Before the
Department of Commerce
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Development of the Nationwide	)	Docket No. 120928505-2505-01
Interoperable Public Safety Broadband	)	
Network	)	

COMMENTS OF THE SAN FRANCISCO BAY AREA REGIONAL INTEROPERABLE COMMUNICATIONS SYSTEMS AUTHORITY (BayRICS)

Barry Fraser
Interim General Manager
BayRICS Authority
4985 Broder Blvd.
Dublin CA 94568
(925) 803-7882
barry.fraser@sfgov.org
www.BayRICS.net

EXECUTIVE SUMMARY

The Bay Area Regional Interoperable Communications Systems Authority ("BayRICS") welcomes the opportunity to respond to the above-titled Notice of Inquiry ("NOI") on the conceptual network architecture presentation made at the First Responder Network Authority ("FirstNet") Board of Directors' meeting of September 25, 2012 and related matters. BayRICS offers the following comments, organized in four sections.

BayRICS recommends in Section I that FirstNet take action to quickly restart our Bay Area Enhanced Wireless Broadband ("BayWEB") project and the other BTOP grant projects. Quickly restarting these projects will preserve the work accomplished and immediately infuse an additional $382 million in BTOP funding into the nationwide network. In addition, early deployment projects such as BayWEB can also provide immediate benefits to FirstNet, as pilot projects to test business models and incubators of new public safety applications.

Section II focuses on four key recommendations for improvement of the conceptual network architecture presentation. First, BayRICS supports the concept of multiple network paths incorporating three to six wireless networks. However, we propose that "Layer One" of the conceptual design consist of a mission critical public safety network built with hardened sites meeting public safety grade specifications. This first layer of the network must provide the bandwidth availability, redundancy, and reliability in all network impacting scenarios including natural disasters, large public events, or other large scale incidents. The remaining layers of the conceptual design should consist of "add-on" commercial networks that would provide roaming and redundancy to enhance the coverage provided by the Layer One network.

Second, BayRICS recommends that physically separating the Service Delivery Platform ("SDP") from the Enhanced Packet Core ("EPC") and distributing the SDP core elements locally

will result in reduced backhaul costs, improve system performance and provide local public safety agencies with more control over network functionality. BayRICS has developed a proposed extension of BayWEB to serve the nearby Sacramento, California region in which Sacramento user data traffic could remain in-region by deploying a Remote Serving and Packet Gateway ("RSPG") architecture. This model could easily be adapted to expand service to other western United States regions that would share the San Francisco EPC, while retaining regional control through a localized RSPG architecture. In addition, localizing the RSPG improves system performance and reduces backhaul costs because high bandwidth user data traffic is not routed to the remote core.

Third, to ensure that the architecture model is viable, FirstNet should conduct more research on user devices to ensure availability and practicality for use on multiple commercial carrier networks. Fourth, the FirstNet architecture model must allow sufficient local control over public safety services that will be used by local first responders.

Section III of these comments addresses business plan considerations and provides a high-level overview of the BayWEB business and funding plan. Finally, Section IV describes public safety applications for public safety users and recommends deploying BayWEB as a test bed for application development.

BayRICS eagerly looks forward to the next steps in planning and deploying of the nationwide network, and we encourage FirstNet to treat this NOI response as the starting point in an ongoing collaboration with BayRICS to share information on these matters.

Table of Contents

I. INTRODUCTION 1

II. FIRSTNET SHOULD LEVERAGE THE BTOP PUBLIC SAFETY GRANT FUNDING BY QUICKLY RESTARTING BAYWEB AND THE OTHER EARLY BUILD PROJECTS 2

III. SPECIFIC COMMENTS ON THE CONCEPTUAL NETWORK ARCHITECTURE PRESENTATION MADE AT THE FIRSTNET BOARD OF DIRECTORS' MEETING ON SEPTEMBER 25, 2012 3

A. Design "Layer One" as a Mission Critical Public Safety Network 4

B. Localize "Service Delivery Platform" Functionality to Reduce Backhaul Costs, Improve System Performance and Enable Local Control 5

C. Conduct More Research to Ensure Availability and Practicality of Devices for Use on Multiple Commercial Carrier Networks 8

D. Add Specific Requirements to the Architecture Model to Ensure Adequate Regional and Local Control of Public Safety Services 9

IV. BUSINESS PLAN CONSIDERATIONS 11

A. BayWEB Business Model Highlights 11

B. BayWEB System Funding Plan Highlights 14

V. APPLICATIONS DEVELOPMENT FOR PUBLIC SAFETY USERS 15

A. Applications for Public Safety 15

B. Leverage the Early Builder Networks as Test Beds and Incubators for New Public Safety Applications 19

Before the
Department of Commerce
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Development of the Nationwide	)	Docket No. 120928505-2505-01
Interoperable Public Safety Broadband	)	
Network	)	

COMMENTS OF THE
SAN FRANCISCO BAY AREA REGIONAL INTEROPERABLE COMMUNICATIONS SYSTEMS AUTHORITY (BayRICS)

I. INTRODUCTION

BayRICS[1] submits these comments in response to the National Telecommunications and Information Administration ("NTIA") Notice of Inquiry ("NOI") released September 28, 2012, in the above-entitled proceeding.

