effective emergency response requires multiple government and non-government agencies working together in a coordinated, collaborative environment. That makes achieving interoperability between their communication systems vital. The variety of personnel and communications equipment involved makes a high performance solution mandatory and yet, an extremely difficult goal to achieve.

Because of the high stakes and multiple parties involved, public safety agencies have sought out innovative ways to solve the problem of interoperability. These innovative approaches have excellent applicability to other industries as well such as utilities, education, transportation, resources and hospitality and event management where emergency response may be required from time to time.

Many people first approach the problem of interoperability through the challenges posed by a fragmented infrastructure environment. Public safety agencies in the United States have traditionally made individual choices about what information and communication technologies they should use, and the same is generally true around the globe. Many of these individual solutions are based on radio, which has a loyal user base because of its reliability—but making communication possible between individual radio solutions during an emergency is very hard to achieve. A common approach has been to create new platforms (for example, P25 and TETRA) that would necessitate wholesale replacement of existing systems. Existing communications systems represent a considerable investment and have been fine-tuned and customized over the years to support the daily operations of the concerned agency. It is only in an emergency situation requiring the specialized skills from multiple agencies that limitations to interoperability become evident.

In Accenture's view, to be truly useful and to drive significant value into emergency response, both procedural and technological changes need to be made. Interoperability solutions should incorporate the following elements:

Focus explicitly on the human factor and culture change.

Technology must be seen within the broader context of creating a common framework for communication across agencies or organizations, and putting the processes in place to help enable such communication to occur effectively. Regardless of the technology chosen, change management will assist in defining a successful project. The communications devices may or may not change, but the processes governing how they are used, will. These procedures must be clearly defined and communicated to help ensure that agencies work together how and when required. These aspects of culture and governance must drive the implementation of the technology and not the other way around.

Incorporate capabilities for process automation and advanced analytics.

What can be automated should be—not only to reduce running costs but also to optimize response under pressure. For example, many standard operating processes, such as alerting and notification, can be partially or fully automated depending on the need. Advanced analytics can also be put in place to help enable on the-fly analysis such as detecting the need for additional

personnel, as well as more reflective post-event analysis that can be used to facilitate procedural improvements

Support all forms of media and provide an integrated suite of applications and services.

While voice is the primary medium for any multiagency communication, Accenture's vision is that Unified Interoperable Communications must ultimately offer support for data in any form that is useful, including text, pictures and video. Furthermore, the interoperability platform itself must provide more than connectivity alone. Because the technology exists only to help enable business processes for responders, it therefore must offer messaging services (voice, picture and text), video sharing, encryption, authentication, location via global positioning satellite, media recording, text-to-speech (and vice versa) functionality, language translation and database lookup. Presence, the service that allows users to see not only who is online but how they wish to be contacted, is particularly important because of the role it plays in enabling effective, real-time collaboration.

Successful interoperability relies upon trust; security must be built in and not added on.

The most technically advanced communication system will be rejected by end users if they cannot trust that their data will be securely delivered and only to the intended recipients. Authentication is key to trust, any system must provide a robust and extensible Identity and Authorization Management (IAM) infrastructure. Due the large number of participating agencies, it is difficult to see how this could be achieved without relying on a federated IAM architecture. Some mechanism therefore needs to be in place, such as a centrally managed PKI, to facilitate the trust relationships necessary for the federated IAM.

As and when these services are rolled out across the network, care must be taken to help ensure that they are made available on the existing devices. Of course, given the federated nature of this system, integrating a broad range of specialist areas like these is in itself a complex task requiring business insight, experience in developing governance frameworks, and process modeling and transformation; all core competencies of Accenture.

Organizations have long recognized the need for information. With the advent of technologies that help enable collaboration and coordination, agencies and enterprises are no longer limited to information harbored within their silo of operability. Where once it was acceptable to function as an autonomous organization, recent disastrous events have brought to light the deadly consequences associated with that operating model. Accenture's research has shown that sharing information across agencies can be made possible, but not without extensive planning, commitment, and critical skills. As a trusted third party advisor to some of the largest public and private enterprises in the world, Accenture has developed the strategy, methodology, and skills to help ensure a smooth transition to interoperable communications.

II. Governance

Governance of FirstNet will be a key critical component of this effort. Developing a flexible yet strong governance framework that allows a broad range of stakeholders to successfully interoperate and drive

this project forward is paramount. Local, State, Federal and Commercial entities will need to be able to interact fluidly and carry out disparate mission sets seamlessly and without interrupting the continuity of their respective operations.

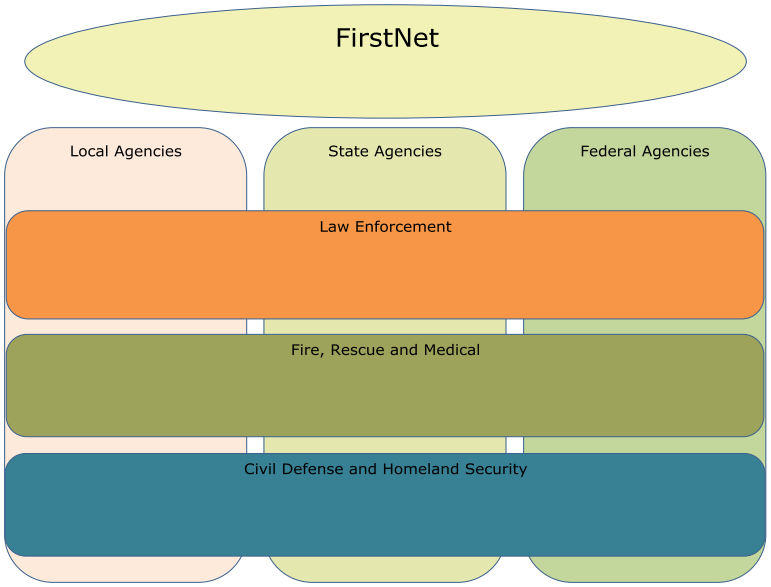
In today's environment Local, State and Federal agencies each maintain and operate separate telecommunications infrastructures. Since each party is most focused on delivering their respective mission they will likely act to protect and help ensure that which they own and operate and from their perspective is in their best interest to maintain. Gaining the trust and ensuring a solid set of operational capabilities will be paramount to enabling a disparate set of stakeholders to adopt FirstNet and support a truly interoperable and shared set of technologies. To gain that trust up front FirstNet should develop a transparent and inclusive governance process that helps ensure a seat at the table for stakeholders so that they get buy in from the outset and so that when something goes wrong, as it invariably will, stakeholders have a voice to readily resolve the issue and feel empowered to achieve their mission and not queuing behind another agency for service.

