Bechtel's NTIA and FirstNet NOI Response

Submitted by:
Gregory L. Frank
General Manager, Defense & Security
Bechtel National, Inc.
12011 Sunset Hills Road
Reston, VA 21090-5919
Office: 703.429.6331 Cell: 240.409.3494
Email: glfrank@bechtel.com

FirstNet NOI Response Summary

This FirstNet Nationwide Network (FNN) Proposal and Presentation to the Board is generally consistent with the recommendations that Bechtel has made for the past 5–8 years in connection with various public safety and border control proposals including Integrated Wireless Network, Secure Border Initiative, and Morgan O'Brien's US Public Safety Initiative in 2004. We have always believed that using the established carrier infrastructures (wireless, backhaul, and national fiber networks) will be the most cost-effective FNN approach. Bechtel has performed site acquisition and has built and upgraded more than 115,000 cell sites across the United States and has installed the associated wireline, microwave and fiber backhaul networks. Based on our experience, duplicating this effort for the FNN would be neither cost effective nor efficient.

Due to the complexity of deploying the FNN based on a single, nationwide network architecture that evolves with technological advancements, we believe it is absolutely essential to the success of the FNN that NTIA and the FirstNet Board select a single recognized program management firm to implement the program. This firm must be technology and vendor agnostic, along with being carrier neutral. The need to deploy a reliable, ubiquitous, redundant, and interoperable broadband network for public safety users clearly requires an integrated systems engineering approach. Furthermore, program success is a direct function of empowering national

oversight (setting technology standards, controlling costs and schedules, deconflicting logistics and network issues) while maximizing state, local, and tribal content ("national reach with a local touch"). The general attributes of such a program management firm are detailed later in this discussion.

This "single-point accountability" program management approach generally described above will:

1. meet public safety requirements for priority, quality of service, and preemption features;
2. use, to the extent possible, existing radio access network and core network infrastructure installed by commercial mobile operators in order to maximize the coverage and performance delivered to public safety while minimizing the capital expenditures;
3. reach operational capability as quickly as possible; and
4. enable voice services (cellular telephony and push-to-talk) both within the FirstNet network and to/from other commercial networks including the public switched telephone network.

Furthermore, we suggest a continuation of state, county, parish, local, and tribal (generically "local") grant programs on a nationally controlled and systems integrated basis. Many procurement requirements involve the need for continuity of local operations and maintenance support. A few examples include vehicles purchased from local dealers (to a common specification), training budget support, and hiring of key local personnel such as a Communications Security (COMSEC) Officers or local Facility Security Officers (FSOs), etc. These grant programs are best managed by local authorities, many of whom are not able to muster the necessary budget to support FNN success at the local level. A grant request process would be beneficial in identifying additional areas that are best served by these local authorities.

Some Specific Comments to FirstNet Nationwide Network Presentation

Slide 3 lists one of the FirstNet assets as the 2 x 10 MHz of nationwide spectrum, which lives at the 700Mhz level in Band 14. While a dedicated spectrum is beneficial, most of the presentation focuses on LTE/4G radio access network (RAN) technologies, and most of the smartphone technologies working at today's LTE/4G spectrum allocations are not living in the 700MHz, Band 14 spectrum area. Future smartphones based on software-defined radios may be more readily adaptable to the FNN dedicated spectrum. Bechtel's Chief Technologist (Integrated IT and Communications Sector) is an LTE/4G expert and is willing to develop an executive overview on the last mile RAN technology issues, which could be helpful to NTIA and the FirstNet Board since it would be objective (technology agnostic, vendor and carrier neutral). NTIA and the FirstNet Board need to be wary of those who would attempt to leverage old LMR technologies to continue to supply dedicated radios that work only at the FCC-granted 700 MHz, Band 14 spectrum. Reaching out to Apple and other smartphone suppliers at this early stage on this 700 MHz issue is very important.

Another issue worth considering is that most first responders usually carry their own smart cellphones. This is the same issue that the corporate enterprise world is dealing with (i.e., bring your own device, BYOD). Aside from important BYOD cybersecurity concerns, FNN needs to encourage the use of smartphones that have high-resolution cameras and video capabilities so responders can stream critical footage of crisis or emergency events live to local, state, or national response centers. Carrier-specific applications (plus training) would allow these first responders to use their own smartphones to record such events without incurring high data usage costs. This will encourage proactive behavior immediately and provide the best "on-the-scene" intelligence, probably from multiple sources that will be crucial to assessments and

allocation of the proper support resources and forces. More details are provided in the FNN applications section at the end of this submittal.