BayRICS welcomes the opportunity to comment on the conceptual network architecture presentation made at the FirstNet Board of Directors' meeting held on September 25, 2012 and related matters. As a 700 MHz public safety broadband spectrum waiver recipient and beneficiary of a Broadband Technology Opportunities Program ("BTOP") grant, BayRICS members and staff have dedicated the past several years to developing an extensive body of knowledge on public safety broadband networks, business models and applications, specifically geared toward the early deployment of the Bay Area Wireless Enhanced Broadband ("BayWEB)

[1] The BayRICS Authority is a 13-member California Joint Powers Authority organized pursuant to the Joint Exercise of Powers Act, California Government Code Section 6500 *et seq*. Members of the BayRICS Authority include State of California, City and County of San Francisco, City of Oakland, City of San Jose, Counties of Alameda, Contra Costa, Marin, San Mateo, Santa Clara, Sonoma, and "hub" City groups from the East Bay and South Bay.

project.[2] We encourage FirstNet to treat this NOI response as the starting point in an ongoing collaboration with BayRICS to share information on these matters.

As a member of the Early Builders Advisory Committee ("EBAC"), BayRICS concurs in and supports the comments submitted by EBAC, as well as the joint comments of the National Association of Telecommunications Officers and Advisors (NATOA), the National League of Cities (NLC), the United States Conference of Mayors (USCM), and the National Association of Counties (NACo). BayRICS also supports the comments of the Washington State Interoperability Executive Committee (SIEC), particularly as they relate to the innovative concept of a multi-state pilot project for Pacific Rim states. BayRICS describes in Section II below specific network architecture enhancements that would facilitate such a pilot.

II. FIRSTNET SHOULD LEVERAGE THE BTOP PUBLIC SAFETY GRANT FUNDING BY QUICKLY RESTARTING BAYWEB AND THE OTHER EARLY BUILD PROJECTS

The FirstNet Board must move quickly, and in close coordination with state, regional, tribal and local entities, to develop a plan for the construction of the nationwide public safety broadband network ("NPSBN"). One way this can occur is to allow early builders, such as BayRICS, to complete their projects. Allowing these early pilot projects to continue will create valuable and cost-effective solutions to many of the challenges faced by FirstNet, and will also immediately infuse an additional $382 million in BTOP funding into the nationwide network.

BayRICS asks the FirstNet Board to quickly provide recommendations to NTIA to allow the BTOP-funded BayWEB project to restart deployment. This is a matter of the utmost urgency for the Bay Area. BayRICS Members and Motorola have worked for two-years on extensive

[2] BayWEB is a public-private initiative with Motorola Solutions, Inc. Motorola is the recipient of the BTOP grant funding for the BayWEB project.

efforts to launch the BayWEB project and begin network build-out. We have laid a solid foundation by completing the most complex and time-consuming project tasks required for system deployment. No other multi-jurisdiction urban region has progressed this far toward project deployment of a public safety broadband network.

We believe that it is in the best interest of both Bay Area public safety and FirstNet to complete the BayWEB project as soon as possible. Quickly restarting the project will preserve the work accomplished and the funding and other resources committed to the BayWEB project. Quick action to complete these projects will also fulfill the Obama Administration's goal of spending federal stimulus dollars in a timely manner.

Early deployment of BayWEB can also provide immediate benefits to FirstNet. The BayRICS-Motorola partnership, described in Section III below, is based on a business model that contemplates local infrastructure contributions and private partner management and operations, The BayRICS model could be used by FirstNet as the starting point for a viable business model template for local agency participation. In addition, the Bay Area, as home to a host of communities of application developers, can become an incubator of innovative public safety applications. As we describe in Section IV, BayWEB could become a robust test bed for new applications development—but only if it is allowed to proceed soon.

III. SPECIFIC COMMENTS ON THE CONCEPTUAL NETWORK ARCHITECTURE PRESENTATION MADE AT THE FIRSTNET BOARD OF DIRECTORS' MEETING ON SEPTEMBER 25, 2012

The conceptual design provided by FirstNet provides a solid initial framework on which to build the National Public Safety Broadband Network. BayRICS encourages FirstNet, as it develops this model, to incorporate design elements that create a dedicated, truly mission-critical broadband network that remains viable during weather-related incidents, natural disasters and

other widespread emergencies. This network must be capable of carrying increased traffic loads during such incidents, in contrast with carrier-grade networks, which often experience congestion, dropped calls or outages in similar situations. With this design vision in mind, BayRICS offers the following specific comments to enhance the conceptual architecture model.