Governance Purpose & Potential Structure

Instituting a comprehensive governance strategy in a static environment is challenging, but developing and instituting it in an evolving environment such as the FirstNet where organizations and systems are being integrated and where budgets are being significantly reduced, adds additional layers of complexity. A Governance approach will require all stakeholders and FirstNet leadership to have a mutual public safety broadband vision. Governance at a high level is meant to:

- Manage the journey, set a strategy, manage progress and help ensure value is realized. Understand that each stakeholder may define value differently. Value from an acquisition standpoint can be cost reduction and the ability to field capability earlier. Value from the emergency responder's perspective can be reduced operational timelines, increased Op Tempo, the ability to accomplish missions with fewer personnel, etc.
- Evolve the enterprise capabilities to adopt, build and support the FirstNet platform-as-a-service.
- Migrate the organization from application-centric to service-centric, by transforming the architecture from client/server to platform-as-a-service.
- Establish and manage business & technology alignment.

Accenture has a proven track record in helping our clients develop and implement straightforward, manageable and successful governance structures to solve complex business and program issues. FirstNet's governance structures must accommodate the disparate stakeholder base, but also drive interoperability across this varied constituency. Accenture advocates a simple multi-tiered approach. By allowing varied mission entities within Local, State, and Federal agencies to act within their own communities, yet also communicate functionally across different communities. The figure below depicts a proposed governance structure that will meet these requirements.



Proposed Governance Structure

This framework helps enable clear lines of mission control and execution at all levels from Local to State to Federal and does not introduce any legal impediments that could inhibit mission delivery. It also helps enable cross domain interoperability of law enforcement, fire, homeland security and civil defense as well other public safety entities ultimately ensuring ubiquitous communications for first responders. Because it is uses a model similar to the Incident Command System widely used in the United States, it provides an easily understood structure that will be familiar to and elicit buy-in from emergency responders at all levels

Governance can be achieved when the public safety broadband users, other stakeholders, and FirstNet leadership together help ensure alignment and value realization. Without an effective governance approach, uncontrolled, ad-hoc development of services can occur that introduces functionality that is not based on a set of standards, that may be difficult to maintain or extend, and that may incorrectly use data. These scenarios can prevent FirstNet leadership from achieving the value it expects from its FirstNet vision and more importantly may negatively impact the mission. One of our tactics to support vision alignment has been to employ an Agile Development methodology wherein the Emergency Responder, Acquisition Stakeholder (PMO) and Trainers (i.e. those who modify Tactics, Techniques, and Procedures or Regulations) meet together during capability development to help ensure that the appropriate governance structures have been established for the development being performed.

Governance Capability Maturity Model & Approach

The following narrative describes four levels of maturity that organizations may pursue related to Governance. Level 4 is generally viewed as a best practice approach to establishing governance but it is important for FirstNet, as the executive agent effecting the implementation of the public safety broadband, to determine the appropriate level for the public safety broadband. FirstNet obviously has completed or initiated many of the activities shown in the following four-phased approach. We would like to have further conversations with FirstNet to confirm where you are on this journey and the level

you would like to attain. A roadmap should then be developed that aligns to the planned Network Integration Events.

Level 1: Plan & Organize – Governance Activities

- FirstNet Strategy & Roadmap
  - Come to an agreement on the urgent need to remove barriers to interoperability
  - Establish Roadmap and transition strategy
  - Establish and identify justification for transition/ROI or cost savings, as applicable
  - Assess organization readiness to adopt Platform-as-a-Service
  - Identify and align business and technology goals
- Journey Management & Communication
  - Achieve buy-in from stakeholders and IT management
  - Identify a well-respected champion to provide leadership
  - Begin to set and manage stakeholder expectations
  - Assess funding options for future phases
- Service Life Cycle Management
  - Establish service life cycle definition including policies and procedures for service identification, development, and deployment
  - Establish runtime (production) support and monitoring framework for services
- Capability Development
  - Assess IT operations readiness for Platform-as-a-Service
  - Define and validate Architectural Framework
  - Assess process modeling, design, and execution tools
  - Evaluate FirstNet standards infrastructure and protocols (e.g. security and other standards)
  - Establish basic patterns and design guidelines
  - Analyze security requirements and legacy application architecture

The critical success factors for Level 1: Plan and Organize includes:

1. Management/Stakeholder buy-in achieved
2. Business Case and ROI model established and communicated
3. FirstNet Framework Fit Assessment performed
4. Operations, Intelligence, and IT Management goals outlined, compared, and coordinated
5. Organizational approach determined and responsible parties identified
6. Service Identification and Development policies created

Level 2: Tactical – Governance Activities

- FirstNet Strategy & Roadmap
  - Identify tactical service implementations to support the justification and ROI objectives
  - Identify infrastructure and base services which will have a high level of usability

    - Facilitate IT and stakeholder coordination in the service/capability identification process
    - Create FirstNet Core Competency Group
    - Capture design patterns and best practices from project groups
- Journey Management & Communication
    - Target early wins to build support for the journey
    - Show value of tactical implementations
    - Track implementation progress while managing risks and issues
    - Verify and revise budgeting estimations
    - Continue to manage stakeholder expectations and maintain open communication
- Service Life Cycle Management
    - Apply and revise Service Life Cycle management policies
    - Verify and revise the Service Identification policies and procedures to help ensure focus on process modeling
    - Verify and revise the Service Development policies and procedures based on real life experience
- Capability Development
    - Establish Service Repository
    - Identify and resolve overall capability gaps (tools, training, etc)
    - Evaluate process modeling and tool adequacy
    - Update training materials to be relevant with real life experiences
    - Prepare architecture for integration with related process development

The critical success factors for Level 2: Tactical Governance includes:

1. ROI/Cost Savings etc. shown
2. Service identification and development processes proven and revised
3. Initial phases of the Service Life Cycle are verified
4. Operations- and Intelligence-focused processes modeled and supported by implemented services
5. Service Repository established.

