Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	**PS Docket No. 06-229**
	)	
Comments on Interoperability, Out of Band	)	
Emissions, and Equipment Certification for	)	
700MHz Public Safety Broadband Networks	)	

## I.	INTRODUCTION

The Bay Area UASI, on behalf of the San Francisco Bay Area, respectfully submit

comments in response to the Federal Communications Commission's May 18, 2010 request for

comment on Interoperability, Out of Band Emissions, and Equipment Certification for 700MHz

Public Safety Broadband Networks. The Bay Area is in preparing for the implementation of a

700MHz LTE Wireless Broadband Pilot System for public safety and government use. The Bay

Area is collaborating with the State of California through the California Statewide

Interoperability Executive Committee (CalSIEC), the Public Safety Spectrum Trust (PSST), and

neighboring systems to coordinate the future public safety broadband system. The Bay Area

realizes the importance and fully supports the minimum requirements for interoperability and

proposes several ideas and comments for further rulemaking, which are set forth in the

document.

## II.	INTEROPERABILITY

The Federal Communications Commission seeks comment on several specific aspects of

the technical rules for interoperability as follows:

Applications: The applications specified in the National Public Safety

Telecommunications Council's Broadband Task Force Report are sufficient for the purpose of

promoting nationwide interoperability. The following applications: (1) Internet access; (2) VPN

access to authorized sites and home networks; (3) Status information "homepage;" (4) Access to

responders under the Incident Command System; and (5) Field-based server applications were intended as minimum requirements and are achievable by initial deployments. We support the Commission in incorporating these five (5) requirements into its rules for the nationwide public safety network. Although we support the eventual availability of all the applications and use-cases identified by NPSTC, we do not believe that additional applications should be enforced as minimum requirements today, as several are not supported by the LTE standard, and would add undo capital cost to the network. The Commission should not specify performance measures for the applications within a given network or while roaming on other networks. Rather, the Commission should enforce that the network support a standardized solution for priority access for users and applications. This will ensure that critical users have prioritized access to data in the most efficient way the network can deliver the information. Further, the local network operators should be allowed to manage the system bandwidth on a regional level, on an incident by incident basis, so in critical situations, public safety will have the ability to respond and utilize the network to its fullest extent. If this is not allowed, public safety will be subject to the same limitations they have today on the carrier networks. The Commission should continue to work with the National Institute of Standards and Technology (NIST) and public safety representatives to address the availability and timeliness of the standards development process and technical evolution of LTE as it relates to the requirements. As the technology evolves, the Commission will need to rely on the technical expertise of these bodies to address the need and reasonability for future rules on applications to ensure interoperability.

Roaming: The Waiver Order requirements on the two types of roaming categories: (1) Home-routed traffic, such that a "visiting" public safety user's traffic is routed back to the home network to enable the use of home resources, and (2) Local breakout traffic, such that a visiting public safety user can utilize the resources of the host network; is sufficient for roaming requirements. We do not feel it is necessary to enforce the requirement of roaming to and from commercial networks. The Commission should consider adopting a flexible approach to commercial roaming which allows local areas creativity in deployment and partnerships. But, the requirement for commercial user roaming should not be required on all regional public safety systems. For example, a Region may decide to build their public safety system to maximize coverage throughout its jurisdiction, rather than having excess capacity in the network. If that Region also has a requirement to allow for commercial users on their network, it may overload

the limited bandwidth of the public safety system.   In terms of roaming agreements between public safety regional networks, we believe that there should be bilateral roaming agreements between networks with specific language required and adopted from the Emergency Response Interoperability Center (ERIC). This can allow flexibility for regions to have unique roaming agreements and allow regions to manage their bandwidth accordingly. There are no other technical and governance requirements the Commission should consider adopting to ensure roaming among public safety agencies at this time.

Priority Access: The Waiver Order does not address the issue of priority access, however it is imperative that a priority access scheme be developed and adopted across public safety networks. The priority scheme should include priority on the wireless access via the common air interface, and the prioritization of traffic throughout the network. Further, prioritization should be Quality-of-Service (QoS) based with an emphasis on the priority of applications and types of users. Ideally, public safety and emergency traffic should be prioritized on both Public Safety and while roaming onto commercial networks. Priority access should be required on all public safety networks, but should be governed, implemented, and enforced at the local level, allowing for local control over bandwidth allocation for critical incidents, events and emergencies. The Commission should not dictate how localities and regions to handle operational and governance issues universally as every region is unique and may have their own preferred operational and governance systems they would like to utilize. The technology and associated standards are not necessarily ready for deployment and ERIC should continue to work with public safety, NIST, and the vendor community to develop an amicable solution.

System Characteristics, Interfaces and Testing: Self-certification is sufficient to ensure the Interoperability Testing (IOT) requirement on a short-term basis but not necessarily on a long-term basis. Required public safety certification in the future should be further developed and collaborated between NIST, public safety representatives and the vendor community. Regarding the selection and use of network identification numbers, the *NPSTC BBTF Report* notes that there are two alternatives for assigning network identification numbers to the regional networks: (1) use a single Public Land Mobile Network (PLMN) identifier for all of public safety, and use a secondary identifier (sub ID) for each individual regional network, or (2) use a different PLMN identifier for each regional network. While the Bay Area does not have specific comment on the technical issues this raises, we believe the Commission should adopt rules that encourage

partnership and sharing of networks, and limit the number of individual networks that are deployed. The Commission should consider basing these rules on several factors, including the geographic area or jurisdiction, the population served and the anticipated subscriber load that the network will support. The rules would simplify the coordination process for assignment of network ID's. Depending on how these regions would be defined, the Commission could take a hybrid approach with PLMN IDs assigned to each region and with another PLMN ID for the Nationwide Public Safety Broadband Network for roaming purposes.