A. Design "Layer One" as a Mission Critical Public Safety Network

On slide 11 of the FirstNet model, the concept of multiple network paths incorporating three to six wireless networks is introduced. These multiple layers create a highly redundant network solution and should remain an ultimate goal of FirstNet. However, this model, on its face, may not provide the level of network reliability that Public Safety requires in mission critical environments.

BayRICS proposes that "Layer One" of the conceptual design consist of a mission critical public safety network built with hardened sites meeting public safety grade specifications, including security and redundant emergency power, HVAC, and backhaul. This first layer of the network must provide the bandwidth availability, redundancy, and reliability in all network impacting scenarios including natural disasters, large public events, or other large scale emergencies.[3] The remaining layers of the conceptual design can then consist of "add-on" commercial networks that would provide roaming outside of the coverage provided by Layer One. The commercial layers could also provide redundancy in the unlikely event that the hardened mission critical Layer One encounters a problem.

BayRICS believes that the Layer One private network can be deployed in many parts of the country in a cost-effective manner by leveraging state and local infrastructure that is already

[3] The need for network redundancy and hardening has been highlighted by recent commercial service outages throughout the eastern United States caused by the June 2012 Derecho and by Hurricane Sandy.

hardened for public safety and other governmental uses. In addition, FirstNet should consider deploying the Layer One Radio Access Network ("RAN") on a State or regional basis, to allow maximum efficiency in identifying and allocating local infrastructure elements. States should also be allowed flexibility to structure partnerships with local critical infrastructure providers to build, use, operate and maintain local RANs. This approach would also provide state and local government an appropriate degree of decision-making authority and control over the implementation of the network to help maximize its usefulness and create buy-in from local public safety agencies.

B. Localize "Service Delivery Platform" Functionality to Reduce Backhaul Costs, Improve System Performance and Enable Local Control

Slide 14 of the FirstNet model presentation describes a "Distributed Core Network" consisting of both an Enhanced Packet Core ("EPC") and Service Delivery Platform ("SDP"). However, in cases where a regional core serves multiple local areas, BayRICS recommends that physically separating the SDP from the EPC and relocating the SDP locally will reduce backhaul costs, improve network performance, and provide local public safety agencies with more control over network functionality.

BayRICS staff, the BayRICS Technical Advisory Committee ("TAC") and Motorola have conducted considerable research in developing a proposed extension of BayWEB to serve the nearby Sacramento, California region. The challenge in providing this regional service was two-fold: (1) how to preserve a large degree of local control for Sacramento public safety users sharing an EPC located in San Francisco; and (2) how to avoid the high backhaul costs of routing Sacramento user data traffic (particularly streaming video data) through the San Francisco EPC.

We devised a model in which the Sacramento user data traffic can remain local by deploying a Remote Serving and Packet Gateway ("RSPG") architecture, as depicted at a high-level in Figure 1 below.

