



**Joseph P. Marx**  
Assistant Vice President  
Federal Regulatory  
1120 20<sup>th</sup> Street, N.W., Suite 1000  
Washington, DC 20036

T: 202-457-2107  
F: 202-289-3699

December 18, 2009

Marlene Dortch  
Secretary  
Federal Communications Commission  
445 12 Street S.W.  
Washington, D.C. 20554

**Re: In the Matter of Implementation of Smart Grid Technology, GN Docket Nos. 09-47, 09-51, 09-137**

Dear Ms Dortch:

I write to provide certain materials as a follow-up to a meeting AT&T had with Nick Sinai and Charles Worthington on October 29, 2009, in which we discussed matters relating to Smart Grid technology, as they related to the Commission's National Broadband Plan.

During the meeting, we spoke briefly about the regulatory accounting requirements to which electric utilities are generally subject and the incentives that they may create for a utility choosing among different Smart Grid communications architectures. Specifically, we discussed how pressure may exist to build a capital-intensive, single-purpose communications network, rather than contracting for services with a commercial wireless provider. I have attached a short discussion of this issue, which includes suggested accounting policy changes that might help to neutralize some of the incentives that may exist to choose less efficient communications architectures.

During our meeting, we also discussed security concerns relating to Smart Grid communications service. I have attached a white paper that discusses the wide range of security measures that AT&T has implemented to protect its data networks. These measures benefit Smart Grid subscribers, as well as AT&T's other customers.

Finally, we discussed the possibilities for public-private partnerships in connection with wireless broadband networks. During that conversation, we spoke about the Request for Information that local governments surrounding San Francisco Bay had recently issued seeking proposals for a broadband network that leveraged both public and private facilities. For your information, I have attached a copy of that document as well.

Please feel free to contact me if there is any additional information that would be useful to your work on these issues.

Sincerely,

/s/ Joseph P. Marx

cc: Nick Sinai  
Charles Worthington

Enclosures

# North American Electric Reliability Corporation (NERC) – Critical Infrastructure Protection (CIP)

Utilities Facing Many Challenges: Cyber Security is One Area Where Help is Available

Art Maria, Solutions Engineering and Architecture, AT&T  
Warren Causey, Sierra Energy Group

---

## Executive Summary

*Utilities are in the crosshairs of many forces in the world today. Among these are environmental global warming concerns putting pressure on the ability to generate sufficient electricity to meet future demand. Another is the multiplicity of computer and communications systems that must be protected against threats from those who would do harm to electric, natural gas and water distribution systems.*

*A Wall Street Journal article<sup>1</sup> in April 2009 focused attention on the security issue by quoting various federal officials who claimed many utilities already had been breached – especially by spies from hostile countries – with bits of code left behind that could be activated in time of war or for other reasons to bring down major portions of the U.S. electric grid.*



---

## Summary continued

*However, utilities long have been aware of these issues, and many report 10,000 or more attempted network security breaches per month, and have done so for years, according to research from Sierra Energy Group (SEG), the research and analysis division of Energy Central.*

*In the aftermath of the 9/11 terrorist attacks on the U.S. the federal government moved to ensure utilities take all necessary measures to mitigate these attacks. Through the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corp. (NERC) the government issued a set of standards and requirements to ensure this mitigation. These standards and requirements are called NERC-CIP (CIP=Critical Infrastructure Protection). These mostly have been developed by private enterprise through vendors and other organizations.*

*Telecommunications carriers such as AT&T have addressed cyber security longer than most utilities because of the public nature of their communications systems. On the average business day, AT&T transports approximately 17 petabytes of data on its network. As a result, AT&T has gained significant knowledge and experience in regard to security architectures and encryption methodologies.*

---

## Utilities in the Crosshairs

The U.S. utility is challenged as never before in history. The challenges are myriad: from generation capacity constraints and declining capacity margins to environmental global warming remediation demands, to economic conditions, to cyber and physical security concerns. The April 2009 Wall Street Journal story referenced earlier brought additional attention to a security issue utilities have been aware of, and attempted to mitigate for years.

Before the Wall Street Journal article brought the issue to widespread public attention utilities knew they were under attack. SEG is aware that utilities have quietly collaborated with the FBI, various national laboratories, vendors, the Department of Homeland Security and others to mitigate these on-going attacks. What was different about the Wall Street Journal article was the claim by various government officials that some of these attacks have been successful and that cyber spies from hostile countries have been mapping the U.S. electrical grid, and leaving behind bits of sleeper code that could be activated and used to damage the grid or cause blackouts in the event of war.<sup>2</sup>

For several years it has been general knowledge that cyber spies have been disrupting utility systems and causing blackouts in Eastern Europe and around the globe; sometimes even demanding ransom money to cease the attacks. Electric, water and wastewater utilities in several countries have been affected according to SEG. Thus far, no similar attacks have been publicly acknowledged<sup>3</sup> in the U.S., but the Journal article pointed to the likelihood that such attacks may be inevitable and may have even already occurred.

## Attack Vectors

The widespread use of the Internet as a communications mechanism is a major driver for increased cyber attacks, but the problems go much deeper. Since the 1980s utilities increasingly have been using computerized communications systems and networks, primarily SCADA (Supervisory Control and Data Acquisition) and DA (Distribution Automation), to communicate with and control many remote devices on electrical grids and both natural gas and water distribution systems. Many of the early SCADA and DA systems that are still in service today were built with early technologies that are relatively easy for sophisticated hackers with modern tools to breach and manipulate. Recent technology trends have emphasized the “networking” of all utility computers and control systems for efficiency and collaboration. As more networks are linked, the pathways for cyber spies become myriad and the means of protecting such networks becomes increasingly difficult to maintain. There now are a large number of cyber pathways at most utilities and a determined hacker – particularly one backed by a less-than-benign government – likely will find one.

Furthermore, prior to the September 11, 2001 terrorist attacks there really was not a systematic security approach to address utility critical infrastructure protection in the United States. Each utility was essentially on its own, and security of computer systems and even physical security at plants, substations and other facilities were the responsibility of individual utilities without any oversight. This created a significant risk in that there are more than 3,000 electric and natural gas utilities and approximately 15,000 water distribution utilities in the U.S. Before the terrorist attacks there were many different approaches to cyber and physical security.

## Critical Infrastructure Protection

In 2008, FERC approved eight new CIP reliability standards designed to protect the nation’s bulk power system against potential disruptions from cyber security breaches. These standards were developed by the NERC and provide a cyber security framework for the identification and protection of Critical Cyber Assets.

The eight Cyber security standards address the following:

- Critical Cyber Asset Identification
- Security Management Controls
- Personnel and Training
- Electronic Security Perimeters
- Physical Security of Critical Cyber Assets
- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plans for Critical Cyber Assets

As mentioned NERC-CIP is a framework to help address security of our national utility systems, but there is still much work to do. For example, there have been cases where security updates have not been installed on assets, and unfortunately many “patches” are only issued after a hacker or cyber spy already has found and taken advantage of a security flaw. Multiply potential flaws by the number of utilities and again by the number of utility networks and you can begin to understand the cyber-security challenges around securing utility networks.

AT&T has invested significant resources in developing cyber security systems for its networks, and thus has significant expertise that utilities may find helpful in addressing their own security needs.

For AT&T cyber security is the collective set of services, procedures and practices. These capabilities assure the information, applications and services AT&T's customers want and use are secure, accurate, reliable and available wherever and whenever they are needed. Cyber security is a corporate priority and AT&T is investing significant resources in making its network and customers' information secure.

Cyber security capabilities include understanding and identifying emerging threats in early phases of their development. Network exploits, malware, flooding attacks, protocol anomalies and other threats are generally visible and often abundant on the Internet long before they have any significant affect on enterprise security.

AT&T is uniquely established to understand and deal with cyber threat. These include:

- Operating as the largest provider of Internet services
- Operation of a global IP network footprint
- An Internet data analysis platform that examines internet threats including botnets, network worms, DoS attacks, network exploits and other activity anomalies
- An analysis team that operates 24x7 to assess any significant activities on the Internet that could affect network services
- An algorithm research team that continually investigates and tests methods for automated detection of network threats
- AT&T Labs and Chief Security Office researchers, who participate in the security and networking research communities

The technology within AT&T's network is rapidly evolving to support new applications and services. In the course of 2009 alone, AT&T expects to invest \$17-18 billion in expanding the capabilities of its network and infrastructure to meet the rapid global expansion of advanced information technology and services to enhance reliability and security. The size and scope of AT&T's global network, coupled with AT&T's industry-leading cyber-security capabilities, gives it a unique perspective into malicious cyber-activity.

AT&T's advanced network technology currently transports on average more than 17 Petabytes each business day of IP data traffic and the load is expected to double every 18 months for the foreseeable future. AT&T's network technologies give the company the capability to analyze traffic flows to detect malicious cyber-activities, and in many cases get very early indicators of attacks before they have the opportunity to become major events. For example, AT&T implemented the capability within its network to automatically detect and mitigate most Distributed Denial of Service Attacks within the AT&T network infrastructure before they affect service to AT&T customers. AT&T has grown from one domestic scrubbing complex to multiple locations across the United States, as well as having scrubbing nodes in Europe and Asia. This gives the AT&T the ability to filter attack traffic as close to the source of the threat as possible.