<u>Level 3: Architected – Governance Activities</u>

- FirstNet Strategy & Roadmap
    - Track progress and help ensure alignment of stakeholder and IT objectives
    - Verify ROI model and justification
    - Identify more complex Operations and Intelligence processes to implement with the support of the growing services foundation
- Journey Management & Communication
    - Revise budgeting as needed to optimize costs
    - Assist identification of processes and domains that could benefit the most from FirstNet
    - Increase FirstNet awareness in IT with stakeholders through communication and training

- Service Life Cycle Management
  - Apply and revise Service Life Cycle management policies
  - Apply and revise the Service Identification policies and procedures to help ensure focus on process modeling
  - Begin to shape services support organization (effective monitoring and response)
- Capability Development
  - Help ensure new applications/widgets are service-oriented
  - Help ensure compliance with application and interoperability standards
  - Help ensure existing code can be adapted to suit new requirements

The critical success factors for Level 3: Architected Governance includes:

1. Design and development are service-oriented and process-oriented, leveraging a comprehensive set of tools
2. Service portfolio expanded and with many new services in the repository
3. Service Life Cycle management efficient and stabilized
4. Service reuse and ROI are realized

Level 4: Industrialized – Governance Activities

- FirstNet Strategy & Roadmap
  - Shift strategy to maintaining a high quality architecture
  - Establish FirstNet platform-as-a-service as standard practice
  - Define and meet stakeholder-oriented performance metrics
- Journey Management & Communication
  - Reach out to stakeholders who are not fully utilizing the services fabric and communicate the realized benefits of the FirstNet initiative
  - Increase FirstNet awareness enterprise-wide through communication and training
- Service Life Cycle Management
  - Help ensure good visibility of services to maintain a high level of reuse
  - Establish and enforce security policies for identity management
  - Maintain high performance service execution environment through actively monitoring and reporting on KPPs & SLA metrics
  - Track service dependencies and actively manage service versioning and changes
- Capability Development
  - Actively monitor the service delivery infrastructure and help ensure high availability with proper failover and capacity planning
  - Identify new tools to enhance productivity

The critical success factors for Level 4: Industrialized Governance includes:

1. New and existing stakeholder processes are modeled and supported with platform-as-a-service in mind
2. Efficient process implementation due to IT operational efficiency and service fabric
3. IT, Operations, and Intelligence management become truly service-oriented

4. Cross domain processes are supported by implemented services

It is important to have a well-defined approach, as there are significant risks if an active FirstNet governance process is not established early and comprehensively. Examples of those risks are shown below:

Risk	Impact
The business case and value proposition of the FirstNet program are not well defined resulting in a failure to achieve the operational value for moving to the FirstNet program	• Misalignment of Intelligence, Operational and IT Objectives due to a lack of common goals being communicated • Opportunity Cost for not achieving the maximum ROI expected
The roadmap for the FirstNet program is not clearly defined and/or the long-term execution is not managed according to an established set of processes and guidelines resulting in a failure to achieve the broader goals	• Loss of Momentum in making progress to achieve the long term goals, including potential project abandonment • Opportunity Cost for not achieving the maximum ROI • Deterioration in Architecture and a potential increase in cost due to a lack of long term management
The Service Identification process is not standardized and Architecture reviews are not performed resulting in a poorly defined target architecture	• Lack of Interoperability due to siloed organizational services • Lack of Reuse due to a proliferation of single-use services and a tightly coupled & inflexible architecture • Unnecessary Development Expenditure due to service rework and repair
Service development practices are not standardized and policies are not enforced resulting in poorly implemented services	• Lack of Reuse due to unpredictable service quality and services not conforming to Service Level Agreements • Higher Support Costs and/or unavailability of Capability due to poor service quality and higher frequency of outages

From an organizational support standpoint, there is no single "right" organization structure to support the implementation of the FirstNet program, but rather there are a range of options and considerations. Below are some of the potential organizational approaches, and each has its strengths and challenges.

- A centralized/Center of Excellence (CoE) approach may make sense if FirstNet is already experienced with employing a CoE, there is significant demand for platform-as-a-service solutions, projects span traditional organization boundaries requiring brokering and negotiation, FirstNet has already achieved Level 2 or higher in the governance process noted above, and the value of the FirstNet program is clearly understood and established.
- A decentralized approach may make sense if FirstNet assesses itself at a governance maturity Level 3 or 4, since initial projects have already been delivered, as long as methods, tools and technology standards are defined.
- A FirstNet Program approach may be appropriate if FirstNet assesses itself at a Level 3 or below and FirstNet is not prepared to embark on a CoE approach for whatever reason, as long as see where FirstNet is pretty far down the path of implementing the required methods, tools, and technology infrastructure to drive support and adoption, since we understand there is a high level of demand for solutions requiring cross-project management.

Governance Recommendations

- Implement a rigorous but simple multi-tiered governance structure that enables Local, State and Federal domains to carry out their legally required missions, but enables cross domain communications, collaboration and action by communities of practice such as Law Enforcement, Fire and Rescue, Homeland Security and Civil Defense, and others.
- Development and implementation of a FirstNet Governance Framework will be a journey through multiple maturity levels. Think big, start small and scale quickly.