Security: The Bay Area agrees that the current approach to security as per the Waiver Order is sufficient. Additional requirements on security for regional networks will encroach on existing local Information Technology security implementations and could be a detrimental barrier for broadband participation for some agencies due to the cost of compliance.

Performance, Reliability, Capacity and Coverage: In terms of the nationwide network, a "network-of-networks" with different operability criteria at various parts does not hinder nationwide interoperability. A minimum level of service ubiquity is not important for public safety across all networks. The benefits of local control over these matters will outweigh the benefits of service ubiquity and transparency. Regions across the nation will have different requirements and needs for coverage and capacity. Within the Bay Area, there already is disparity in those needs in different counties across our region. Coordination of those needs, even in our area, require a number of resources. If the Commission chose to coordinate those efforts across the nation, it would be a costly endeavor. If the Commission chose to dictate a level of service, capacity, and coverage, there will be public safety agencies whose needs will not be met and as a result might not participate in the system. The regions and local areas will know their related requirements and areas of needed coverage and can work with vendors to develop and implement a broadband system that meets their specific requirements. The Commission should not adopt public safety specific performance, reliability, capability and coverage requirements beyond the standard for the networks and the devices. Public safety organizations, NIST and the vendor community can address this requirement and bring it to the Commission if there are universal needs in this area.

Nationwide Core: There should not be a single nationwide core for the public safety broadband network. A single core for the entire nation would act as a single point of failure for all broadband networks. Conversely, we also do not believe that every locality needs a core

network. Instead, there should be a mix of multiple cores for large regions throughout the Country. The Commission should consider basing the deployment of core networks on several factors, including the geographic area or jurisdiction, the population served and the anticipated subscriber load that the network will support. The Commission should allow waiver deployments to implement core networks that can serve as a regional core network for the nationwide broadband system. ERIC, along with public safety, NIST, and the vendor community, should work together to develop core-to-core interoperability requirements to achieve the goal of nationwide interoperability.

Network Operations, Administration and Maintenance (OA&M): The Commission should not address the operational capability in order to maintain and enhance interoperability. As mentioned in our above comments, public safety is operationally different across the nation. We fully support the existing technical requirements as put forth by the Commission and the need for interoperability. With the deployments of the waivers across the nation, everyone has and will see varying operational, administration, and maintenance models. Every region faces unique financial challenges, political, and jurisdictional landscapes. A single, standardized OA&M model from ERIC would not support a system-of-systems model due to these different challenges. The Bay Area utilizes a system-of-systems approach to our regional interoperable voice system due to these same issues. The Commission should allow for full flexibility in OA&M models to encourage participation in the national broadband implementation.

Governance: The Commission should require the waiver jurisdictions to submit reports to the FCC that detail the steps they are taking to align their investments to governance standards relating to interoperable emergency communications, including alignment of investments to relevant Statewide Communications Interoperability Plans (SCIP), coordination of expenditures with the grantees' Statewide Interoperability Coordinators (SWIC), and any review required by the relevant Statewide Interoperability Governing Bodies (SIGB) and network. By coordinating and aligning with their respective States, the waiver regions will be alignment with national plans such as the National Emergency Communications Plan, for governance. This will also enforce cooperation with neighboring jurisdictions and allow for feedback at a national level through their respective States on such issues.

III. OUT-OF-BAND EMISSIONS (OOBE)

Currently, the Commission has a chance to avoid the OOBE issue and future balkanization of public safety broadband spectrum by giving public safety full use of the D Block, which is continuous with the PSBB Block. The Bay Area supports the *Waiver Order* specified 43 + 10logP dB as the OOBE limit for operations in the PSBB Block. If the Commission continues with the auction of the D Block, extensive tests need to be done where both a D Block and PSBB Block system occupy the same or adjacent space to see if there is significant interference. Even if more stringent OOBE limits were applied to the PSBB Block to mitigate interference, it would not be possible to attenuate signals outside the band without a guard band between D Block and the PSBB Block. In this case, the guard band should be taken out of the D Block frequencies as the size of the PSBB Block already limits the amount of bandwidth available for public safety systems. These tests should be run before the D Block is auctioned off with any future changes to be made solely to the D Block if the auction is successful. The issues surrounding OOBE and their solutions should not affect waiver deployments. The Nextel 800MHz rebanding issue and ruling across the nation is a prime example as to the complication and cost of OOBE interference and the changes to public safety systems.

IV. EQUIPMENT CERTIFICATION

In the *Waiver Order*, the Commission waived the equipment certification requirements under Section 90.203 of the rules and required the manufacturers to comply with the various technical requirements of 3GPP Release 8 LTE specifications pending finalization of the rules. The Commission should be cognizant that any changes to these rules could severely impact any existing deployments by forcing costly equipment migrations. To minimize these occurrences and for processes and implementation on equipment certification, ERIC should work with waiver recipients, public safety, NIST and the vendor community.

Cooperation among the aforementioned parties will assist licensees and manufacturers address the continued evolution of the 3GPP standard from Release 8 LTE to future 3GPP releases.

DATED: June 21, 2010

Respectfully submitted,

BAY AREA UASI

LAURA PHILLIPS
General Manager

BY: _____

       LAURA PHILLIPS
       General Manager