AT&T has made significant investments in the security of its mobility network. AT&T's Radio Access Network (RAN) complies with 3GPP airlink security standards. The RAN uses secure protocols in order to maintain and manage communication with the mobile station as well as specific procedures including power control and handover management. An important security mechanism that protects the radio link against eavesdropping is encryption. Encryption protects both user data and network control information and occurs between the cellular towers and the wireless device.

Following authentication and key agreement the network and end user equipment uses a 128-bit key and strong encryption algorithms. Significant resources have also been invested in the AT&T core mobility and wide area network in order to comply with and exceed industry security standards.

### **Cyber Security Assets**

AT&T is responsible for managing the security of a worldwide data network, which consists of multiple components converging into a common Multi-Protocol Label Switching (MPLS) network. In order to support these objectives, AT&T maintains a comprehensive global security organization comprised of over 700 security professionals. This organization is dedicated to the physical and logical security of the AT&T global network and its service offerings. It supports a broad range of functions from security policy management to customer-facing security solutions. The AT&T global security organization reviews and assesses AT&T's security control posture to keep pace with industry security developments and to satisfy regulatory and business requirements. AT&T actively participates in a number of global security organizations, and maintains a comprehensive set of security standards based in part on similar leading industry standards (COBIT, ISO/IEC 27001:2005, etc.). Given the dynamic environment that AT&T supports, the library of AT&T security standards is continually re-evaluated and modified as industry standards evolve and as circumstances require. In addition, AT&T supports the following programs.

#### **Confidentiality**

To ensure confidentiality, information is accessible only to those authorized. AT&T has implemented a three-tiered Information Classification framework for categorizing information based on sensitivity of the content and specific legal requirements.

#### **Physical Access Control Requirements**

AT&T operates in a highly secured environment where physical access to staff office space, switching centers, global network and service management centers and other network facilities is strictly monitored and controlled.

#### **Network Element Access Controls**

Access is provided to AT&T technical support personnel only on an as-needed basis for individuals with responsibility for network element maintenance and support.

#### **Network Perimeter Protection**

AT&T external network connections are protected by firewalls that screen incoming and outgoing traffic based on source and destination address, protocol and port, in accordance with the security policy.

### Intrusion Detection

AT&T employs a combination of internally developed and commercial tools to detect attempts by unauthorized persons to penetrate AT&T Global Network. AT&T does not monitor individual customer connections for intrusions, except when part of a managed security service.

### Workstation Security Management

Workstation security policies protect AT&T and customer assets through a series of processes and technologies including verification of personnel workstation accesses, PC anti-virus protection, operating system hardening and updates, full disk encryption where permitted by law to protect sensitive information on portable assets, along with a personal firewall intrinsic to remote access software implemented on workstations or portable PCs that remotely connect to the AT&T network.

### Security Status Checking and Vulnerability Testing

AT&T conducts regular tests and evaluations to ensure that security controls are maintained and are functioning in accordance with policy. These initiatives include Security Status Checking and Vulnerability Testing, Security Incident Reporting and Management. AT&T uses a consistent, disciplined global process for the identification of security incidents and threats in a timely manner, to minimize the loss or compromise of information assets belonging to both AT&T and its customers and, to facilitate incident resolution.

### Business Continuity and Disaster Recovery

AT&T Corporate Business Continuity Planning Services provides technical consultation and program management expertise to address the business continuity, disaster recovery and managed security needs of AT&T and its customers.

### Security Products and Services

AT&T offers managed security products and services to its customers designed to assess and protect their vital network infrastructure, including managed services in the area of Intrusion Detection, Firewall Security, Endpoint Security, Token Authentication, Encryption Services, Security Email Gateway Services, Vulnerability Scanning and Consultative and Engineering Security Services.

### Managed Services and Hosting

AT&T Managed Services take advantage of the security of AT&T's global Internet Protocol/Multi Protocol Label Switching (IP/MPLS) network. MPLS technology enables the creation of feature-rich network-based services coupled with AT&T's management expertise, tools and automation. AT&T's network-based managed services include Enhanced Virtual Private Network and Managed Internet Services.

### Hosting Services

Hosting services provide utility computing services that offer tailored or turnkey solutions. The mix-and-match tailored solutions offer IT infrastructure, hardware and/or software components, reliable and secure data center facilities, value-added services (i.e., security, backup and restore, professional services, monitoring, portal/reporting, utility and disaster recovery), server virtualization and integrated client networking. A fully managed turnkey solution provides capacity on demand, managed firewall and network Intrusion Detection System (IDS) functionality, proactive alerting and patching dedicated virtual servers and, total isolation of each client's data in a data center environment.

AT&T has implemented in-depth access control layers with multiple levels of firewalls that isolate core network element functions from customer-facing interfaces. These security perimeters enable AT&T to offer voice and data interfaces to its customers while helping to preserve the integrity of its core network resources. AT&T offers a Commercial Connectivity Services (CCS) solution which allows utilities to define transport network paths for data delivery. This enables utilities to transport data from the Advanced Metering Infrastructure (AMI) to core IT infrastructure using authorized and encrypted capabilities.

CCS implements custom Access Point Names (APNs) that provide linkage from the wireless network to the utility's core IT infrastructure using either frame relay circuits or MPLS connectivity. AT&T also offers Enterprise on Demand (EOD), which enables customers to selectively activate and deactivate devices (SIMs) on a real-time basis. These capabilities involve multiple levels of security, access controls and encryption that many electric, natural gas and water utilities will find beneficial.

In addition to CCS and EOD, AT&T offers a suite of Security and Business Continuity Services that will assess vulnerabilities, secure data and infrastructure, detect attacks, respond to suspicious activities and provide for non-stop operations.

AT&T stands ready to work with utilities and bring its extensive experience and capabilities in cyber security to the many challenges ahead.

1. Electricity Grid in U.S. Penetrated by Spies by Siobhan Gorman, Wall Street Journal, April 8, 2009.

2. Ibid

3. Ibid

**For more information contact an AT&T Representative or visit [www.att.com/business](http://www.att.com/business).**



**at&t**

Your world. Delivered.

# **San Francisco Bay Area**

Request for Information (RFI) 2009-DEM01

**for a**

**Regional 700MHz Wireless Mobile Broadband Network**

**Issue Date: September 29<sup>th</sup>, 2009**  
**Response Due: November 16<sup>th</sup>, 2009**

**Pre-Proposal Conference**  
**Wednesday, October 21st at 1:30pm**  
**Alameda County Emergency Operations Center**  
**4985 Broder Blvd, Dublin CA**

# TABLE OF CONTENTS

<b>I.</b>	<b>Introduction.....</b>	<b>1</b>
<b>II.</b>	<b>Project Approach.....</b>	<b>1</b>
A.	Project Background.....	1
B.	Technology Approach.....	3
<b>III.</b>	<b>System requirements for the Broadband network.....</b>	<b>3</b>
A.	Coverage Requirements.....	3
B.	Interference Mitigation.....	5
C.	Network Capacity and Throughput.....	5
D.	Mobility and Handoff.....	6
E.	Roaming.....	7
F.	Network Reliability, Availability and Hardening.....	7
G.	Network Security.....	7
H.	Network Priorities.....	8
I.	Network Compatibility and Interfaces.....	8
J.	Network Administrative and Operational Capabilities.....	8
K.	Device Requirements.....	9
L.	Technical Applications and Use Case Scenarios.....	10
<b>IV.</b>	<b>Preparing a Response.....</b>	<b>13</b>
<b>V.</b>	<b>Submittal Instructions.....</b>	<b>17</b>
<b>VI.</b>	<b>Riders.....</b>	<b>19</b>
<b>VII.</b>	<b>Public Records Act/Sunshine Ordinance.....</b>	<b>19</b>
	<b>APPENDIX A– PILOT PROJECTS.....</b>	<b>21</b>
A.	San Francisco.....	21
B.	Oakland.....	23
C.	San Jose.....	25
	<b>APPENDIX B – Potential Radio Sites.....</b>	<b>26</b>

## I. INTRODUCTION

On behalf of the San Francisco Bay Area Region, the City and County of San Francisco, the City of Oakland and the City of San Jose (“Bay Area”) are requesting expressions of interest and information (“RFI”) from commercial vendors, systems integrators, service providers, and/or other interested parties (“Respondents”) for the deployment of a Regional 700MHz Wireless Mobile Broadband Network (“Broadband Network”). The Bay Area welcomes information and comment from both interested parties as well as organizations with a commercial interest in the project. The intention of the RFI is to assess potential approaches and the costs associated with the deployment of a region-wide 700MHz broadband network. Based on the review of RFI responses, the Bay Area will consider pilot projects in the Cities of San Jose, San Francisco, and Oakland, beginning in 2010.