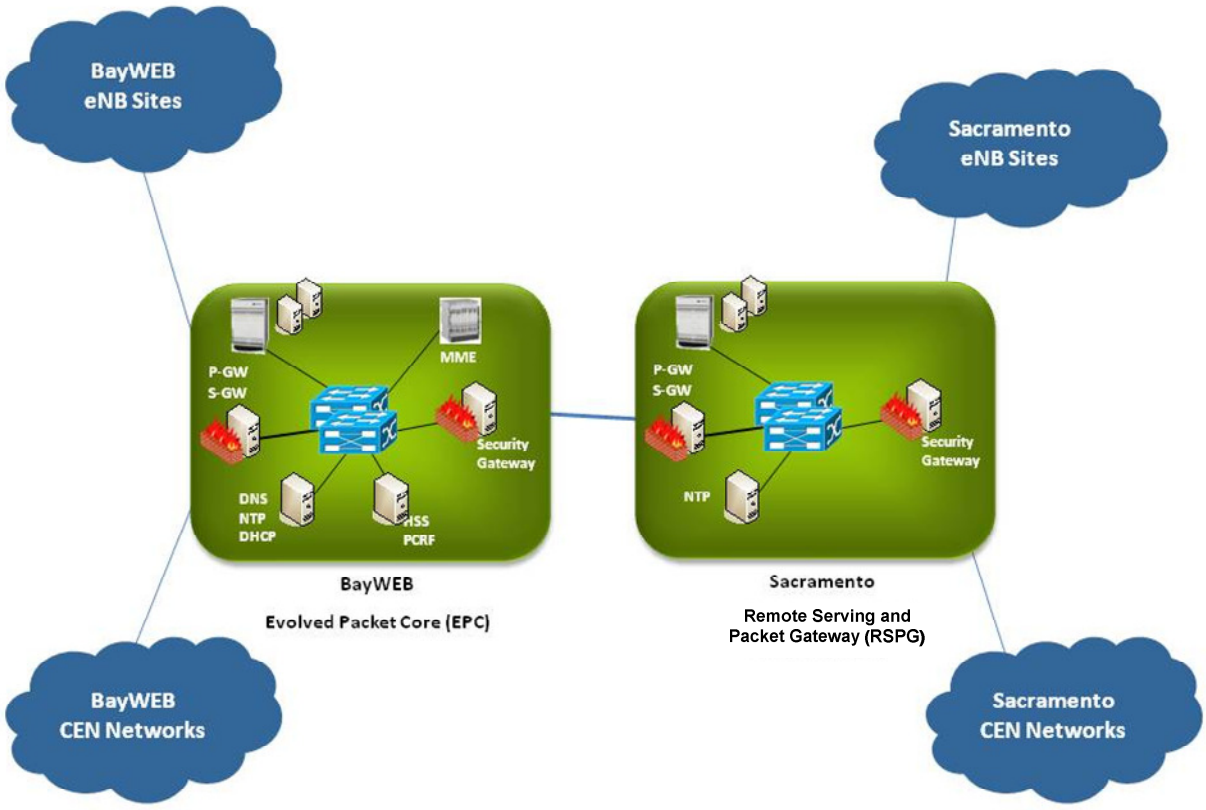

Figure 1: Remote Serving and Packet Gateway Architecture

This architecture describes a fully functional EPC located in San Francisco, but allows other agencies, Sacramento in this case, to connect to the EPC remotely through a RSPG. This architecture allows the high bandwidth user traffic to remain local to the region in which the RSPG is implemented in and the low bandwidth signaling traffic to be passed on to the EPC. This configuration provides several advantages to the FirstNet Network and the public safety agencies using the network.

One key advantage is lower bandwidth requirements (and lower costs) for regional backhaul. The implementation of the RSPG architecture provides improved backhaul reliability and eliminates the need for long distance and very expensive high capacity backhaul circuits to be routed to a BayWEB/FirstNet EPC that could be geographically distant. The RSPG architecture allows the high bandwidth user traffic (*e.g.* streaming video) specific to a region to remain in that region with short, high-bandwidth backhaul links. Only the very low bandwidth signaling and control traffic would continue to be routed to the BayWEB/FirstNet EPC, reducing bandwidth requirements and costs for EPC connectivity to the remote region.

In addition, localized RSPG would provide the optimum network reliability for all regions served by an EPC. An incident with high bandwidth requirements in one RSPG region would not impact the system performance in another RSPG area because RAN coverage and capacity and backhaul capacity are isolated and local to the impacted region. Without a localized RSPG, each RAN site would require a high bandwidth, reliable, redundant connection to the distant EPC. The RSPG architecture requires only a connection from RAN site to the local RSPG, reducing costs and simplifying the EPC network.

The localized transport of the RSPG architecture also improves the inter-eNodeB handoffs. Because the RSPG keeps traffic local to the coverage area, the handover speed of switching between eNodeBs (eNBs) improves due to reduced backhaul latency. In addition, RSPG architecture requires less complexity for IP network interconnections and associated security perimeter enforcements. Another benefit of the RSPG architecture is improved application performance due to reduced end-to-end delays between the user and the core. The end-to-end delays impact the performance of mission critical Push to Talk and video services over LTE.

The RSPG can also provide geo-redundancy of the bearer traffic because regional RSPGs could be configured to back each other up. The RSPG architecture simplifies the connectivity between each eNB and the EPC.

Finally, and most importantly to public safety, the RSPG architecture provides increased control of the network by the local users. The RSPG allows local users (Agencies) to establish connections from their enterprise networks to the local packet gateway controlled by the region. BayRICS believes that this would facilitate the adoption of FirstNet service within smaller agencies. Additionally, the Priority Service Manager responsible for identifying call priority and Quality of Service ("QoS") could be located at the regional RSPG, thus allowing priority and preemption settings to be controlled locally.

Although this model was developed specifically to allow for a San Francisco-based EPC to more efficiently serve Sacramento, the model could easily be adapted to expand service to other western United States regions to share the San Francisco EPC, while retaining regional control through a localized RSPG architecture. BayRICS encourages FirstNet to explore the localized RSPG architecture model as a way to address the concerns of many public safety agencies regarding local control issues.