Slide 6 puts forth the concept of mobile network operator (MNO) partners. We suggest going a little further by having FNN be a more formal mobile virtual network operator (MVNO) that is technology neutral, vendor agnostic, and carrier neutral, retaining the specific rights to deploy special cyber security monitoring equipment, priority switching, and encryption technology at various parts of the network.

The scope on Slide 6 strongly indicates the need for the program management approach suggested earlier to manage the FNN relationships. Our comment on the last bulleted point on this slide is that Bechtel has extensive experience in forming, managing, and financing public/private partnerships. This experience stems from our Bechtel Enterprises and Bechtel Systems and Infrastructure projects over the last few decades where we have helped develop numerous shared infrastructure models for public/private collaboration, including some for global wireless carriers.

Slides 8 and 9 point out the complexity of creating a diverse nationwide network that interconnects multiple wireless networks and systems—this is part of the scope involved in the "managing complexity" requirement. Although it is complex, this approach entails the lowest overall cost, but only if it is managed correctly.

Slide 10 shows the over 285,000 national cell sites; Bechtel has played a role in establishing over 115,000 of these. This reinforces our mutual agreement on not duplicating any established infrastructure that may be used. An important lesson learned is the need for proper early focus on the national backbone network. Many previous implementations place the greatest focus on the "last mile" radio link issues; however, success requires an equal focus on the "cyber

secure" national backhaul network, especially with the current real threat of a "cyber Pearl Harbor." We all remember the early cellular deployments that started out using T1 (1.5 Mbps) copper lines as backhauls to early 2G cell towers. Today's 4G/LTE data-intensive cell sites require fiber optic bandwidth capabilities. The FNN could look like DISA's and the IC's dedicated networks using leased fiber IRUs with truly diverse physical routes. Today, a fiber pair can carry 40 x 100 Gig DWDM wavelengths. **Slides 13–19** show this distributed core network in a conceptual framework. This network requires collaboration with more than just AT&T and Verizon … Level 3, Google, and others could also play an important role. Additionally adding these other network players to the mix will ensure a better competitive environment and keep cost under better control. **Slide 11** illustrates this point but is not clear on the national backhaul network that will be the key backbone during regional or national emergencies when connecting to the state-controlled National Guard or DOD forces may be necessary. Additionally, it will be critical to connect to the FBI, DHS, and NSA/Cyber Command (NTOC, etc.) centers to blue and red team the network, keep cyber defenses current, and help combat cyber-attacks/penetrations. The ability to work closely with NSA's Information Assurance Mobility Fusion Team is another critical technical resource that needs to be incorporated including the ability to talk strategically with them on the tough N2K (need-to-know) issues.

Slide 20 "FNN Solves Several Critical Issues" is generally correct, assuming that some qualified program management firm is managing the complexity rigorously. However, the FNN needs to incorporate the cyber security and national fiber optic backbone network elements more clearly. "Ubiquitous US coverage provided through satellite network integration" (last bullet) will not solve the problem. Satellites have low bandwidth, are more expensive to operate, and are not reliable under a number of attack scenarios (nation state, cosmic solar flares, etc.).

Program Management Firm Attributes to Manage Complexity (A National Trusted Agent)

These attributes are offered as a basis for a minimum requirements document and are not in any order of importance. The firm must:

1. Have the required program management talent pool including persons with FBI InfraGard memberships and TS//SCI clearances in order to understand and work on complex cyber security issues with the full range of federal agencies.
2. Be a recognized program management organization that is known for managing complexity and, importantly, is technology agnostic, vendor and carrier neutral.
3. Have trusted agent experience (US and foreign).
4. Be experienced in serving multiple wireless/wireline carrier customers.
5. As a Federal Procurement, the FirstNet work would be subject to government audits. The program management firm must be organized for transparency, must have been audited by the US Government on a regular basis, and must be compliant with US Government auditing requirements.
6. Have the ability to augment its resources from its commercial business units and/or team with other firms, as may be required.
7. Have an established and proven national procurement subcontracting system capable of soliciting and managing competitive bids from local installation and O&M contractors. The prospective PM firm should state the number of qualified subcontractors that it has used previously in national communications deployments that would benefit the FNN and be able to maximize local content using local contractors for construction and life-cycle O&M. In other words, the prospective PM firm should demonstrate how work is

subcontracted on a local city, county, and state basis. This coverage helps ensure that every congressional district gets work.