This RFI does not attempt to describe all intricacies, functions and system architecture of the Broadband Network. Instead the RFI asks for information in a format that organizes the responses for potential analysis, while allowing Respondents flexibility in describing their solutions’ benefits, capabilities, functionality, and service offerings.

Respondents may respond to any combination of the overall scope of the project, but the Bay Area seeks a comprehensive response to all of the questions posed within the RFI. The Bay Area will not award a long term contract based on this RFI; however, the Cities of San Jose, Oakland and San Francisco may enter into a two year pilot project based on the responses received to this RFI. Please see Sections IV and V of this document for details about preparing and submitting a response.

## II. PROJECT APPROACH

### A. Project Background

In 2007, the Bay Area embarked on a regional interoperability program known as Bay Area Regional Interoperable Communications System (BayRICS). The program intends to improve interoperable communications, both voice and broadband data capabilities, throughout the 10 counties which comprise the Bay Area Urban Area Security Initiative (UASI). This includes the counties of Alameda, Contra Costa, Marin, Napa, San Francisco, San Mateo, Santa Clara, Santa Cruz, Solano, and Sonoma, as well as the cities, townships, special districts, and incorporated areas within (“Region”).

The program lays out a framework to construct a Project 25 Voice (Land Mobile) Radio Network throughout the Region, utilizing 700MHz/800MHz frequencies as well as VHF frequencies for rural operations. The program takes a multi-jurisdiction and multi-disciplinary approach to interoperability, and includes communications capabilities for First Responders and Public Safety professionals, as well as all other government services including public works, transportation agencies, and critical infrastructure organizations.

The Region has invested millions of dollars on site development, microwave backhaul improvements, backbone fiber optics and cable pathways, core networking equipment, and hiring personnel to manage system implementation. It is the intention that the Broadband Network would take advantage and build upon these investments in a *leveraged network model*<sup>1</sup> for construction and deployment. Through this RFI, the Bay Area seeks comment on this approach

---

<sup>1</sup> A leveraged network model assumes the Respondents will consider the assets currently deployed within the participating jurisdictions owned both commercially and governmentally.

as well as business and cost models required to deploy and sustain the network throughout the Region.

To provide interoperability, the Region seeks to deploy a system that is compatible and interoperable with the Shared Wireless Broadband Network (SWBN)<sup>2</sup> as proposed by the Federal Communications Commission (FCC). As such, Respondents should propose solutions for the Broadband Network that incorporate the Technical, Operational and Governance requirements as outlined by the National Public Safety Telecommunications Council (NPSTC), Broadband Task Force. Specifically in terms of governance, the Bay Area assumes the Broadband Network will be deployed under a *de facto* lease agreement with the Public Safety Broadband Licensee (PSBL) as outline in the NPSTC 700MHz Public Safety Broadband Task Force Report and Recommendations (NPSTC Report). In terms of technical and operational needs, these requirements can also be found in the NPSTC Report and further technical and operational requirements for the Bay Area's Broadband Network are outlined in Section III.

The Broadband Network shall use the 10 MHz of spectrum (763-768/793-798 MHz) (Public Safety Spectrum) assigned for public safety broadband use. The Bay Area has applied for a waiver to enable the Region to begin planning and implementation of the Broadband Network and to begin providing service within two years of obtaining the waiver. Respondents should assume the Bay Area waiver will be approved in accordance with the timelines discussed within the RFI. It is also the intent of the Bay Area to use the Broadband Network not only to meet the ever increasing requirements of public safety first responder data operations, but also to integrate other government service resources as appropriate to provide intra-agency interoperability that is paramount to sustaining public confidence and quick recovery during a time of crisis.<sup>3</sup>

The Bay Area is requesting information from Respondents on a project and/or service offering approach for the possible implementation of the network. The anticipated phases for the program are the following:

- Phase 1 - First deployments in limited area within the Cities of San Francisco, Oakland, and San Jose. Timeline for implementation begins in Q1 2010 with application trials beginning late-2010.
- Phase 2 – Citywide deployments for San Francisco, Oakland and San Jose. Provide initial deployments/service offerings within Marin, Santa Clara, San Mateo, Contra Costa and Alameda Counties.
- Phase 3 – Provide countywide deployments/service offerings to include Marin, Santa Clara, San Mateo, Contra Costa and Alameda Counties. Provide initial deployments/service offerings within Napa and Sonoma Counties.
- Phase 4 – Provide countywide deployments/service offerings include Napa, Sonoma, Solano and Santa Cruz Counties.

As the Broadband Network is constructed in this phased approach, the infrastructure must remain backwards compatible with the equipment and devices deployed in the earlier phases. Respondents should consider these anticipated phases in developing the cost and business models for the system deployment. It is the Bay Area's vision to have wireless broadband coverage throughout the Region by 2015.

---

<sup>2</sup> Recently, the National Public Safety Telecommunications Council re-termed this network the Nationwide Broadband Data System (NBDS); as such these terms may be interchangeable in the RFI and in the RFI responses.

<sup>3</sup> Request for Waiver, PS Docket No. 06-229

## **B. Technology Approach**

The Bay Area would like Respondents to outline the technology approach that they believe will provide the highest level of interoperability throughout the Region, and can be deployed in a cost effective manner for government entities.

The Bay Area realizes that broadband network technologies are still evolving and there are competing standards available throughout the market space. Several of the major Public Safety Agencies, including the National Public Safety Telecommunications Council, Association of Public Safety Communications Officials, and National Emergency Number Association have recently endorsed Long Term Evolution (LTE) as the broadband technology standard for the SWBN and Bay Area seeks a solution that will utilize the LTE standard.

## **III. SYSTEM REQUIREMENTS FOR THE BROADBAND NETWORK**

The following subsections outline the overall system requirements for the Broadband Network. It is expected that Respondents address each of the subsections with their methodologies on how they will meet and/or provide the requirements outlined.

### **A. Coverage Requirements**

The Bay Area seeks comment on how the Respondents will offer coverage throughout the Region. The following table outlines the anticipated coverage requirements for the Region based on each phase of the system deployment. In terms of designing the system for coverage versus capacity, the Bay Area prefers that the Broadband Network provides adequate coverage at the onset of the network. It is assumed that additional sites can and will be added, in subsequent phases, to address capacity and throughput issues that may arise once more bandwidth intensive applications are added to the system.

The Broadband Network should be designed to meet 95% coverage probability on all named streets within the service area (not including in-building coverage). The service area is defined geographically, by the county boundaries. These coverage needs should be used as guidelines for developing a phased approach to system deployment and/or service offerings. There are three types of coverage outlined within the table, which are as follows:

- Mobile Coverage – Assumes a dongle-type device (I.e. USB modem interfaced to a vehicle mounted computer) located inside a vehicle, with no external antenna, providing coverage on the street
- Portable Coverage – Assumes a handheld device, mounted on the hip, providing on street coverage
- In-Building Coverage- Assumes 1<sup>st</sup> wall penetration of buildings using a handheld device and/or a dongle device within a computer. Also assumes coverage in tunnels and underground.

	Dense Urban*	Urban*	Suburban*	Rural*
Phase 1^				
San Francisco (City/County)	Mobile Coverage	Mobile Coverage	Mobile Coverage	N/A
Oakland - Downtown	Portable Coverage	Portable Coverage	Mobile Coverage	N/A
San Jose	Mobile Coverage	Mobile Coverage	Mobile Coverage	N/A
Phase 2^				
San Francisco (City/County)	Portable, In-building Coverage	Portable, In-building Coverage	Portable, In-building Coverage	N/A
Oakland – Entire City	Portable, In-Building Coverage	Portable, In-Building Coverage	Portable, In-Building Coverage	Mobile Coverage
San Jose	Portable, In-building Coverage	Portable, In-building Coverage	Portable, In-building Coverage	Mobile Coverage
San Mateo County	N/A	Mobile Coverage	Mobile Coverage	Mobile Coverage
Santa Clara County	N/A	Mobile Coverage	Mobile Coverage	Mobile Coverage
Alameda County	Mobile Coverage	Mobile Coverage	Mobile Coverage	Mobile Coverage
Contra Costa County	N/A	Mobile Coverage	N/A	N/A
Marin County	N/A	Mobile Coverage	Mobile Coverage	N/A
Phase 3^				
Alameda County	Portable, In-Building Coverage	Portable, In-Building Coverage	Portable, In-Building Coverage	Mobile Coverage
Contra Costa County	N/A	Portable, In-building Coverage	Portable, In-building Coverage	Mobile Coverage
Marin County	N/A	Mobile Coverage	Mobile Coverage	Mobile Coverage
San Mateo County	N/A	Portable, In-building Coverage	Portable, In-building Coverage	Mobile Coverage
Santa Clara County	N/A	Portable, In-building Coverage	Portable, In-building Coverage	Mobile Coverage
Napa County	N/A	N/A	Mobile, On Street	Mobile, On Street
Sonoma County	N/A	N/A	Mobile, On Street	Mobile, On Street
Solano County <sup>+</sup>	N/A	N/A	Mobile, On Street	Mobile, On Street
Santa Cruz County <sup>+</sup>	N/A	N/A	Mobile, On Street	Mobile, On Street
Phase 4^				

Marin County	N/A	Portable, In-building Coverage	Portable, In-building Coverage	Mobile Coverage
Napa County	N/A	N/A	Portable, In-building Coverage	Mobile, On Street
Sonoma County	N/A	N/A	Portable, In-building Coverage	Mobile, On Street
Solano County <sup>+</sup>	N/A	N/A	Portable, In-building Coverage	Mobile, On Street
Santa Cruz County <sup>+</sup>	N/A	N/A	Portable, In-building Coverage	Mobile, On Street

\*Morphologies based on population are defined in the National Public Safety Telecommunication Counsel, Statement of Requirements Document, Section 5.1

^Project phases are not necessarily sequential. Populous areas within the counties listed in Phases 3 and 4 may be built out early based on need and/or funding availability.