III. Public Private Partnerships

For the past 30 years, Public Private Partnerships (PPPs) have served as an established means for financing economic and social infrastructure. Recently, interest in PPPs has increased as one approach to overcome government financing gaps, stimulate recovery in mature economies, and as a way for emerging countries to achieve a rapid provision of infrastructure. The overall concept of PPPs varies depending on the type of funding, services involved and risk sharing mechanisms. Some examples of risk/reward sharing and funding models include:

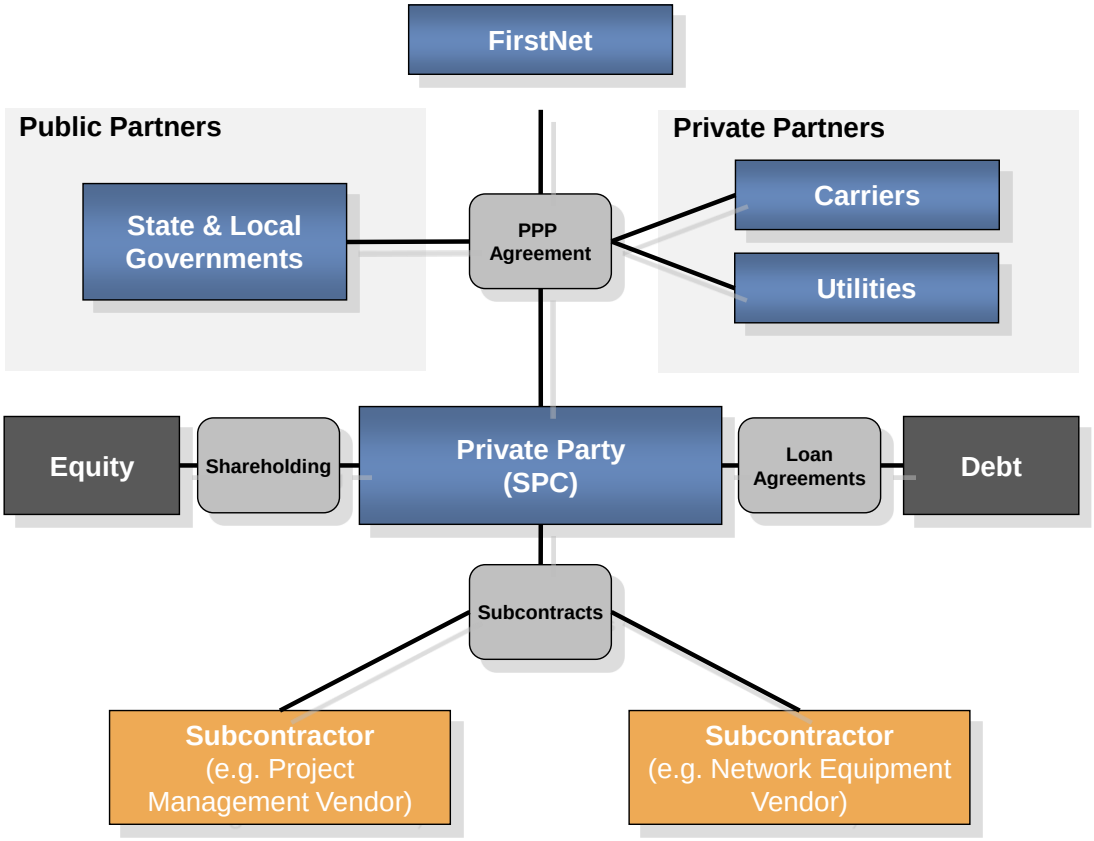
- The government provides assets (and/or financing) and the private-sector partner provides the service delivery for free or at a discounted rate.
- The private-sector partner provides the funding and service delivery, and the government pays back a fee for service over time.
- Both the private- and the public-sector partners contribute some assets and financing, and the end users (for example, the drivers on a toll highway) pay the fee for service. In this case, the private-sector partner takes the maximum risk in terms of demand.

In the United States, PPPs have traditionally being focused on economic infrastructure (transport/water) but there has also been significant interest to explore PPPs in other areas like public safety. Lately, the United States is applying PPPs to provide services in education and in labor market services like skilling

and training[1]. Some other areas where PPP's have been effective include healthcare, e.g. the National Plan to address Alzheimer disease[2], as well as cyber security[3].

Accenture has experience in developing these PPP's globally across various areas such as healthcare, education, and infrastructure. One notable example includes establishing a PPP to finance, implement, operate and maintain a multiservice network (WAN, LAN, hotspots) in a municipality in South America.

Based on this experience, Accenture believes that a structure similar to the one identified in the diagram below would be most effective for FirstNet. The PPP model involves a relationship between FirstNet and a Specific Purpose Company - SPC, which would be created for the purpose of building out the nationwide network and would manage subcontractors under a particular debt/equity structure as identified below.



Potential Structure of Private-Public Partnership

[1] United States Department of labor: US Labor Department awards more than $183 million for technical skills training to help American workers fill jobs in high-growth fields; Feb 22, 2012;
[2] National Alzheimer's Project Act, ; Feb 22, 2012; AFP:;
[3] Bipartisan Policy Center hosts policy discussion on improving cybersecurity; Feb 22 2012;

Potential Partnership with Carriers

In terms of potential public-private partnerships for FirstNet to consider, Accenture believes that partnerships with commercial carriers are particularly important. These carriers and mobile network operators have made significant investments in building out nationwide networks for commercial purposes. Developing a partnership with the mobile operators can provide access to their existing network coverage and capacity. As the demand for mobile data is skyrocketing and competition for subscribers intensifies among the carriers, FirstNet's access to valuable spectrum resources and plans to expand coverage into new markets could incentivize the carriers to engage in these partnerships.

In addition to access to existing network coverage and capacity, FirstNet could also benefit from carriers' experience with deploying and managing wide scale cellular networks. The carriers' familiarity with LTE technology and experience with large network roll-outs could provide some valuable lessons learned and best practices on how to manage a nationwide deployment. Furthermore, in order to manage a nationwide network with multiple stakeholders and SLAs, a robust management solution and support model will need to be developed. FirstNet could consult with the carriers to better understand their Network Operations Center (NOC) capabilities and experience.

