Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	)	WT Docket No. 06-150
	)	
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)	PS Docket No. 06-229
	)	WP Docket No. 07-100
Amendment of Part 90 of the Commission's Rules	)	

COMMENTS OF TELCORDIA TECHNOLOGIES

Telcordia Technologies ("Telcordia") hereby submits its Comments in response to the *Fourth Further Notice of Proposed Rulemaking* in the above-captioned proceeding.[1] The FNPRM seeks comments on technical requirements to establish interoperability among public safety broadband networks that will operate in the 700 MHz Band, including network architecture, security, resiliency, robustness, roaming, and priority access. It also requests input on coverage requirements, including in-building coverage. In addition, it seeks comments on requirements implementation, verification and testing.

[1] *Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Service Rules for the 698-746, 747-762 and777-792 MHz Bands, Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, WT Docket No. 06-150 *et al.*, 26 FCC Rcd 733 (released January 26, 2011) ("FNPRM"); *Public Notice, Public Safety and Homeland Security Bureau Announces Publication in the Federal Register of the Fourth Notice of Proposed Rulemaking in PS Docket 06-229*, 26 FCC Rcd 2084 (released February 24, 2011).

BACKGROUND

Telcordia is a leading software, engineering and network design consulting company. We have led the industry with patented breakthroughs in DSL, ATM, SONET, and AIN as well as primary contributions to the design and specifications of optical fiber networks, Internet Protocol (IP)-based Next Generation Networks (NGN) and Next Generation 911 (NG911), and wireless system protocols including roaming and number portability. Our contributions in emergency communications and public safety include developing detailed standards and industry requirements for our nation's existing emergency priority services, namely the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS), and we continue to work with the industry to develop the standards and industry requirements for more advanced priority services in the NGN environment for wireline and wireless technologies including Long Term Evolution (LTE).

Telcordia has significant experience and capabilities in operating clearinghouses to provide central management, control and exchange of operational and other data among telecommunications networks and systems. Recently, Telcordia was conditionally selected by the Commission's Office of Engineering and Technology (OET) as a TV bands white spaces device database administrator[2] and is the leading provider of number portability clearinghouse software systems worldwide.

Telcordia draws upon its body of work and experience, and its vendor-neutral approach to network technology and architecture, in offering our comments in this proceeding.

[2] *Order, Unlicensed Operation in the TV Broadcast Bands, Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band*, ET Docket 04-286 *et al*., 26 FCC Rcd 554, 556 (released January 26, 2011) ("TV White Spaces Order").

DISCUSSION

Technical Rules for the Public Safety Broadband Network

Architectural Framework (¶ 17)

Telcordia applauds and supports the FCC's adoptions of architectural principles as guidance that will support interoperability and also ensure the necessary flexibility for innovation from a services and technological perspective.

While the focus of the FNPRM's narrative is on the LTE access technology, it is critical for the development of a mission-critical grade, interoperable public safety broadband network that the description and requirements for the Core Network be established in detail. By Core Network we mean the IP Multimedia Subsystem (IMS) as well as non-IMS architectural capabilities to support data. The Core Network interconnects with access networks and provides the services, features and applications that interoperate with the LTE and other access networks. The Core Network consists of service signaling/control and IP-based transport, and must interoperate with the clearinghouse functions. Telcordia believes this should be based on the IP Multimedia Subsystem (IMS) as well as other architectural capabilities. The Core Network specifications will facilitate a minimal set of services in each jurisdiction, and support -- via standards-based network interfaces -- interoperability between jurisdictions and nationwide.

Components of the Nationwide Broadband Public Safety Network (¶ 18)

One of the many virtues of implementing an Internet Protocol (IP)-based network is its inherent design flexibility and the wide range of network topologies that can be accommodated. The Commission's network-of-networks approach is sensible for the air interface (LTE) portion of the nationwide network, inasmuch as the national broadband public safety network will

leverage and interoperate with the dedicated public safety LTE networks to be developed by grantees of 700 MHz early build-out waivers and others. The nationwide public safety network and its subparts also will likely leverage and interoperate with commercial wireless networks via appropriate Quality of Service (QoS) mechanisms, prioritization protocols, and business arrangements.

While this network-of-networks approach is appropriate for the LTE network layer, Telcordia believes that ideally there should be one national public safety network in order to achieve optimal economies of scale and assure the appropriate reliability, redundancy, security, diversity, and prioritization for a potentially expanded user base.[3] In addition, an architecture with one nationwide backbone network supporting public safety will ensure that applications, and gateway and/or other access for other radio technologies *(e.g.*, WiMAX, CDMA/EVDO, GSM/UMTS/HSPA, and P25) are fully supported on an end-to-end basis. We believe that having one nationwide network provides efficient use of resources with minimal duplication, as well as the prospect of any false sense of diversity and redundancy, that can be obtained with separately planned and administered duplicative backbone infrastructures. Efficient design of this network would include utilizing leased transport services and elements of competing commercial carriers (both wireline and potentially satellite), with proper network architecture assuring appropriate QoS and reliability (inclusive of redundancy and diversity). Depending on the particular existing backhaul architectures of pre-existing public safety LTE networks, this national backbone network could also incorporate tangential backbone extensions of network