<sup>+</sup>Coverage Requirements are assumptions and may change after receiving RFI responses

Respondents should consider these coverage requirements, as well as the potential sites listed in Appendix B, and any other sites that Respondents can leverage, as a baseline for developing the system architecture and associated costs. Respondents should use a leveraged network model, where available, to minimize the cost of infrastructure.

Respondents should discuss how in-building coverage is provided.

Coverage maps should be provided for each Phase. It is recommended that the maps be shown per geographic (County) area to give the best detail possible. Coverage maps should be accompanied with information giving site locations, the coverage assumptions, link budget analysis, and all parameters used in developing the coverage predictions. Throughput assumptions should also be described.

## **B. Interference Mitigation**

The Broadband Network should employ interference mitigation techniques that will avoid signal/throughput degradation issues between overlapping coverage areas. This may include coverage within the Region's Broadband Network, as well as coverage implemented by a neighboring network or SWBN. Respondents should describe how these techniques are implemented within the network infrastructure and/or equipment. Any mitigation features that are unique to a Respondent's proposed technology, that improve interference mitigation capability, should be described.

## **C. Network Capacity and Throughput**

The Broadband Network shall meet the throughput levels defined by the LTE standard. Respondents should discuss how their network, and the proposed system, is designed to support these throughput levels, which should be given in terms of:

- Maximum theoretical and average throughput<sup>4</sup> (assuming 70% loading) per sector (both uplink and downlink)
- Maximum theoretical and average throughput (assuming 70% loading) per 3-sector site (both uplink and downlink)
- Cell edge throughput (assuming 70% loading) per sector (both uplink and downlink), serving the 95<sup>th</sup> percentile and above.

All modeling and traffic assumptions should be provided in the RFI response. Respondents should provide capacity predictions using the 10MHz of Public Safety Spectrum only. The backhaul (throughput) required to meet the proposed system architecture throughput performance should be described.

In order to accommodate more detailed capacity requirements as the Broadband Network is implemented, the designers of the Network shall coordinate with the Bay Area to:

1. Design capacity, working with both the day-to-day and disaster scenarios of numbers of users and applications used.
2. Develop an initial service and capacity footprint, with the ability to enhance capacity in later phases of deployment.
3. Determine and discuss how additional capacity will be made available in an emergency—for example, by terminating non-critical users.
4. Determine how capacity in particular geographic areas can be enhanced in an emergency, for example, by deploying cells on wheels.

Jurisdictions may need to modify their requirements in an emergency, where the geographic distribution may be different from any plan, and out-of-area responders (neighbors, state, federal) may take part. As a result, the Broadband Network will need to be sufficiently flexible to add capacity in an ad hoc manner. Respondents should discuss how these design changes and capacity enhancements can be implemented within their proposed solution.

## **D. Mobility and Handoff**

The technology deployed should allow for portable, high speed (75mph) mobility and seamless handoffs between base station nodes within the Region's Broadband Network. Further, the infrastructure should allow for mobility across base station nodes while maintaining a secure connection (VPN session) and session persistence in a portable environment. Respondents should discuss how this feature is provided within the proposed Broadband Network. In addition, Respondents should discuss how mobility and handoff are handled when entering into adjacent networks, including the SWBN.

---

<sup>4</sup> To generate average throughput and cell edge throughput levels, Respondents can assume a mix of applications and usage scenarios, with users evenly distributed throughout the coverage area. Respondents can use the NPSTC Statement of Requirements document (section 3.2) as a reference for assumed traffic loading per application.

## **E. Roaming**

To ensure nationwide interoperability and compatibility, the Broadband Network and subscriber devices should support intra-system<sup>5</sup> roaming and inter-system roaming<sup>6</sup>. Roaming capabilities should have the following characteristics:

- In the absence of coverage from the home network, the ability for the User Equipment (UE) to scan supported bands, perform cell selection and authentication on a visited network
- After authentication on a visited network, the assignment of an IP address, and the ability to communicate with the public Internet
- Handoff of active sessions / calls between home and visited networks is required when both networks are using LTE technology
- Handoff of active sessions / calls between home and visited networks is not required when a visited network is using earlier generation wireless technologies.

Respondents should discuss how roaming is provided within their network, and proposed subscriber devices.

## **F. Network Reliability, Availability and Hardening**

To meet public safety standards and first responder expectations, the Broadband Network should minimize and/or avoid single points of failure in the system design. Respondents should discuss how the major components of the system are highly available, or redundant. This should include power systems, backhaul, site equipment, core network equipment and network operating centers (NOCs). In terms of the Radio Access Network, sites shall have on-site backup power of at least 8 hours for all of the network equipment. The system shall have redundancy of the backhaul connection between an antenna site and the core infrastructure. There should be high availability of radio signal within the service area, and mechanisms that will provide redundant coverage (i.e. in the case of a base station outage) should be discussed. Respondents should discuss the Mean Time Between failure for all system components, including devices.

## **G. Network Security**

The Broadband Network must allow for secure, standards-based, user authentication techniques, end-to-end encrypted transmissions<sup>7</sup>, and mechanisms to detect rouge units or unlawful behavior on the network. Auditing capability, to track users and usage should be included within the network management system. The Broadband Network must allow highly secure public safety applications, including local, CLETS and NCIC

---

<sup>5</sup> Intra-system roaming refers to roaming amongst early-build out networks in localized regions as well as the National Shared Wireless Broadband Network (SWBN).

<sup>6</sup> Inter-system roaming refers to roaming between the public safety 700MHz broadband network and commercial carrier networks. This includes legacy or alternate technology networks including HSPA, EDVO, WiMAX, or other network standard.

<sup>7</sup> Statement assumes encrypted transmissions meeting Federal Information Processing System (FIPS) Publication 140-2 (Level 1 minimum) standards, or applicable DOJ standard when network is implemented.

database traffic the ability to traverse the network. The Network must support Virtual Private Networking (VPN) sessions administered by local jurisdictions. Respondents should discuss the security mechanisms offered within their proposed solution.

## **H. Network Priorities**

The Broadband Network must support the ability to prioritize users as well as applications. It should support multiple levels of priorities that can be separately assignable to individuals or applications. In addition, the prioritization scheme should allow for the following<sup>8</sup>:

- Ensuring that critical users remain continuously connected even as many critical and non-critical users attempt to use the network and the network becomes saturated.
- Ensuring that critical users are able to newly connect to the network, regardless of use or saturation and even if non-critical users must be disconnected or limited.
- Providing sufficient priority mechanisms to key applications such as voice and video that would suffer in the event of interruption.
- Enabling critical users to remain connected as they roam from cell to cell.
- A prioritization scheme among the first responders, so that in the event of saturation by the first responders themselves, the incident commander can prioritize particular applications or particular groups of responders.
- Dynamically prioritize users and applications in a segmented area of the Network (i.e. in the case of a localized incident).
- Priorities must be maintained as roaming is allowed, and as users roam onto the nationwide SWBN

Respondents must discuss how these requirements can be provided within their system architecture and enabled within the Broadband Network.

In addition to these priorities, Respondents should discuss how the proposed network supports Quality of Service, IPv6 network addressing, Preemption, Partitioning, and how these mechanisms are maintained through the Broadband Network, on the access channel as well as the transmission channels.

## **I. Network Compatibility and Interfaces**

The Broadband Network must interface to existing IP-based public safety systems, including existing terrestrial (Internet), satellite and wireless networks. Respondents should discuss how their solution is compatible with these existing systems.

## **J. Network Administrative and Operational Capabilities**

---

<sup>8</sup> “Prioritization” refers to the mechanism to allocate a party of higher priority a higher level of service availability so that their transmissions are given higher priority for continuous connectivity than lower-priority parties.

The proposed Broadband Network must have robust network management and administrative capabilities to allow for long term operations and maintenance of the system. These features should include the following:

- Easily maintain users within the system
- Detailed statistical and reporting capabilities, including data volume, network/component failures, detailed airtime summary reports, system utilization and capacity reports, and accounting reports
- The ability to determine who has access to the sites and knowledge of the infrastructure
- Determine how individuals obtain devices and how they connect to the network
- Manage capacity usage on the network with a range of techniques, including, maintaining priorities (for users and applications) on the system and selecting and authorizing all accounts and devices, managing Quality of Service and Tier of Service
- In the event of a security or other event, can immediately disconnect a user or de-authorize a device.