Finally, the carriers' existing relationships with device manufacturers and OEMs could be important for Public Safety as these organizations will require devices that support their mission critical voice and data.

With these opportunities, however, come challenges that would need to be addressed. One of the primary concerns is network prioritization. Public Safety requires mission critical voice and data even in times of emergency. A partnership with commercial carriers would be dependent on their commitment to prioritize this traffic. Other concerns would arise around network management and regarding how FirstNet's spectrum would be shared with the carrier(s).

Potential Partnership with Utilities

Additionally, Accenture believes that alignment with the utilities industry would be particularly compelling. Utilities have started to make significant investments in their private communications networks to support evolving mobile workforce and smart grid requirements. In a Public Safety sharing scenario, these capital funds could be directed to help build out a nationwide network. Utilities' goals and requirements are consistent with Public Safety's goals in that both parties require ubiquitous coverage, even in rural areas, and prioritization of network traffic, particularly in emergencies.

In addition to capital investments, Utilities generally have a significant amount of network infrastructure already built that can be leveraged for a nationwide broadband network. This includes significant footprints of fiber and microwave backhaul, right-of-ways, and existing towers that could be ideal candidates for cell sites. This extensive infrastructure could significantly reduce the cost of a nationwide deployment.

While it is clear that there are common goals and similarities between Public Safety and Utilities, a network sharing partnership poses a number of questions that need to be addressed. These challenges include both financial challenges as well as technical challenges. Some challenges include:

- Detailed network planning would be required in order to estimate deployment costs, and determine the appropriate funding sources
- Prioritization of network traffic as both Public Safety and Utilities have requirements to operate critical infrastructure in times of emergency.
- Network segmentation and security design would have to accommodate robust security controls to properly serve both Public Safety and Utilities, including strict regulatory requirements such as NERC Critical Infrastructure Protection (CIP).
- Network operations model would have to support multiple organizations and provide SLAs to multiple stakeholders.

Public Private Partnership Recommendations

Based on Accenture's previous experience and our understanding of FirstNet's challenges in developing partnerships with Utilities and Commercial Carriers, we have identified the following key success factors for PPPs:

1. An appropriate legal and institutional environment:

    - A clear and sound legal framework establishing the basic requirements and mechanisms for dispute resolution and cancellation of contracts.
    - An effective governance model, as described in Section II of this document
    - Strong political commitment and communication with stakeholders

2. Well-Informed Network Planning and Decision Making:

    - Systematic use of sound cost-benefit analysis of network deployment options, to help ensure adequate rates of economic and social return.
    - Strong program management capabilities and clear communication among all partners and stakeholders

3. Clear, unambiguous responsibilities and contracts, to help reduce the risk of lengthy and costly renegotiations. Contracts should define in detail the following responsibilities among others:

    - How capital and operational costs will be shared by the parties in the PPP
    - How FirstNet's spectrum will be shared with the parties in the PPP
    - Identification of the party(s) that will own the network assets

- Identification of the party(s) that will design and deploy the network assets
- Identification of the party(s) that will operates and manage the network assets

4. Open, competitive, and transparent procedures for bidding and awarding of contracts.

5. Appropriate sharing of risks between the public and the private partners.

    - Governments and private entities should assume the risks that they are better equipped to bear. Private partner(s) should bear the risks of construction, network build and network performance. Governments should bear risks related to policy and regulatory uncertainty.

IV. 4G / LTE Network Strategy

The Internet is going wireless and communications and high tech companies on the quest for high performance are positioning themselves for the next wave of devices and services that promise to provide affordable, high-speed Internet access and data traffic for consumer electronics devices on the go. With 4G, FirstNet will have the opportunity to leverage carrier LTE networks to deliver lower-cost high bandwidth broadband services, VoIP, video and Internet access to a wide base of public safety users. However, prior to introducing these services, FirstNet should evaluate the entire range of options across the network, from entertaining new services, total CAPEX and OPEX costs, along with build and deployment strategies. The below information illustrates Accenture's Assets and point of view on the strategic components for planning and strategizing the introduction of new services and network build out costs.

Comprehensive modeling tools for plotting your course to high performance through 4G

To help service providers make wireless broadband decisions that can help drive high performance, Accenture has developed a unique 4G Solution Accelerator. This distinctive asset includes:

- A 4G modeling tool that gives providers the ability to model revenue potential, customer segmentation, future product strategy and the implications of various 4G build-out strategies. The tool helps providers highlight the costs, opportunities and tradeoffs involved with various wireless broadband technologies.

- Cost-effective approaches for retooling and then supporting operational and business support systems for a 4G world. The solution accelerator helps service providers jumpstart their 4G programs, reducing the risks and costs of introducing new 4G services.

The innovative modeling tool helps clients plan for their 4G future using three interlinked models:

1. Business Case Model

For existing operators looking to diversify their strategies and offerings, or for new wireless entrants, this integrated financial model helps enable analysis of the economics underlying any mobile business launch. For each of the different technologies and deployment strategies available, we use a unique business case model to help companies understand several critical business case metrics associated with a 4G deployment: revenues, impact on average revenue per user, market penetration, customer penetration, product strategies and underlying financial metrics.

2. Network Cost Model

   Using this modeling tool, we can help you estimate the cost of building out a 4G network based on LTE. This cost model can be based on various sets of business assumptions and product assumptions which allow the analysis of various mobility build-out strategies. The outputs of the model are:
   - An estimate of the spectrum needed, given the usage and subscriber growth projected by the business
   - Estimated network build costs in CAPEX and OPEX per year
   - A qualitative assessment of the various wireless technology options

3. Product and Services / Bandwidth Model

   This modeling tool helps operators estimate network bandwidth requirements for various combinations of products and services. Findings from this analysis can be input into the network cost model to provide a more detailed picture of the build-out costs.

Using these three models, and drawing on our own experience in the wireless broadband marketplace, we help incumbent operators and potential new market entrants make a fully informed decision regarding their entry into the 4G space.