C. Conduct More Research to Ensure Availability and Practicality of Devices for Use on Multiple Commercial Carrier Networks

Slide 11 in the FirstNet architecture presentation assumes that multiple terrestrial mobile partners will provide overlay coverage and service to support and enhance the FirstNet Band 14 network. However, such a model would require user devices capable of operating on the spectrum bands of each mobile partner. The devices available to public safety must support the final network configuration requiring a robust chipset that will support multiple bands. The

antenna design must also support the various frequency bands used with each of the network layers. Additionally, these devices typically must support additional wireless technologies such as Bluetooth, GPS, and WiFi.

In addition, accessing and roaming between the various network layers and the additional technologies typical in these devices will require a significant power source. A public safety officer typically carries a device on the uniform and another device in the vehicle. It is imperative that these devices support all network layers while maintaining the familiar "look and feel" of current mobile and portable devices, while also including a power source that will last typical shift durations, in order to conserve valuable space on the officer's belt and in the vehicle.

BayRICS supports this concept of a robust market for multi-band devices for public safety, but recommends that FirstNet conduct more research into the availability of such devices at a reasonable price, and ways to encourage device manufacturers to make multi-band devices more readily available to public safety users.

D. Add Specific Requirements to the Architecture Model to Ensure Adequate Regional and Local Control of Public Safety Services

BayRICS is concerned about the lack of attention in the FirstNet architecture presentation to the need for local public safety control over NPSBN network services. The vast majority of uses anticipated for the NPSBN will be in response to local incidents and by local public safety responders. Local jurisdictions must have direct control over many administrative functions of the NPSBN. Local jurisdictions are the most knowledgeable about their staff, their roles, responsibilities and assignments. Furthermore, they are more aware of internal policies and external relationships that can impact how a public safety user is deployed, managed, and reassigned during incidents. These functions should be reflected in network management and

operations during an incident, to ensure effective control over user setup, provisioning, and priority assignment according to the user's role, responsibility, rank, device/application access rights, skills and certification history.

Local law enforcement agencies are also concerned with the security of the NPSBN. As a requirement to use the network, agencies must demonstrate that they have complied with all Department of Justice requirements to secure the data traversing the network. Specifically in California, the California Law Enforcement Telecommunications System (CLETS) requires end to end encryption of data, and in many cases requires network improvements, sometimes at high costs to agencies, to ensure the data is secured across a trusted network. This network design is best implemented at a state or regional level, because of the specific security requirements of the particular jurisdiction.

Local jurisdictions also need control over certain network operational functions, especially when large scale or multiple incidents involving a wide range of resources, applications, and assets are competing for resources. To effectively manage complex response operations, local and regional entities must have "hands on the knobs" control to establish priorities for managing staff, devices, applications, and incident access/priority through the local RAN.

BayRICS believes that some measure of local control can be ensured through the technology ultimately deployed. As discussed above, deploying the EPC and Level One RAN as a private, mission critical network, leveraging local infrastructure where practical, and incorporating localized RSPG to maximize local control over user data traffic are fundamental requirements for the success of the network. In addition, FirstNet must encourage innovative

public-private partnerships that include state, regional, tribal and local participation. In the next section, we describe the BayWEB business model as an example of such a partnership.

IV. BUSINESS PLAN CONSIDERATIONS

Although FirstNet has not provided detailed information about proposed business models, the NOI seeks comments on business plan considerations. BayRICS encourages NTIA and FirstNet to conduct additional rounds of inquiry specifically seeking comments on relevant business models. We believe that many excellent examples of successful public-private partnerships and municipal networks are in operation today. These examples include both public safety networks and other municipal networks with innovative business plans. FirstNet will benefit from learning more about these models and incorporating the best elements of these projects into the NPSBN business model.

To that end, BayRICS provides information below about the BayWEB business model, which we believe provides many lessons learned and best practices that can inform and improve the FirstNet business plan. BayWEB was developed as a sustainable public-private model that is very similar to the anticipated FirstNet public-private partnership. The BayWEB business model and system funding plan are the result of over two years of exhaustive research into the specific roles, contributions and benefits flowing from a model based on public contribution of infrastructure and private management and operations.

We provide a high-level description below, and welcome the opportunity to provide FirstNet with more detailed information.

A. BayWEB Business Model Highlights

Bay Area Wireless Enhanced Broadband (BayWEB) is a public-private initiative to build and operate a wireless broadband network for use by San Francisco Bay Area public safety.

BayWEB is governed by BayRICS, a joint powers authority established in August 2011, comprised of representatives of seven Counties and three core cities making up the BayWEB geographic service area.