Network management should include system performance monitoring and fault management detection. The system must be able to alert staff to items affecting performance degradation and component failure. The system architecture and network configuration should be easily viewable and will be graphically displayed presenting system and segment bandwidth allocation and utilization. Respondents should discuss how their proposed solution meets these requirements.

## **K. Device Requirements**

The devices that operate on the network must have the following capabilities:

- Capable of IPv6
- USB connectivity in the form of a dongle or modem
- Remote modem should be capable using 12VDC power source and adaptable to 120VAC
- Remote Modem should have a detachable antenna capable of being extended or RF port compatible with mobile antenna products.
- Modems should provide link/connectivity status indicators
- All devices should be over the air upgradable/configurable
- System/network specific configuration should be retained by the device
- Ethernet connectivity to client devices in the form of a remote modem
- Ability to operate as a remote node or wireless router to support WiFi device connectivity
- All devices should compliment system performance i.e. throughput, latency and coverage expectations.
- All devices should provide web base configuration, status and troubleshooting access
- Laptop, notebook and work station PCI and PCIE installation
- Provide connectivity to PDA style devices

- Development of a handheld device emulating Land Mobile Radio operation and features using data and VoIP and providing high voice fidelity.
- For migration and system scalability a mesh router should be made available.

It is understood that some of these device features may not be available within the timeframe discussed in the RFI. Respondents should discuss the device form factors and features that are available in the first deployment of the Broadband Network. For those device features that are not available, a roadmap, discussing availability, should be provided in the RFI response.

## **L. Technical Applications and Use Case Scenarios**

The following is a list of use case scenarios<sup>9</sup> that are applicable to the operational capabilities of the Broadband Network. Respondents should discuss how the proposed solution will allow these applications to be delivered to end users. It is understood that some of these use cases may not be available within the timeframe discussed in the RFI. For those that are not available, a roadmap, discussing availability, should be provided in the RFI response.

- **Global Internet Access** - Users will use the Internet both as a way to access home network systems and to access other systems and services available over the public Internet, including but not limited to messaging systems and web servers.
- **Mobile VPN Access** - Public safety and other public sector users of wireless broadband networks require access to home networks and applications while roaming on other public and commercial networks. Virtual private networks are commonly used to logically extend home networks and provide security for information traversing untrusted networks. U.S. criminal justice agencies accessing Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) Division systems, such as the National Crime Information Center (NCIC) and criminal records systems, are subject to the particular security requirements that commonly lead to the use of VPNs.
- **Universal Network Greeting Capability** – the Network must provide a standard method to obtain a "home page" for visitors to the system. This "home page" will facilitate access to and distribution of available applications, alerts, incident-specific information, system status information, and information that the operator deems important to share with visitors to the system. Federated authentication could be used to allow for online resource registration (Example: user arrives and registers as urban rescue tech,) including announcing to Incident Command who the user is and what equipment/resources he or she has on hand.
- **Network Messaging** – The Network shall provide the ability for users to send and receive text messages. For example, a Public Safety user arrives on a visited network while responding for mutual aid for disaster recovery. She is able to receive text messages providing status updates on staging locations and voice radio assignments. Once on the scene, she is able to take photographs of damaged

---

<sup>9</sup> Use Case Scenarios reference the National Public Safety Telecommunications Council (NPSTC) – Operations Working Group, Network Requirements Document. See the NPSTC 700MHz Public Safety Broadband Task Force Report and Recommendations for additional detail.

infrastructure and send them to the local EOC. She also exchanges multimedia messages with support staff who utilize commercial cellular phones on commercial networks run by various carriers.

- Location Based Services – The Network should include the capability to collect and convey subscriber unit location data in real time. Location data should be accessible to appropriate applications, as may be authorized by management level policy. Location data applications may be located on both subscriber units and associated agency level command/control applications. Subscriber units should meet the same minimum location data information requirements (format and accuracy) as is currently applicable on current commercial services networks in order to retain a broad level of compatibility with incumbent systems.
- NIMS/ICS Compatibility – Responders in mutual aid to agencies served by the Network need access to carry out their responsibilities and communicate with the agencies served. The National Incident Management System (NIMS) Incident Command System (ICS) provides a logical framework for command, control, and communications that can be used to determine information nodes and flows. All responders falling within the ICS structure defined for the mutual aid incident should be provided access to the network.
- Medical Telemetry - Ground and air ambulances routinely transport patients through multiple jurisdictions and past multiple hospitals. Patient telemetry and other broadband applications should be able to be sent to the destination hospital as well as other hospitals en route that may need to be communicated with if a patient emergency arises.
- Multicast Capability – The Network should provide one-to-many communications capabilities to users responding in mutual aid, within or outside the network. These communications capabilities should extend from voice, as commonly used in traditional land mobile radio systems, to text messaging, to video, and other forms of data communications.
- Land Mobile Radio (LMR) Interface – The Network should provide voice interoperability interfaces to existing agency LMR systems in the Bay Area. Public Safety users on such home or visited networks should be able to call or hail an authoritative dispatch agency or control point using the 700 MHz subscriber device with microphone and speaker for two-way audio and talk or be connected to other serving agency voice communications resources.
- Public Switch Telephone Network (PSTN) Interface – The Network should interface with the Public Switched Telephone Network and its full-duplex voice capabilities. A user shall have access to voice telecommunications services using commercially available cell phone like devices, and should have the ability to place and receive phone calls across the network.
- Field Deployed Service – The Network shall support the use of field-deployed server applications such that client devices consistently and continuously reach these server based systems from any location on the Internet.
- Embedded Devices – The Network must support embedded device/modem operation to create wide-area wireless networking capability. This would enable applications including remote SCADA, telemetry, traffic monitoring and control, meter reading applications, remote alarms/sensors, and fire station alerting.

- Software Updates and Over-the-Air Programming – The Network must support the ability to wirelessly update software, applications, and/or devices operating on the Network. It is desired that users have the ability to download applications in the field, and have their mobile device automatically configured to operate.

## IV. PREPARING A RESPONSE

### Overview

Respondents must submit the requested information in the format specified below. Brochures, literature and demonstrations are welcome, but should not be submitted in lieu of responding to the individual items below. As described in the Introduction, the Bay Area's goal is to provide a Regional 700MHz Wireless Mobile Broadband Network ("Broadband Network") providing mobile wireless broadband services throughout the geographic area of the 10 Bay Area Counties. The Bay Area would like Respondents to outline the system, technology, and business model approach that they believe will provide the highest level of interoperability throughout the Region, and can be deployed in a cost effective manner for government entities.

In addition to addressing the requirements in Section III, items A-L, Respondents should provide information to the numbered questions below. The description after each item number is meant to be a starting point, and Respondents are encouraged to provide any information that is pertinent to the item. If you are not responding to an item number, then indicate "not offered, not applicable," etc.

1. Provide a letter of introduction with a brief description of your firm, experience in the industry, number of years providing similar services, primary client type, and a brief summary of solution offered. Include company name, address, contact name, title, phone number, fax number, and email address.
2. The Bay Area realizes that to build a regional broadband network, encompassing the entire jurisdiction of the 10 bay area counties, there will be significant investment needed. Therefore, the Bay Area seeks comment regarding the best choice of business model for the regional network. Possible approaches include:
  - 1) Public-private partnership (with either a commercial or not-for-profit partner); In this regard, the Bay Area is open to a leased or hosted network model
  - 2) Public/government build-own-operate (possibly in partnership with a system integrator or infrastructure vendors);
  - 3) Hybrid approach
  - 4) Other models

The Respondents shall explain in detail how their recommended model will address the geographic, economic and political characteristics of the Region, the service needs of the public safety community, and recognized funding limitations.

3. Respondents should discuss the technology platform that they are proposing, its compliance to the LTE standard and how it integrates to the endorsed LTE standard. If the Respondents do not believe the LTE platform should be the network technology platform, their reasoning should be explained. The explanation should discuss the methods to make the

differing technologies interoperable. It is the intention of the Bay Area to utilize a network that conforms and is in full compliance with the LTE standards, as specified by the 3GPP standards organization.

4. Fourth Generation (4G) LTE equipment may not be commercially available within the timeline indicated in the RFI (for the initial phases of the system deployment/service offering). If the 4G LTE platform is not proposed, due to product availability, Respondents should discuss how to migrate their proposed equipment to this technology platform to then be compatible with the SWBN. Further, any additional costs for migration to the (4G) LTE platform should be identified and included in the baseline deployment for each phase.

5. D-Block Spectrum Alternative - Currently the Bay Area Cities expect to gain access to 10 MHz (5MHz+5MHz) of the Public Safety Spectrum that has been reserved for public safety use. In addition, it is possible that an additional 10 MHz comprising the D-Block may become available for public safety use, making a total of 20 MHz (10MHz+10MHz) available for the proposed network.

Respondents should discuss how the addition of this 10 MHz of D-Block Spectrum would change Respondents cost analysis or recommended business model. Can a network (initially built to use only the 10 MHz of Public Safety Spectrum) be easily adapted to incorporate the additional 10 MHz of D-Block Spectrum? Can the same equipment be leveraged in a 20MHz system? Respondents are asked to comment on how they would structure a public-private partnership with the additional spectrum available.