A jumpstart for 4G business and operations support systems

Based on industry and technical skills with 4G technologies and solutions, Accenture provides 4G operators with a cost-effective and integrated approach to retooling their business and operations support systems for a more challenging 4G network environment.

Representative processes that we support include:
- Order-to-bill: from the customer service subscription made through the Web or a customer service representative, to the activation on the network as well as rating and billing.
- Customer care: including customer request management, trouble ticket management and contact management.

- Service delivery: including content management, network integration and delivery of value-added services through multiple channels

Our related business process outsourcing capabilities provide ongoing management of selected processes on behalf of a service provider according to predefined service level agreements. Such outsourcing capabilities can grow with you as your 4G strategy evolves.

Leveraging Accenture's Global Delivery Network and Innovation Centers we offer:

- Handset testing to help deliver a positive user experience of value-added services on multiple devices
- Digital content management
- Call center support (selected countries)
- A product factory to help manage the end-to-end service innovation process from service concept definition to implementation and operations

High performance delivered: Making the move to 4G

Accenture is already providing value to wireless providers based on its 4G Solution Accelerator. For example, a potential new entrant into the wireless broadband marketplace asked Accenture to help them evaluate possible entry strategies. The company needed to understand:

1. The revenue model associated with deploying a 4G network.
2. How much spectrum (for each technology) was required, given the company's usage and subscriber projections?
3. What the network CAPEX and OPEX costs would be to deploy such a network.

Using the three models at the heart of our scoping solution, the Accenture team prepared an in-depth analysis of the financial business case for the company's wireless broadband strategy.
We also provided valuable insight into the spectrum needed by the company, and the cost implications for putting various wireless broadband specifications in place, including a preliminary design for build-out of a nationwide 4G network.

Network Strategy Recommendations

Prior to building out a nationwide public safety network, Accenture recommends that FirstNet carefully evaluate all cost components associated with building a new network, roadmap for product service introduction, and an implementation timeline. Some of these activities include the following:

1. Wireless Strategy and Roadmap
    - Market Analysis
    - Business Strategy

   - Product Roadmap
2. Network Cost Model:
   - Wireless Technology and RF Assessment
   - Network Build Costs (OPEX and CAPEX)
   - Spectrum Requirements
   - Scenario Modeling and Sensitivity Analysis
3. Economic Models
   - High Level Revenue and Cost Model
   - High Level Cost information
4. Implementation Plan
   - State by State priority list

After the above areas are looked at in greater depth, FirstNet will have an understanding of the total costs of the network, product service introduction timeline, and implementation plan for new or shared network components.

V. 4G / LTE Network Sharing

Network Sharing is a common practice and something that Accenture has a great deal of exposure with globally. The more extensive a network share, the more advanced the organizational and contractual model between the sharing partners needs to be. The simplest form is site sharing, whereby mobile network operators share a site and one party pays a rental to the other for the use of a site. FirstNet will be required to look at a more extensive network sharing model that looks to share costs across all phases of network planning, build, and run activities. Some examples of network sharing include:

- **Operating joint venture**: where the network sharing organization manages and operates the assets of both "parents". Both parents contribute financial and human resources to the joint venture, which charges back its services to the parents on a net-net basis. Asset ownership typically stays with the respective partners.

- **Asset-owning joint venture**: where the network sharing organization takes control of the assets and liabilities related to the network share (for example, site leases or RAN equipment). In exchange both parents have an equity stake in the organization. Both also contribute human resources, which can be formally transferred into the joint venture or seconded to it.

- **Third-party operated:** where a neutral third party operates and manages all aspects of the network sharing venture and charges back all relevant costs to the different partners.

Network Sharing Recommendations

Pulling off a nationwide network with this size and scope will require a detailed network sharing modeling. FirstNet should look at the Third Party Operated model as one potential solution. In this model, FirstNet works with 1 or 2 neutral third parties in the effort of managing the network deployment and overall project/vendor management effort. An example, of how the model could work is below.

1. Recommendation on Network Sharing Model – **Third Party Operated**:
    - FirstNet:
        - Governance: Setting Network Policies and enforcing regulations
        - Asset Layer: Managing Core Network, Service Delivery Platform, NOC
    - State Government:
        - Asset Layer: Shared Radio Access Network and Backhaul
    - Wireless Network Operators:
        - Asset Layer: Shared Radio Access Network and Backhaul
        - Process Layer: Network Design, Optimization, Build, and Maintenance
    - Utilities:
        - Asset Layer: Shared Radio Access Network and Backhaul
    - Third Party – Integration and Network Deployment/Management
        - Company A: site acquisition, network design, and deployment of FirstNet network requirements
        - Company B: partner integration, testing, and project management, vendor management

2. Manage integration challenges
   Once a joint network sharing agreement is fully executed between the Wireless Network Operators, Utilities, and FirstNet the work to integrate these organizations will take place. In doing so, there will be some integration challenges to work through. Some of which include:

    - Network and site inventory systems rarely contain fully accurate information. So identifying which sites are available for sharing and where exactly they are located can be a much bigger challenge than typically anticipated. A network inventory validation and clean-up exercise at the start of the network sharing venture is therefore not a luxury

    - Mobile Network deployment is a complex and multi-staged activity and the workflow systems supporting this process reflect that. These systems are typically home-grown and aligning and coordinating between them can be resource-intensive. Recognizing this challenge early on and driving towards the selection of one preferred system can help

- In the case of active network sharing, the shared active elements need to be integrated back into fault monitoring and other OSS systems, while at the same time maintaining clear demarcations between the parents and the sharing venture.

A nationwide public safety network of this size and scope will require many players at the Federal and State Government level along with new partnerships with Utilities and Wireless Network Operators. Therefore, when considering the final network sharing model that best fits FirstNet, FirstNet should carefully balance the benefits, challenges, roles, and responsibilities across all partners to reap the benefits of a network sharing model.