[3] Depending on eligibility restrictions and other considerations, this expanded user base may be upwards of 10 to 20 million users, including first responders (police, fire, EMT), National Incident Management Systems (NIMS) users, National Response Framework users, National Security/Emergency Preparedness (NS/EP) users, Federal Agencies with public safety responsibilities (investigation, asset protection missions, transportation, border control, or anyone with Continuity of Operations (COOP) roles, critical infrastructure owners/operators/decision makers, key state/regional/municipal leaders and decision makers, public health organizations, and key public services (sanitation, snow removal, etc.).

assets owned by regional, state and local governments if cost-effective to do so, provided these elements meet the needs and standards of, and can be sufficiently managed by, the national backbone network.

Driven by the realities of governance, funding mechanisms, pre-existing buildouts and institutional and jurisdictional issues associated with public safety, the nationwide public safety network will be a virtual amalgam of multiple networks.

Regional or Tribal Network Characteristics (¶ 19)

As set forth in more detail below, Telcordia generally agrees with the Commission's list of common characteristics that regional LTE networks must "support and maintain."[4] Many of these characteristics are vital to proper function and interoperability of the entire national network, such as network identification schema, roaming, QoS, priority access and security, and thus ideally are centrally managed by the national network. Telcordia believes the Commission's use of "[s]upport of"[5] should mean that the regional networks will enable and not hinder these functions emanating from and managed at the national level. "Support of" should not be understood to mean that the regional networks can or will originate and administer these functions independently. In addition, we note that testing and verification of interoperability might also be most efficiently and reliably administered at the national level, rather than by user agencies of regional network operators.

Roaming Authentication and Internetworking Functions (¶ 21)

Telcordia agrees that roamers must be authenticated and proposes the establishment of third party clearinghouse(s) to perform the following two sets of key functions:

[4] FNPRM, 26 FCC Rcd at 741 (¶19).
[5] *Id*.

(1) Roaming clearinghouse functions, which include real-time authentication, authorization and accounting (AAA), non-real-time clearing, settlement, and fraud management for users roaming in visited regional/tribal networks. The roaming clearinghouse functions are designed to be policy driven so that they can adapt to different or changing roaming agreements (for inbound and outbound roaming) among the regional/tribal networks as well as potential extensions into roaming between regional/tribal public safety networks and commercial 700 MHz LTE networks;

(2) Shared resource functions, which include directory services for common services/applications as well as the hosting of the common services/applications among regional/tribal networks. The technical specifications for the shareable common services/applications need to be determined and evaluated for impacts in the following areas: capacity, scalability, performance, reliability, security, priority access, and peering with required QoS across networks. The FCC should consider incorporating the results of these analyses into their guiding principles.

Nationwide Backbone Network (¶ 22)

For cost consideration and timely deployment, Telcordia strongly encourages the leveraging of commercial networks (which are robust with significant capacity) to support nationwide backbone networking and to support the end-to-end interoperable connections traversing the nation. A core set of appropriate Service Level Agreements (SLAs) should be established for various levels of services and applications to ensure that consistency in reliability, availability and QoS is maintained as part of the nationwide network. We believe that in times of national crisis the public safety backbone and the commercial network backbones will be congested if not architected properly. Hence, it is important to consider priority access protocols

(for users, applications and services) and their consistent implementation across the public safety networks to allow mission critical functions to be accomplished.

Nationwide Services and Capabilities (¶ 23)

Telcordia believes that the "services, applications and capabilities" the Commission recognizes as essential for supporting "nationwide interoperability" must be accomplished both through "a set of national core capabilities" *and* "locally through capabilities offered by regional or tribal networks."[6] Greater commonality can be driven, and efficiencies gained, by the national network providing a core suite of mainstream services and capabilities available to public safety agencies and its users (footnote 4), such as voice features, messaging and location services. This should include the availability of some common, widely-used categories of applications, such as e-mail, which agencies can choose to implement versus their own hosting and administration of the same.

At the same time, inasmuch as the public safety community is a federation of numerous entities each essentially operating their own IT enterprises with a variety of particularized management and operations applications, the national network must be able to support nationwide access and connectivity to such localized enterprise applications, provided they meet basic compatibility/interoperability standards to be determined. Consideration must be given to assigning access priorities of such applications, as discussed above regarding the Nationwide Backbone.

For optimal functionality, reliability and security, Telcordia believes that authentication and directory services can and should be provided exclusively by the nationwide network. In the commercial wireless world, clearinghouses generally fulfill the functions of network AAA, and

[6] *Id*. at 742 (¶23).

clearing and settlement between networks in different administration domains. Based on Telcordia's many years of experience designing and operating clearinghouses, we urge the Commission to adopt this concept and operate these functions through a clearinghouse dedicated to supporting the nationwide public safety network. In addition to providing AAA and directory services, the clearinghouse is also well suited to providing other functions of national scope or common interest, such as testing and certification of devices, hosting and managing core applications, and even managing operation of the nationwide network itself.