8. Have site acquisition and real estate talent to understand how to deal with all tower companies for infrastructure sharing and tower upgrades. The firm must have a proven ability to work with not only carriers, but also the many tower or other shared infrastructure providers, if and when necessary. It must also be able to perform make/buy financial analyses and assess RF issues for areas of low coverage where using dedicated infrastructure on an existing tower as compared to a carrier's infrastructure on that tower will offer benefits.
9. Provide strategic planning capability to integrate national carrier interests with local competitive bidding for non-emergency services.
10. Understand MVNO concepts for potential strategic integration of national carrier with local first responder needs and desires.
11. Understand wireless RF spectrum technical and political issues.
12. Understand and have the ability to integrate existing (or organize building new) national backhaul to ensure national emergency response capability.
13. Have established, recognized communications industry safety programs and culture; safety must be a core value. Bechtel examples include ARC Flash and Tower Climbing Safety Programs.
14. Bring cyber security savvy and must understand the impact on US critical infrastructure.
15. Have an understanding of US Government-approved security operations to support classified operations; NSA's Secure Mobility Program (Fishbowl) may play into FNN at some point.

16. Have developed smartphone applications for internal use on project sites or environmental cleanup operations in order to improve communications efficiency and solve problems locally with central or national resources support.
17. Have established program/project management and cost control systems to manage a nationally distributed program consisting of numerous local projects and diverse workforces.
18. Have design engineering depth to design any unique FNN needs, integrate national standards adapted to meet local zoning requirements, and properly assess tower/infrastructure upgrades including load limits as any new FNN equipment may be added to existing systems/infrastructure. The firm must be adept in developing conceptual design, performing systems engineering, managing detailed design life cycle, and managing competitive firm fixed price bidding for specific task orders or local projects.
19. Be able to utilize lean Six Sigma processes and techniques to increase quality while prudently reducing costs.
20. Understand the need to share critical infrastructure for economies of scale and develop cooperative tower company and carrier relationships.
21. Be able to field rights-of-way and site acquisition teams nationally to create consistent leases in an integrated, manageable database. The firm must have the ability to work out local zoning issues and mitigate schedule delays and associated cost ramifications.
22. Have worked with an identified small business that can provide a program management office (PMO) and would create an additional agnostic layer between the integrator and the PMO.

Information Systems and Technology Capabilities and FNN Application Suggestions

Bechtel has an extensive corporate Information Systems and Technology (IS&T) infrastructure including teams that develop applications to support efficient global project deployments. Bechtel has awarded a number of internal technical grants to develop wireless technology applications for use on its project sites, and many of the applications may be directly relevant to the FNN and the first responder community. For example, we have developed the ability to bring national or central engineering talent to the local jobsite via video conferencing and recording using wireless hardhat cams, iPads, and smartphones. NTIA and the FirstNet Board should review this evolving capability to determine its applicability at a later date. This review will involve an extensive dialogue with our Corporate CIO and his Global Business Unit CIOs, especially Bechtel's Government Company CIO who works closely with our Government Security & Surety team on COMSEC, OPSEC, and cybersecurity matters—all critical to FNN success.

One immediate use of the LTE/4G network would be development of a specific application for qualified first responders to communicate with their respective local, regional, or state command centers. Called "FNN-Time," this application would be similar to Apple's "FaceTime" and would provide the following features and benefits:

1. It enables immediate use of the LTE/4G evolving national infrastructure incorporating a BYOD concept since many first responders carry their own personal smartphones.
2. It provides an interim solution while awaiting software defined radio improvements that better utilize the FCC-granted 700 MHz, Band 14, spectrum in commercial off-the-shelf smartphones.
3. The costs associated with using this application for FNN purposes would not bill to the

individual but to some central cost reporting source based on an MVNO agreement with each carrier.

4. National Communications Systems GETS-like network priority tasking can be achieved working with the specific carriers.
5. MiFi-enabled video cameras and recording devices could be integrated (e.g., helmet-, body-, or hand-mounted/controlled cameras).
6. Real-time video enhanced incident reporting will be significantly improved. Aside from immediate use by the appropriate command center, this information source can be added to national incident databases for after-action analysis. One example would be linking the compiled feeds into the classified and unclassified FBI InfraGard "Daily National Incident Reports" that are grouped by critical infrastructure sector.
7. Per MVNO agreements with specific carriers, dedicated Cellular on Wheels units could be deployed to sites where extensive longer-term HazMat or rebuilt infrastructure projects would be required. This would free up data-intensive use of the local carrier's cell sites; however, it does directly link to issues associated with the FNN national backbone.
8. Regional network handoffs to the FNN broadband network (transition from commercial cellular and backhaul to the FNN) can evolve logically and prudently. The application would provide improved cyber security and related monitoring for these backhaul circuits to incident response analysts for greater national assessment by the appropriate agency or government department such as the FBI, DHS, FEMA, DOD and related agencies, DOE, NRC, EPA, et al.