VI. Mobile Application Strategy

The rapid evolution of commercial mobile devices has made technology an essential requirement for both government and commercial end users. The growing need to produce new and innovative mobile applications that provide mission critical or enhanced capabilities to our first responder workforce, along with common capabilities like security, has led to an enormous challenge when providing standardized solutions. FirstNet has the opportunity to provide a suite of mobile solutions that supports the array of commercial mobile operating systems and devices, satisfy robust and required security features, include scalable enterprise management functions, and provide features and capabilities required by emergency responders. Providing a suite of enterprise grade solutions that aligns with FirstNet's Mobility and Wireless solution needs requires detailed planning, assessment/evaluation, acquisition, development, integration, disposition, and continuous life cycle management of mobility products and services.

Accenture has a dedicated Mobility Services practice with thousands of people globally supporting mobility consulting, mobile security, mobile applications development and testing, mobile embedded software, and mobile managed services (e.g., mobile device management and application management and mobile business integration services) supporting a broad range of mobile work force solutions.

Furthermore, Accenture brings Federally-focused mobile and wireless security expertise, including:

- Experience deploying, configuring and supporting mobile devices for Department of Defense (DoD) clients.
- Support next generation secure mobile architecture for a Government agency.
- Authors/co-authors of NIST 800 series Special Publications, Defense Information Systems Agency (DISA) wireless security guidance/policy and Security Technical Implementation Guides (STIGs).
- Leadership in standards bodies, such as the Bluetooth Special Interest Group Security Expert Group and the Trusted Computing Group's Trusted Mobility Solutions Working Group.
- Active member of the DISA/DoD Mobility Working Group.
- Active member and contributor to the Open Web Application Security Project (OWASP)

- Accenture also has experience securing hosted and on-premise computing infrastructure for many Federal clients.

FirstNet Mobile Applications

For FirstNet, mobile applications can provide collaboration and communication to increase security and safety. Some examples of possible mobile applications include:

Safety Capabilities

1. Responder safety is paramount; mechanisms, preferably automated, that enhance responder safety must be built in at every level.
2. Location based services and applications which provide enhanced GPS information indicating where a distressed person is located (e.g. include indoor positioning and elevation).
3. Wild Fire Alert / Tracker App, Tornado Alert / Tracker App, Hurricane Alert / Tracker App, Health Service Location & Hours, Health Living Training App, Homeless Services App, Child Drug Protection App

Dispatch Capabilities

4. Process Automation – integrated standard operating procedures and alerting
5. Secure unified communications, Text to Speech / Speech to Text, Augmented Reality, Messaging apps, Push to talk apps
6. Sign-on / Signoff (on-duty, off-duty, etc)
7. Language Translation
8. Database lookup (license plate databases, drug interaction databases)
9. Real time patrol/fire/ambulance tracking

In the Field Public Safety Capabilities

10. Ease of use, the system cannot get in the way of the emergency responder as they try to do their jobs
11. Geospatial data, GIS Map Based Alerting and GPS Tracking
12. Voice, Text and video including recognition, incident recording and sharing
13. Sensor based applications for real time situation/mission awareness, recognition, identification of hazardous material and life safety, incident reporting.
14. Analytics application for traffic, safety and mission critical data.
15. Real time traffic awareness and remote control
16. Electronic mission and procedure compliance

Network Application Features

17. In Car – Wi-Fi to Cellular
18. Vehicle to Vehicle communication for network independent ad-hoc network for sharing data and real time imaging and video capabilities.
19. On-the-fly ability to create communication groups. It is impossible to predict in advance the parties that will need to communicate with each other in an emergency.

20. EANs – Emergency Area Networks – similar to the way Bluetooth allows devices to communicate with each other in a small area, devices should communicate with each other in an emergency area, for example, if the sensor on a firefighter's air pack signals low air supply, nearby firefighters should also be alerted.
21. The system should scale upward and downward. It should work equally well when there is connectivity with centralized infrastructure (cell sites, RF towers, etc.) or if only a handful of devices are in close proximity (firefighters fighting a wildfire in a wilderness area)
22. Ability to interoperate with ESInets as described in the NENA NG9-1-1 standards

Application Development

In order to develop applications in an open environment, public standards must be established through a community driven process. A Mobile Enterprise Application Platform (MEAP) should be established to connect with enterprise / back-end data sources and provide online/offline functionality, unified communications, security and data protection. The MEAP can provide firewalls to back-end IT infrastructure for public facing apps. For dynamic applications that need to access data sources, a cohesive API that does "one thing well" will help enable a clean interface where it needs to interact with other services. A clear strategy must define which APIs are public, consumer facing and those are private, 'authorized' users only.

An application security framework can address security at an application, network, device and data level to avoid security threats to public information as well as smooth operation of safety critical missions and data transfers. Features such as encryption, remote wipe and user control will need to be implemented and enforced. The MEAP can be employed to provide over the air security policy configuration and asset application inventory and reporting. A clear policy statement should also be created to explain what sensitive data about the members of the public is being held by whom and for how long.

Mobile applications can be developed in Native Operating Systems or as Cross-Platform applications. Accenture had a complete set of tools for Cross-Platform development and testing. For mobile application support regarding technology, platform, infrastructure and support, a Mobile Center of Excellence (MCoE) can be established to provide governance and strategy. MCoE will serve as the nerve center for all mobility development, promoting adherence to mobility strategy, acting as catalyst for every stage of mobile lifecycle - concept, development, testing, deployment and maintenance. Key MCoE responsibilities include:

- Coordinated selection, provisioning, management and control of both devices and applications using centralized tools for mobile device management (MDM) and mobile application management (MAM). Establishment of user support services for app developer and end users.
- Architecture and technical services to launch development kits for enhanced application development as well as integration of 3rd party components and tools to address the development of reusable component libraries for quick time to market.

- Evaluation of commercial off-the-shelf (COTS) or development of accelerators for application development for reducing time to market and standardization and enhanced quality.

The MCoE may be involved in defining or engaging a Mobile Application Factory. The Application Factory Delivery Model industrializes the delivery process, ensuring an enterprise can scale mobile solution delivery to meet standards. The MCoE model for testing solution would include a test strategy, test tool assessment, test infrastructure and selection, and development of deployment automation tools.