From a technical perspective, the Bay Area is also seeking guidance on the additional services that can be deployed over the network utilizing all 20MHz of spectrum. The Bay Area is seeking a capacity analysis giving guidance on whether the network can support all data services, including mission critical voice services, video services, and other multi-media data capabilities. Will the 20MHz of spectrum provide the bandwidth necessary to deploy all of these services? For the capacity analysis, Respondents asked to make general assumptions for system usage (i.e. X number of users per sector, serving X number of PPT calls, video sessions, and Internet sessions). Respondents should provide these assumptions as part of the capacity analysis.

6. The system architecture should be discussed in detail, including the components for the Radio Access Network, the Core IP Network the network management system, power systems and the backhaul. Respondents should include all the network equipment necessary to process the communications end-to-end and must be capable of interconnection with each jurisdictions' WANs;

7. In terms of the Core Network, each component that is proposed by the Respondent should be described in detail. It is assumed the Core Network will provide subscriber authentication, mobility management, policy enforcement, and gateways to alternate packet switched networks (including Internet) as well as a path to roam between the SWBN, and other regionally deployed networks. The Bay Area is open to a vendor-owned/hosted or managed model for the Core Network.

8. For the Radio Access Network (RAN), the space requirements for the rooftop antenna systems should be described for a typical site. The rack space and space footprint required for

typical site equipment should be identified, including power systems, backhaul equipment, network equipment and base stations. Heat dissipation and power loading requirements for a typical site should also be defined. Respondents should provide architecture overview diagrams, network diagrams, including all proposed components, within their response. As an option, the Bay Area is considering the co-location or sharing of base station sites, with existing government owned sites (listed in Appendix B) and/or private (i.e. cellular) sites that could be leveraged for the system.

9. Respondents should discuss the types of mobile and portable devices that are available (or can quickly and cost-effectively be made available) for the Broadband Network users. Can commercially available devices that exist today be easily adaptable for the 700 MHz Public Safety band and/or upgradable to the LTE standard? What types of costs will such upgrades entail? Do these devices have a standard interface that can easily and cost-effectively connect with existing commercially available devices/equipment? Are there devices available that can roam between the existing commercial cellular networks in the United States and the proposed Broadband Network<sup>10</sup>? Are there leasing options available for devices?

10. Cost Modeling: The Bay Area seeks detailed cost models to support the Respondents estimates for the recurring and non-recurring costs of the proposed Broadband Network. Costs must take into consideration the different business model approaches proposed by the Respondents. To the extent feasible, please provide detailed cost information, which includes itemized pricing for:

- Design and engineering costs
- Deployment costs, including construction, network equipment, installation, acceptance testing and training. Cost for equipment should be itemized and separated from professional services fees. (For estimation and evaluation purposes, costs for a typical RAN site should be itemized and provided as an option)
- On-going network lease fees, hosting fees, site access or co-location fees (if applicable)
- Network management and operations (See items #13-16 below for further details on Network Management requirements)
- End user devices costs (per unit), and (if applicable) monthly service fees, and leasing fees end user devices
- Commercial providers responding to the RFI should consider network roaming fees, and outline agreements that can be made to provide inter-system roaming.

11. Respondents should provide cost breakdowns for each phase of the project. Similar to the coverage models, to the extent feasible, costs should be broken down for each jurisdiction. If there are advantages to combining jurisdictions and sharing components across counties, those costs should be identified. As an option, the following cost breakdown can be used:

1. City of Oakland

---

<sup>10</sup> The statement assumes the Bay Area already has the necessary network roaming agreements in place with the commercial carriers.

2. City and County of San Francisco
3. City of San Jose
4. County of Alameda
5. County of Contra Costa
6. County of Marin
7. County of Napa
8. County of San Mateo
9. County of Santa Clara
10. County of Santa Cruz
11. County of Sonoma
12. County of Solano

Costs should also be derived based on the number of sites needed to provide the coverage and throughput requirements discussed in Section III. At a minimum, costs must include 8 hours of backup power, costs for the estimated backhaul needs, including redundant site links. The sites proposed should be actual, feasible sites that could be built out and/or leased by the Agencies. Site coordinates, and system architecture drawings should be provided in the response. Potential government-maintained site locations are listed in Appendix B.

The Bay Area reserves the right to use these costs estimates for grant applications, funding opportunities and budget purposes. In several instances of Federal Grant Programs, Grant Applicants are required to provide cash and/or in-kind matches of up to 25% of the total grant award. Respondents should discuss their willingness and ability to partner with Grant Applicants to provide the cash or in-kind match requirements for Grant applications.

12. Respondents should provide a Maintenance Plan that includes an experienced-based equipment/system preventive maintenance, repair, and lifecycle replacement program. The Maintenance Plan should include a user agency trouble reporting process and the use of modern Ethernet network management, fault management/system diagnostic equipment, recommendations on how alarm/alerting notification should be implemented, responded to, and resolved, as well as how repairs will be addressed during normal business/weekends and/or after business hours for all non-critical and critical/emergency repairs, also include response time expectations, and cost estimates for a centralized and distributed/regionally shared program. Respondents should offer as an option 1-5 year Network Management and Maintenance Service Level Agreements for providing 24x7 network administration and technical support services for the network.

13. Respondents should provide detailed information in support of their proposed system that include the required management, technical support and maintenance services necessary to sustain the proposed Broadband Network during its specified initial warranty period and

thereafter on an ongoing basis. This information should provide the Region with a clear picture on-going maintenance requirements, including roles and responsibilities of each required staff position, as well as the minimum staffing levels (i.e., full-time, ¾-time, ½-time, or other), on-going training and technical experience required by classification working within one or more support centers as required to manage, maintain and repair the proposed system based on an ongoing 24x7 continuous operation.

14. Respondents should provide the anticipated replacement schedule, and estimate the lifecycle (3, 5, 10, 15, other years) the proposed system will provide. The equipment lifecycle replacement program should identify the anticipated useful life of the overall system and its replacement cost on an annualized basis. Some hardware equipment and/or software may have a projected lifecycle well below that of the overall system. Understanding that there is a difference between mandatory and desired replacement schedules, please include both considerations in your response. Respondents need to provide an anticipated equipment replacement schedule, with estimated costs that include estimated time and cost to install, on an annual basis, over the life of the proposed system.

15. In terms of network management, the Bay Area is exploring what role its participants will play in the ongoing operations of the network. It is possible that different jurisdictions will have different involvement. It is requested that the Respondent describe its operational role and the cost to the Bay Area of two different system management approaches:

- Respondent provides design, equipment, integration, user training, and spares for all core and base station components and software. Respondent is available 24x7 for Tier Three technical support. Jurisdictions operate a help desk and network operations center, operate accounts, provision devices and provide Tier One and Tier Two technical support.
- Respondent provides design, equipment, integration, and user training. Respondent operates help desk and network operations center 24x7. Respondent sets up and operates accounts, provision devices, and provides all technical support under supervision of jurisdictions.

## V. SUBMITTAL INSTRUCTIONS

### A. Paper Submittal

To submit a hard copy response, include ten complete sets, as well as 30 Compact Disk (CD) copies, in an envelope labeled RFI response for Regional 700MHz Wireless Mobile Broadband System. See schedule below and mail to:

Bay Area Urban Area Security Initiative  
Attn. Clement Ng  
10 Lombard St, Suite 410  
San Francisco, CA 94111

## B. Electronic Submittal

There will be no electronic submittals for the RFI response.

## C. Inquiries

Any requests for clarification concerning the RFI must be made by e-mail to:

[Clement.Ng@sfgov.org](mailto:Clement.Ng@sfgov.org)

by the “Deadline for RFI clarification questions” listed below. The City and County of San Francisco will coordinate with the other Bay Area Cities and/or Counties to ensure the inquiries are addressed and answered by the appropriate jurisdiction. The City will post all inquiries and their responses on the website (<http://sunset.ci.sf.ca.us/pbids.nsf>), and will not respond directly to the person who submitted the inquiry other than to note that the response is posted on the website. The choice whether to respond to such requests shall be at the Bay Area’s sole discretion. No oral responses by any employee, consultant or agent of the Bay Area shall be binding, or shall in any way constitute a commitment by the Bay Area.

## D. Schedule

The following is the schedule for this RFI process. Responses must be submitted as provided above by the time on the responses due date indicated below.

<u>Phase</u>	<u>Date</u> *
RFI is issued.....	September 29 <sup>th</sup> , 2009
Pre-proposal Conference (1:30 p.m.)^ .....	October 21 <sup>st</sup> , 2009
Deadline for RFI clarification questions in writing (5 p.m.) ** .....	October 28 <sup>th</sup> , 2009
Summary of clarification information available .....	November 6 <sup>th</sup> , 2009
Response due date (5 p.m.) .....	November 16 <sup>th</sup> , 2009

\* Each date is subject to change by issuance of an addendum to this RFI.