BayWEB is a three-way partnership between BayRICS, regional public safety agencies and Motorola Solutions, Inc. The unique public-private business model relies on contributions from each of the three partner entities:

- Motorola, using Broadband Technology Opportunity Program (BTOP) funding and matching funds, would build, operate and maintain the "middle mile" network, consisting of Evolved Packet Core (EPC), microwave backhaul network and eNodeB Radio Access Network (RAN).
- Local public safety agencies would contribute radio sites for the RAN and backhaul infrastructure (primarily dark fiber) through Site Use Agreements.
- BayRICS Authority would provide regional governance and oversight and will also be responsible for shared microwave and fiber backhaul, as well as specific "local control" functions (billing, subscriber provisioning, prioritization and certain training and support functions). These various responsibilities are defined in a master "Build, Own Operate and Maintain" (BOOM) Agreement with Motorola.

The operational funding plan assumes a "pass-through" model, in which all BayWEB billing, provisioning, and support costs would be passed on to user agencies as a surcharge added to the $38/subscriber/month base user fee paid to Motorola. The funding plan assumes an initial subscriber surcharge set at $5 per month. However, future system expansion, backhaul and system refresh costs may require increasing the surcharge to cover those costs in future years.

The BayWEB funding plan identified additional costs to members, and ways to mitigate those costs. For example, a member that contributes radio sites to the system will incur specified site costs. However, the Member may control those costs somewhat through the Site Use

Agreement. If, for example, the cost for a site is found to be excessive, the agency may choose to eliminate that site from consideration.

Another concern of members were the so-called "back office" connectivity costs, *i.e.* the cost of connecting the dispatch center or public safety answering point (PSAP) to the core. Such costs will vary from member to member, depending on the nature of the applications desired, the bandwidth required to operate those applications and the physical location of the facility to be connected. Individual Members that require a dedicated fiber or similar back office connectivity must estimate the costs to their agencies based on the circumstances of each individual facility. However, BayRICS has identified several less expensive alternatives that would allow smaller agencies to connect at much lower costs.

The BOOM Agreement with Motorola specifies that the Authority and its Members are not required to make minimum subscriber commitments. Therefore, if a Member has no users, it will incur no subscriber or device charges, and will not require back office connectivity or related costs. Most of the costs to Members will apply only to agencies that actually load users on the system. Other key provisions of the BOOM Agreement include:

- Motorola would operate the network for 10-years under the BOOM Agreement, and would then transfer the entire system to the BayRICS Authority at no cost.
- Motorola will execute site use agreements directly with site owning jurisdictions; jurisdictions will pay no costs related to site remediation. Jurisdictions must pay for site lease costs, utilities and staff time to provide access to the sites.
- Agencies have no obligation to purchase a minimum number of user accounts and Motorola assumes all risk of loading users on the system.
- Motorola will offer an introductory rate of $38/user/month for the first year of operation, and for subsequent years will maintain a rate that is driven from the commercial competitive market and is more affordable than rates for comparable services. BayRICS Authority will review rates annually.

- BayRICS will be responsible for all billing and collections, with start-up support from Motorola. BayRICS will add a service fee to user bills to cover its cost of operation.
- BayRICS will be responsible for backhaul connectivity to the BayWEB system core. Regional microwave radio sub-system will be used for backhaul where other options are not feasible.
- Member jurisdictions will contribute sites, dark fiber and will pay the costs of back office connections from agency enterprise networks to the core.
- Roaming:
    - Users will be responsible for roaming charges both inside and outside the BayWEB service area.
    - Motorola will provide reasonable technical assistance to the Authority concerning roaming services from that commercial carrier;
    - Users will be provided with a web-based application that will allow them to report system performance and coverage deficiencies on a real-time basis. Solutions to be considered will include: adding sites, enhancing backhaul, bi-directional amplification, device replacement or remediation, or roaming availability. BayRICS and Motorola will jointly agree on the cost-effectiveness of the solution.

B. BayWEB System Funding Plan Highlights

BayRICS developed a comprehensive Systems Funding Plan to capture all of the costs of BayWEB to participating member jurisdictions. This Section provides a high-level outline of the funding plan.[4]

The Plan identified and quantified the following categories of costs:

1. Costs to All BayRICS Members:
    a. Annual membership fee paid by members to the Authority;
    b. For Members negotiating Site Use Agreements, site costs related to lease payments, staff time for access by Motorola and electrical utility charges;
2. Costs to Members with System Users:
    a. Device costs;
    b. Member agency back office connectivity costs;
    c. User fees, paid directly to BayRICS, including:

[4] The full plan is available at http://www.bayrics.net/governance-documents.html.

i. User fees charged by Motorola;
ii. BayRICS Authority surcharge, which includes:
    1. Costs of billing user agencies on behalf of Motorola;
    2. Costs related to enhancing system coverage allocated to the Authority, including any roaming charges;
    3. Additional Administrative costs not covered by annual member fee

3. Costs to BayRICS not passed on to members (funded from other sources):
    a. Costs of increasing capacity and performance of the system allocated to the Authority, for example adding additional fiber to the backhaul system
    b. Any Backhaul Costs
    c. System refresh (year 10 and beyond)

V. APPLICATIONS DEVELOPMENT FOR PUBLIC SAFETY USERS

A. Applications for Public Safety

NTIA seeks input on the FirstNet Board's conceptual discussion of a potential framework for developing applications for public safety use. BayRICS and its member jurisdictions have conducted extensive research and planning for data applications anticipated to be available on BayWEB. We have also put considerable thought into the process for applications development. We believe that the public safety agencies and users of the system will be the best source of ideas for new applications, based on their experiences and needs in the field.