To meet application certification requirements, First Net should establish a testing framework and test lab equipped with devices across all platforms where applications will be launched and users will run the apps on multiple platforms. A user experience (UX) framework will be established for user evaluation, user interface (UI) and usability testing. Automation tools or test suites can be used for standard functions such as security testing, interfaces, reusable library components, mobile device and application management for all categories of testing for certification such as functional, protocol conformance, performance & benchmarking, service monitoring, geographical variance, wireless network variations, security of data on the device and in the air.

The test framework should address the entire test lifecycle approach to certify and launch apps including strategy and planning, setup and execution, reporting, and post launch maintenance – for all types of application platforms such as native, hybrid, web app/html, middleware or MEAP platforms, widgets and browser apps.

A mobile steering committee can provide the governance overlay to manage mobility policies, standards and processes. Developing a primary mobile strategy will guide the selection and prioritizations of products for devices, OS, platform and applications that helps ensure a framework for all sub-strategies. The lack of primary mobile strategy can lead to backtracking.

Application Delivery

There are several avenues available for App developers and Enterprises to Deliver Mobile Applications to their consumer/employee base.

1. Apple AppStore, Google Play, BlackBerry AppWorld, Windows MarketPlace
    a. Online Stores hosted & managed by the OS/device manufacturers for application hosting/purchase/delivery
    b. Revenue sharing may apply
    c. Strict Application Certification process
    d. High level of security & confidence in the quality of apps
    e. Discovering apps is easy on these stores

2. Web apps downloaded via web portals
    a. Web hosting/purchase/delivery, can be hosted by any web portal owner
    b. Revenue sharing does not apply

c. Application Certification does not apply
d. Low confidence on security and quality aspects
e. Discovering is hard as the users have to get to the web portal first to discover the app

3. Enterprise App Stores (Accenture's EAC)
    a. Stores hosted by NTIA to provide enterprise apps to emergency responders, other employees and public safety workers
    b. No revenues sharing or App certification applies. However the NTIA can have their own Certification/entry process
    c. Highly secure and can be restricted within public/private cloud.
    d. Policy enforcement is easier and more effective
    e. MDM, MAM solutions can be integrated with this solution

4. Network Operations Store
    a. This concept has not been explored much in commercial but this could be something NTIA can look to setup for network specific apps for emergency responders. This can host applications for network performance monitoring and optimization as well as user apps.
    b. This could also include network roaming apps and geo-location based on network infrastructure in cases where GPS is not available.

Mobile Application Recommendations

Mobile Assessment

Since the mobility landscape is continuously changing with evolving technologies, conducting a thorough or updated assessment of FirstNet's mobility environment along with its requirements would help to identify any additional needs for mobility services. Accenture has supported a number of government agencies and commercial companies with strategy and technology consulting services that included conducting mobility assessment as the first step identifying the requirements to determine an appropriate set of solutions to meet those requirements.

Mobile Application Security

There are essentially three key steps to securing mobile applications – development, testing, and deployment and maintenance. Organizations seeking higher security for mobile applications need to develop a defined process and guidelines for a secure mobile application development lifecycle. Accenture takes a vendor-agnostic approach that pulls together best-of-breed solutions for each phase of the lifecycle for a range of solutions. This includes mobile application security code review, vulnerability assessment and penetration testing.

Mobile Research, Testing, and Pilots

Staying current on evolving mobile technologies such as new operating systems, devices, applications, and hardware components would provide FirstNet with a proactive way of determining if emerging solutions improve or modernize existing capabilities to meet near and long-term objectives for mobility. Accenture has five global Technology Labs focused on understanding our clients' needs and forecasting new and emerging technologies and trends in order to meet current and future challenges. For Mobility, we evaluate capabilities of the future and work with industry leaders and small business with unique solutions. We have the infrastructure and resources with the capabilities to assess, test, and pilot mobile solutions to better understand the features and functionalities before they become mainstream products.

Conclusion

FirstNet has great opportunity ahead of it and it is important that the program identify challenges and pave the way for success. What FirstNet achieves will be historic and the culmination of over a decade of hard work and coordination among first responders in the public safety community. As discussed, there will be many challenges for the FirstNet program including governance, funding, technical and operational issues related to network planning and deployment, as well as the associated set of challenges for application development and support. Nonetheless, it is possible to overcome all of these challenges through the right organizational structure, strong leadership, and a sound strategy. With these things in mind, Accenture recommends that FirstNet consider the following activities for immediate next steps over the next 60-90 days:

1. Formalize governance structure and roll-out across federal, state, and local levels.
2. Implement awareness campaign to ensure that knowledge about FirstNet decision-making process is disseminated across all stakeholder groups.
3. Initiate FirstNet Nationwide Network and Mobile Application Strategy effort to assess business, technical, and operational requirements for the FNN and related applications.
4. Develop high-level network architecture based on agreed-upon approach for PPP and various operational entities.
5. Develop detailed network cost model based on intended architecture and conduct financial assessment across all funding entities.
6. Revise business model, underlying network architecture, and deployment plan as required to reflect available sources of funding and input from stakeholders.
7. Develop procurement strategy and create detailed sourcing plan.
8. Formalize PPP and solicit states for individual state-by-state plans.
9. Initiate network sourcing effort based on state-by-state plans.
10. Work with vendors to solicit proposals and select potential industry partners.

By drawing on the best industry experience available and the leveraging the recommendations provided above, it is Accenture's belief that FirstNet can overcome the myriad barriers to success and achieve what has never been achieved before: a nationwide interoperable public safety broadband network for the United States of America and its dedicated core of first responders.

Respectfully submitted,

Accenture Federal Services LLC

Christopher Smith
Chief Technology and Innovation Officer
christopher.l.smith@accenture.com
+1 703 947-3409

Robert Casselman
Public Safety Broadband Lead
robert.c.casselman@accenture.com
+1 917 452-4484