\*\* Times shown are PST.

^Pre-Proposal Conference is Wednesday, October 21st at 1:30pm Alameda County Emergency Operations Center at 4985 Broder Blvd, Dublin CA

## E. Costs for Pilot Project/Early Deployment

It is not the Bay Area’s intent to award a contract based on this RFI; however, the Bay Area reserves the right, at its sole discretion, to request additional information, demonstrations or presentations, or to form test or pilot projects. Based on the quality of the Respondent’s RFI response, the Bay Area Cities will consider funded trial deployments in targeted areas within three jurisdictions. As described in San Francisco Administrative Code Section 21.5, the Cities will engage in pilot projects, with duration of no more than 2 years. Subsequent to the pilot projects, a competitive solicitation may be formalized and released by the Region.

The requirements for the pilot project are given in the Section III of the RFI, and additional information for each jurisdiction is described in Appendix A. The Cities may exercise pilot deployments with multiple Respondents, including service providers, equipment manufacturers,

system integrators, and/or non-profit organizations. However, vendors that are selected for pilot projects are required to comply with a variety of compliance requirements.

## **VI. RIDERS**

### **Submitting a Response to the RFI**

The submittal of a response to this RFI does not guarantee use of the information provided. This is not a Request for Proposals (RFP). The Bay Area, at its sole discretion, will determine if a Request for Proposal or other competitive solicitation may be issued at a later date. Any RFP issued by the Bay Area may differ significantly in content from the equipment and services described in this RFI document. This RFI is to be used solely for the purpose of this industry review and the Bay Area assumes no responsibility for any other use of this document. It is not a requirement to participate in this industry review process in order to be considered by any competitive solicitation arising out of this process. Participation in this industry review is strictly voluntary and the Bay Area will not reimburse participants for any costs in connection therein. Submission of the RFI does not guarantee any future business with the Bay Area participants. The issuance of this RFI does not constitute agreement by the Bay Area that any contract will actually be entered into by the Bay Area participants. The Bay Area expressly reserves the rights to:

1. Waive or correct any defect or informality in any proposal, response or response procedure;
2. Reject any or all responses and re-issue a new RFI, RFQ or RFP;
3. Prior to submission deadline for responses, modify all or any portion of the schedule for receiving responses;
4. Procure any materials, equipment, products or services specified in this RFI by any other means; or
5. Determine that no project will be pursued.

### **No Financial Responsibility**

The Bay Area accepts no financial responsibility for any costs incurred by a firm in responding to this RFI.

## **VII. PUBLIC RECORDS ACT/SUNSHINE ORDINANCE**

Responses to this RFI become the exclusive property of the City and County of San Francisco (City) and are subject to the California Public Records Act and the City's Sunshine Ordinance. Those elements in each submittal which are trade secrets, as that term is defined in Civil Code section 3426.1(d), or otherwise exempt by law from disclosure and which are prominently marked as "TRADE SECRET," "CONFIDENTIAL," or "PROPRIETARY" may not be subject to disclosure. The City shall not in any way be liable or responsible for the disclosure of any such records including, without limitation, those so marked if disclosure is deemed to be required by law or by an order of a court. Respondents who indiscriminately identify all or most of their submittal as exempt from disclosure without justification may be deemed non-responsive. In the event that the City is required to defend an action on a Public Records Act or Sunshine Ordinance request for any of the contents of a submittal marked "CONFIDENTIAL," "PROPRIETARY," or "TRADE SECRET," respondent agrees, upon submission of its submittal for the City's considerations, to defend and indemnify the City from all costs and expenses, including attorney's fees, in any action and any liability arising under the Public Records Act or Sunshine Ordinance.



## APPENDIX A– PILOT PROJECTS

### A. San Francisco

The City and County of San Francisco pilot project will service public safety users and participating government services personnel within the City and County of San Francisco. Dependent on the costs and available funds for the pilot project, the City will determine the extent of the deployment, and the geographic service area.

At a minimum, the critical service area for the trail deployment is the southeast portion of the City, as shown in the attached figure. In addition, potential city-wide sites that can be utilized are described in Appendix B.



The City is interested in the following applications operating on the Network:

- San Francisco Police Department (SFPD) wireless applications including VPN access, access to SFPD 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 San Francisco County Mugshot system access
- San Francisco Municipal Transportation Agency (Muni) wireless applications including Internet and WiFi access within Muni vehicles, real-time Fare Collection System that integrates to onboard fare boxes within Muni vehicles, and Muni onboard video systems to stream images dynamically from the mobile fleet
- San Francisco Public Utilities Commission wireless applications including Master to Remote and Remote to Remote SCADA Ethernet Communications
- Department of Technology applications including Wireless Call Boxes, embedded Traffic Signal Control, and general Internet/VPN access in the field for City Departments

In addition to the technical and operational requirements provided in Section III, San Francisco is interested in other backup power solutions for each site, including a combination of solar, battery and generator power options. The solution should allow for 3 days of backup power.

## B. Oakland

The City of Oakland's Public Safety mobile data requirements are being driven by an expansion in the availability of graphically rich applications and increased resolution of content, including full motion video, office applications, and mapping/GIS-enabled reporting tools. Public Safety applications are now demanding mobile access to traditional desktop applications and emerging rich content information types, driving the requirements for high quality, high speed, reliable and flexible Internet Protocol (IP) - based broadband capabilities.

Successfully developing and deploying broadband mobile data capabilities in the Downtown Oakland area will provide the infrastructure for a new high-performance mobile data system that will include in-vehicle email access, in-car video streaming, patient care report transfer, location based services, secure web browsers, field-based reporting, intra-application data transfer and other advanced field communications tools. Oakland's public safety broadband wireless network will significantly enhance crime-fighting and fire-suppression capabilities and allow our first responders to be much safer and more productive on the streets by providing access to real-time data and additional critical information.

The Public Safety Broadband Wireless Network will assist the first responders to have instant access to criminal databases for suspect information, improved situational awareness using video technologies, and real time tracking of assets, firefighters and resources would be available throughout the Oakland downtown. The LTE based network will be designed and deployed in the Oakland downtown, utilizing the current infrastructure of buildings, conduits, fiber optic cables, antenna structure.

The Pilot project will be deployed in the Oakland downtown, utilizing the City buildings and facilities. City of Oakland proposes installation at five (5) sites, located in the Downtown area and within walking distance from the Port of Oakland, as part of the wireless broadband subsystem. This topology will assist in deploying the Pilot network in the heart of the Oakland, and providing a foundation for the future expansion of the public safety broadband access throughout the city. This early build-out of downtown network hubs will assist the City in gaining the immediate benefits by bringing life, business, and safety in the downtown area.

The Pilot project will realize significant cost and time savings by utilizing the City resources, infrastructure as well as human capital and knowledge. A detailed project plan with the timeline and assigned resources shall be developed, based on the guidelines and best practices outlined by the Project Management Institute (PMI).

The five sites proposed for the early deployment - including the buildings and land - are wholly owned by the City of Oakland. Most of the infrastructure, including Fiber-Optic conduits and electrical service, is in place.

- Police Administration Building – 455 7th Street
- Emergency Operations Center (EOC) – 1605 Martin Luther King Jr. Way
- Lionel Wilson Building – 150 Frank H. Ogawa Plaza
- Oakland City Hall – 1 Frank H. Ogawa Plaza
- Fire Alarm Building – 1324 Oak Street

There is an estimated **650 subscribers** in the Downtown Oakland Area, who will be accessing the public safety wireless network for their day to day operations:

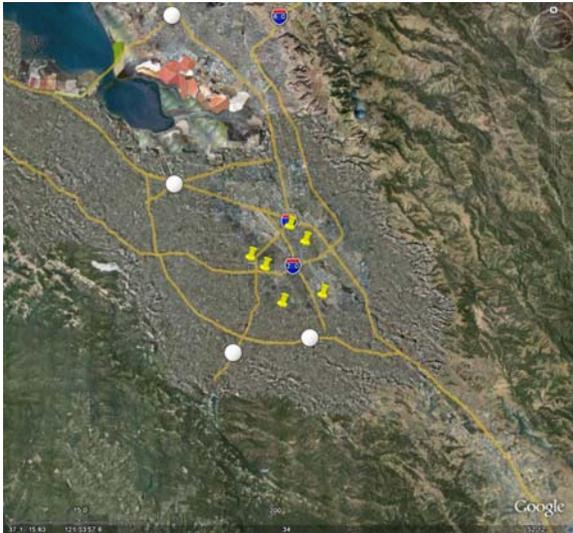


- Police Officers **400**
- Fire Personnel **100**
- Public Works **50**
- Other NGOs, including local public health agencies **50**
- Neighboring first responder agencies **50**

In case of a disaster and emergency situation, the number of users will be significantly higher.

## C. San Jose

The City of San Jose pilot project will serve Public Safety and Government Services operations in a western area of the city. The objective of the trial is proof of concept to provide superior broadband performance replacing the City's existing obsolete wireless data system and intra-agency interoperability by providing a common conduit of connectivity to all applicable government resources essential to the recovery of a catastrophic event. The pilot sites are listed in Appendix B.