Anticipating the early deployment of the BayWEB project, Bay Area public safety officials have developed detailed service and application requirements based on current and future needs. Although the "killer app" most often mentioned involves streaming video, in reality, the most valuable and beneficial applications will likely be those that can effectively utilize "mashups" or integrated data from multiple data sets to provide detailed, real-time intelligence to first responders.

For illustration, BayRICS provides the following Table 1, describing some of the potential applications that can be highly useful to our first responders. It is important to note

that, to be effective, applications require a source of reliable data sets. A well designed application will be useless if it does not interface with relevant, accurate and up-to-date data. We have included information on specific data required for each application in Table 1.

Table 1: Public Safety Agency Applications

Public Safety Agency	Data	Application/Interface
General/ Emergency Management	• GIS: True standard-based GIS data layers with the same attribute and coding standard nation-wide so all PS staff can use without localized training • Support Pictometry based mapping	**Application** • Regional Real Time Incident Management System • Regional CAD: Supports single agency, multi-agency, multi-site or co-dispatch configurations • Standardized and streamlined work flow process management for PS personnel • Regional Enterprise Asset Management (EAM) system • Instantly collects and displays all address and name information to dispatcher and mobile user • Emergency Response Training System (for all participants, including procedure, process, protocol) **Interface** • Interface to 311 information systems • Interface to Human Resources Databases • Interface to WebEOC (Emergency Operation Center) Management
Police	• Citizen database • DMV database • Crime database • Cable data	**Application** • Wireless applications including VPN access, access to secure Intranet • Level II Mobile Data Client (for CLETS / CABLE and RMS Data) • Automated Biometric Information System (ABIS) for field identification, • Shotspotter • Compstat/dashboard type data access (for Incidents, Calls for Service, and Warrant Information) • CalPhoto and Mugshot database access • Capture and save photos from the street and share on the network • Direct call creation for traffic stops and/or officer initiated activity • Integrated messaging capabilities, mobile to mobile, mobile to dispatch or mobile to terminal • One-of-a-kind integrated in-car digital video allows officers to view live streaming video from other squads or fixed camera positions • Online regulation document access **Interface** • Access to Record management system (RMS) • Integrated AVL, mapping and automatic routing information • Access to premise history, name history, and address flag information • Integrated field reporting allows report entry directly into RMS

Public Safety Agency	Data	Application/Interface
Police (cont.)		from the mobile PC • Ability to access Citizen database • Ability to access DMV data
Fire	• Fire Hydrant layer including test record • Fire Station layer • HazMat database • Gas Line Layer • Property data layer • Inspection Data	**Application** • Online training system • ePCR – Electronic Patient Care Report (ambulance to hospital) • HazMat tracking system • Inspections, violation tracking and re-inspection reminders • Personnel Module – personal information, training records and scheduling • Arson investigations – reporting, documentation and tracking • Screen designed to reduce eyestrain and support for Multi-Monitor • SOP, address flag and HazMat flag information attached to call • Self-initiated call creation for fire personnel and inspectors • Fully supports volunteer department protocols • Automatic SOP, address flags and HazMat alerts **Interface** • Fully integrated with CAD and RMS systems with mobile device • Access to EMS and daily activities • Integrated video streaming from squad cars or surveillance cameras • Integrated AVL and call routing information as standard features • Interface to all complete premise history details automatically generated during call transmission • Building/floor plan download capability • Interactive access to the NIOSH, DOT and HazMat Guides etc. • Pre-programmed hospital locations for en route use • "Rip and Run" information displayed upon dispatch
MTA (Municipal Transportation Authority)	• Stop layer • Route layer • Bus Shelter layer • AVL with prediction • Traffic Signal layer • Parking meter layer	**Application** **Interface** • Ability to access to MTA's scheduling and dispatch system • Ability to access to Traffic Sign Control System, The Network can be used as Traffic Signal Priority backhaul forsharing live intersection video • Ability to interface to MTA's Central Control system • Ability to access to MTA's Automated Train Control System • Ability to access to MTA's Nextbus system • Interface to MTA's Radio system • Ability to interface with MTA's 511 system • Ability to interface with MTA's SFPark system • Ability to interface with MTA's Signal Control System • Ability to interface with MTA's onboard video systems to stream images dynamically from the mobile fleet • Ability to interface with MTA's real-time Fare Collection System that integrates to onboard fare boxes within MTA vehicles

Public Safety Agency	Data	Application/Interface
DPH (Public Health)	• Hospital location layer	**Application** **Interface** • Interface to Hospital database • Interface to public Health Care database for paramedic
PUC (Water Dept.)	• Master Hydrant layer	**Application** • Wireless applications including Master to Remote and Remote to Remote SCADA Ethernet Communications **Interface** • Ability to access utility database • Ability to access hydrant database • Interface to PUC scheduling and dispatch system
Dept. of Technology (DT)	• Master GIS layers • Master address and name database • City's Fiber and Network connectivity data	**Application** • Wireless Call Boxes and general Internet/VPN access in the field for City Departments **Interface** • Interface to DT's Email/Office Applications • Ability to Interface to DT's Email/Office Applications • Ability to interface with DT's Master GIS database and aeraphot database
DPW (Public Works)		**Application** **Interface** • Ability to Interface to DPW's CMMS/EAM Application
General Public / Citizen/ Traveler		**Application** • Life-saving access to emergency medical information for first responders • Allows your business community the opportunity to create and update their own business contact templates. Self-entry saves hundreds of hours of agency time and eliminates cumbersome index cards • Participants can update their premise, personal contact, medical and key holder information ensuring accurate records • Integrates IP-based camera feeds into CAD

B. Leverage the Early Builder Networks as Test Beds and Incubators for New Public Safety Applications

BayRICS agrees with the FirstNet Board that innovation in wireless data applications for public safety should mirror the commercial wireless market. As Board Member F. Craig Farrill stated at the September 25 FirstNet meeting, "many of us have seen the explosion of applications on devices . . . that has not been something that the public safety community could see. We'd like to unlock that door and open up a flood of applications to the public safety community . . ."[5]

At the same meeting, Chairman Samuel Ginn described an innovative process for application development: "we're going to invite the world to help us develop apps for public safety employees . . . We're going to call together outside developers in a conference and we're going to say, 'Here are the interface standards, here's what you need to get certified to be on our system. Now, go talk to your local public safety people and see if you can develop an application which solves their problem' . . . so we'll be looking for innovators out there around the country, people who pick up on this capability, run with it, develop programs that go into the system."[6]

BayRICS is uniquely positioned to leverage the BayWEB project to draw on communities of applications developers in the Bay Area. Relying on the concentration of developers in Silicon Valley, San Francisco South of Market (SOMA) and the research universities located in the Bay Area, we always anticipated the BayWEB network to be a test bed for public safety application development.

In fact, Bay Area cities and counties have been active in encouraging applications development through partnerships with organizations like the San Francisco Citizens Initiative for Technology and Innovation (www.sfciti.com) and other application development events. As

[5] See, FirstNet Board Meeting, September 25, 2012, transcript, at 32.
[6] See, FirstNet Board Meeting, September 25, 2012, transcript at 52.

a specific example, the San Francisco Police Department ("SFPD") has partnered with Hewlett Packard and ArcTouch, both local Bay Area companies, to develop a mobile field-based reporting application.[7] This will not only improve the efficiency of SFPD resources, but truly make SFPD paperless citywide.

As discussed earlier, network security is critical for this nationwide network. Fortunately, LTE technology and carefully designed security policies can provide the necessary safeguards to allow the developer community limited access to build and test innovative applications, while being effectively firewalled from public safety network traffic. Access rights can be configured to allow test-bed capacity and priority-preemption rules can provide developers with secondary user rights that can be reduced or preempted during times when capacity is needed for live incident response. Practice data sets can be provided in simulated environment that would allow a wide range of applications testing without causing security concerns or interference issues with public safety users. Strong encryption standards can provide added layers of protection for sensitive public safety data traffic on the network.

The "walled garden" we envision may not be practical on the fully functional nationwide network when it is deployed. However, early build networks could be initially configured in ways that would accommodate simulated testing and limited access. LTE technology could potentially limit access to this test environment to qualified users in geographic areas surrounding research universities or communities with a large developer workforce.

In the Bay Area, the BayWEB project can draw on the brainpower in our region and the resources available to FirstNet to develop an effective test environment for new applications in

[7] See, San Francisco Mayor Ed Lee News Release, "New Mobile Application for Police in the Field," June 27, 2012 (http://www.sfmayor.org/index.aspx?recordid=6&page=846).

the Bay Area. We urge FirstNet to allow early build projects such as BayWEB to continue as soon as possible, to allow these types of test environments to evolve, given the tremendous value they may have for public safety applications development.