The applications that will be trialed are:

- San Jose Police Department wireless applications include City Intranet access, CAD, OWA Email. Portable E-Cite Device applications include Mugshot Media, Finger Print Media, Portable VoIP/data. In car camera/video including live stream video media. Building CCTV surveillance camera monitoring. Mobile Data Computer applications including Media/Video, Radio /GPS/AVL, CAD/Imobile and Finger print. Mobile Fleet inventory control applications. Officer mounted video camera.
- San Jose Fire Department wireless applications include RMS, Fire House, OWA Email, Telestaffing, City Intranet access, CAD/MAPS Prefire Planning Software and internet web site resources. Fixed applications would include Fire Station Alerting and City Intranet access.
- City of San Jose Department of Transportation wireless applications include Traffic Signal Control, Traffic Control Systems and Video Traffic Surveillance systems.
- Other applications to include SCADA and telemetry for control and monitoring public infrastructure.

## **APPENDIX B – POTENTIAL RADIO SITES**

See Attached Document

# Smart Grid Deployments: Accounting Clarifications to Ensure Efficient Choices

## Introduction

Spurred by increased focus on the nation's energy policy, emphasis on energy security, and the desire to shift the supply mix to cleaner sources of electricity, the utility industry has been focused on upgrading its electrical infrastructure for the 21<sup>st</sup> century. Although the precise end-state vision of the Smart Grid has many complex components, they all rely on enabling elements of the electrical grid to "talk" to the utility and to one another.<sup>1</sup> This, in turn, requires the utility to choose a technology for enabling communication among these smart devices.

Utilities have a number of different network architecture options for achieving this connectivity. The most popular include RF Mesh, Point-to-Multipoint Narrowband, Power Line Communications and commercial carrier solutions using existing wireless networks. Since the industry is still new, no single, dominant network architecture has emerged, and utilities often use a combination of different technologies.

As we explain below, certain regulatory accounting practices may create incentives for Investor Owned Utilities ("IOUs") to opt for an architecture (and an associated funding model) that are neither the most efficient, nor the cheapest for rate payers. This document explores potential accounting policy solutions that could reduce the extent to which factors other than cost and efficiency drive the choice among Smart Grid communication technologies.<sup>2</sup>

## Utility Funding and Accounting Overview

First, it is useful to consider how IOUs set rates and fund large projects. Since the electric industry requires large up-front capital investments, a mechanism exists to ensure that IOUs can earn an acceptable rate of return on their infrastructure investments, while also serving the public interest. To serve those dual ends, IOUs operate in a strict, regulatory accounting environment which defines allowable targets for their rate of return on capital investments. State Public Utility Commissions ("PUCs") have the most direct authority in this process; they apply accounting rules to determine the rates that a utility may charge. The Federal Energy Regulatory Commission ("FERC") and the Department of Energy ("DoE") also have authority to prescribe nationwide guidelines. In particular, FERC issues guidance on the application of accounting rules to electric utilities.

To see how the process works, consider the example of a utility that decides to invest in Smart Grid infrastructure. The funds to pay for the project can come either from expected future cost savings (e.g. elimination of manual meter readings) or from higher rates. If the utility is to impose a rate increase, it must obtain the PUC's approval through the mechanism of a rate case.

A utility can rely on either capital expenditures or operating expenses to support its request for higher rates. Regulatory accounting rules generally require that recurring operating expenses be passed on directly to rate payers. On the other hand, utilities are allowed to earn an 8-12% rate of return (depending on the state) on capital investments. Thus, the utility and its investors earn nothing on increased operating expenses, which are

---

<sup>1</sup> This includes replacing old household electric meters with new "smart meters" that can transmit usage and pricing information on a more frequent, automated basis, and adding devices in the distribution grid that can monitor the health of the grid by, for example, assessing the risk of a potential blackout.

<sup>2</sup> Note that this document focuses on Investor Owned Utilities and does not address Municipal Utilities or Co-operatives. Municipal Utilities and Co-ops are regulated differently and thus do not face the same incentive distortions that we discuss below for IOUs.

simply passed through to customers at the rate the utility pays, without mark-up. But, if a project qualifies as a capital investment, the utility may increase its rates to recover both the cost of the project *and* the approved rate of return on the capital invested. This creates significant incentives for utilities to prefer Smart Grid projects that rely on capital expenditures, even if the total cost to rate payers is lower for a solution funded by operating expenses.

When deploying Smart Grid technology, the utility is presented with the option of (1) building a single-purpose, private communications network (a capital investment, eligible for the prescribed rate of return), (2) using only the service of commercial wireless providers (a revenue-neutral operating expense), or (3) most likely, choosing a combination of these two alternatives. The challenge is to select the mix of private and commercial network capabilities that represents the best long-term choice for consumers, investors and utility operators. While accounting rules do not prescribe this choice, they have significant revenue implications for large projects like Smart Grid deployment. Accordingly, it is important to ensure that accounting and revenue considerations do not outweigh considerations of network functionality, long-term economics and technological obsolescence for utilities that are choosing how to deploy Smart Grid communications functionality.

In many instances, using existing commercial networks will be the more efficient, lower-cost alternative. The utility can purchase only the communications service that it needs at a given point in time, rather than immediately saddling its investors (and its rate base) with a full network that carries relatively little traffic. And it need not concern itself with managing technology upgrades, ensuring backward compatibility, maintaining security and the myriad reliability issues that come with operating a communications network. It is important, therefore, that the regulatory accounting regime and an IOU's goal of maximizing revenues not drive the utility to make a more costly, less efficient choice for deploying Smart Grid capabilities.

This document does not advocate change to the current regulatory accounting rules but rather explores two accounting policy clarifications which may help assure prudent technology choices that serve both investors and consumers of electricity and promote the rapid introduction of Smart Grid functionality.

### **Utility Accounting Options: Prepaid Expense**

One way to address the situation described above would be for FERC to clarify that current accounting rules provide the option for utilities to treat Smart Grid connectivity costs as a prepaid expense. The state PUCs could also contribute to Smart Grid deployment by affording consistent treatment within the state rate case process. There is precedent for treating such connectivity costs as a prepaid expense. Under certain conditions, items typically viewed as operating expenses – rent, insurance, even labor – are treated like a capital investment. Under this asset treatment, a prepaid expense is capitalized and appears on the balance sheet as *an asset* that is eligible to generate a rate of return.<sup>3</sup>

With such a clarification, accounting rules would be less likely to drive Smart Grid deployment decisions. At the same time, the accounting treatment would ideally be at the discretion of the utility rather than be mandatory. This would permit utilities to make Smart Grid connectivity decisions that best meet the needs of their

---

<sup>3</sup> For the duration of the contract (for example, the length of a lease), the company amortizes the good or service received and accrues the expense on the income statement in each period that the service was consumed. Once fully amortized, the prepaid expense is removed from the balance sheet.

particular situation, considering their true technology merits, cost to the rate payer, and actual operational advantages.

### **Utility Accounting Options: Regulatory Asset**

Another alternative for addressing Smart Grid connectivity is to allow treatment of qualifying recurring Smart Grid connectivity costs as “regulatory assets.” This grows out of the Financial Accounting Standards Board’s Statement No. 71, “Accounting for the Effects of Certain Types of Regulation.” Statement No. 71 allows for the creation of a “regulatory asset” where a PUC has permitted an IOU to place certain “extraordinary” expenses on the balance sheet and amortize them over time. Under this treatment, regulatory asset expenses become eligible for the rate of return calculation during a rate case. Expenses that have been classified as regulatory assets include one-time costs associated with grid repairs after a natural disaster or significant maintenance costs, such as tree pruning along the distribution lines. These types of expenses are accorded special treatment because they present a substantial benefit to the rate payer, such as restoring electricity or reducing the risk of outages.

Classifying costs as regulatory assets requires special state PUC approval. Not all utilities would necessarily elect to engage in the approval process, as it may be costly and lengthy. However, some IOUs that plan large Smart Grid investments might well find it beneficial to treat Smart Grid connectivity costs in this manner. Similar to prepaid-expense treatment, allowing utilities to classify Smart Grid connectivity costs as regulatory assets would allow them to consider the full range of technology options more clearly, and ultimately select the most attractive solution from the perspective of the utility and the rate payer.

### **Implications and Conclusions**

In the current regulatory environment, Investor Owned Utilities must constantly balance the interests of rate payers, shareholders and operational factors. With no specific regulatory provisions or accounting interpretations for Smart Grid investments and with intense pressure from Wall Street to produce returns, utilities may be tempted to select a Smart Grid communications technology based on the ability to generate near-term financial results rather than considering longer-term factors like technological risk, total cost to rate payers, network performance and speed to market. As a result, IOUs may gravitate to certain types of network architectures before thoroughly investigating all the options available to them. Providing utilities with options to treat certain Smart Grid costs as prepaid expenses or regulatory assets would allow IOUs more freely to choose a network technology that benefits the direction of our country’s energy policy, is good for consumers and rate payers, and fosters competition and innovation while also upholding their responsibilities to shareholders.