Guiding Principles for Public Safety Broadband Network Architecture (¶ 25)

Telcordia believes that in order to support the vision of the national network it is important to establish guiding principles and a core set of requirements across a broad spectrum of areas that FCC has already provided. We believe that as a practical matter the public safety networks will leverage the already deployed LTE networks built by commercial service providers, state or tribal entities or other federal agencies. Hence, the FCC needs to provide guiding principles for sharing network resources with an emphasis on QoS, reliability, security, and priority access for users and applications. Guidelines for maintenance and restoration practices of the shared networks with zero downtime require special attention. Also, when multiple regional networks with eNodeBs share the same Evolved Packet Code (EPC) and/or Core Network, some multi-tenancy guidelines are needed for the shared resources operators to maintain the separation of administration domains among these networks.

Adopting a Common Architectural Framework (¶ 26)

In order to launch the vision of a national public safety broadband network in a consistent manner Telcordia believes it is important for the Federal Government to establish the network's fundamental rules, guiding principles, and governance structure. We believe that the

Commission's Emergency Response Interoperability Center Public Safety Advisory Committee (PSAC) should continue to play an important role to provide the overall oversight and guidance to ensure that the deployment of the network will achieve necessary requirements. However, at some point in the future when a commercial and interoperable eco-system of equipment vendors has been established, the role of maintaining and enhancing the framework should be transitioned to an industry body/consortia/forum. The membership of the industry entity should include all the public safety stakeholders. Transition to such a model would likely progress in phases where the transition occurs over multiple years. Telcordia encourages the FCC to develop the vision for such a plan with appropriate milestones and transition steps.

Open Standards and Adoption of Open Standards (¶¶ 27-28)

Telcordia strongly supports the FCC posture to have the public safety network built to open standards. We believe that the core set of open standards should include standards for key interfaces, services and application, and processes and procedures necessary to fulfill the vision of an interoperable public safety network. We believe that standards set at the appropriate level do not necessarily interfere with equipment vendors providing differentiators in their products. It is our expectation that once broadband technologies and related services are adopted by the public safety practitioners a lot of above baseline products and services (that are built on the set of open standards) will allow innovators to provide the necessary differentiators in the market place. This would result in an eco-system where the best products/services will be available at competitive prices. Public safety-specific detailed requirements that build on standards are also needed to specify public safety services and corresponding requirements in the handsets, LTE access networks and Core Networks.

Technology Platform and System Interfaces (¶ 29)

Telcordia proposes that FCC consider 3GPP Multimedia Priority Service (MPS), Policy and Charging Control (PCC), and IP Multimedia Subsystem (IMS) as pertinent specifications for additional capabilities within the LTE technology platform that the nationwide network should support (besides Evolved Universal Terrestrial Radio Access [E-UTRA], LTE, and EPC) in order to ensure interoperability. These are functions in the Core Network which interact with the EPC and the LTE platforms and that are needed for end-to-end public safety deployments.

To ensure interoperability of the public safety network, all LTE Releases subsequent to Release 8 must provide backward compatibility to Release 8, including the recently specified Release 10 which includes many new MPS capabilities. Telcordia proposes that the FCC consider moving the baseline forward to subsequent releases as the view of public safety capabilities matures. The FCC should propose a compliance matrix so that equipment vendors can demonstrate compliance to baseline standards, especially to the feature set needed for public safety interoperability in these standards. The Commission's Emergency Response Interoperability Center (ERIC) should maintain a mechanism that provides a detailed view of the compliance of specific equipment by releases and by key interoperability features.

Guidelines should also be set for how often the public safety operators need to upgrade the software. In the past the communications companies have used the policy of upgrading when they are no more than two releases behind. The upgrade timeframes need to take into consideration backward compatibility issues as well as available funding.

Roaming Configurations (¶¶ 35-36)

Telcordia supports the FCC's conclusion that waiver recipients support both home-routed and local breakout roaming configurations. There should be a consistency between the priority

definitions and levels of priority between the public safety network and critical command and control access, such as National Security/Emergency Preparedness (NS/EP) priority services on the commercial networks, and potentially for access needs for Enduring Constitutional Government, National Guard, Red Cross or other such user groups with urgent network access needs.

Roaming Authentication and Internetworking Functions (¶ 37)

Telcordia supports the FCC's tentative conclusion that authentication for roamers is a function best performed by third party clearinghouses. Third party clearinghouses are well positioned to provide device registry, security and interconnectivity/peering functions. Public safety networks should leverage this ability of commercial third party clearinghouses to gain efficiency and cost effectiveness in its operations. As with other Telcordia filings with the Commission for various clearinghouse functions, Telcordia supports a multi-vendor approach to such clearinghouses. The Commission has found in several proceedings that having multiple vendors for clearinghouse type functions provides for significant competitive benefits. Most recently the OET, for example, conditionally named nine vendors (including Telcordia) as TV bands (white spaces) device database administrators and ordered the vendors to interoperate.[7] The FCC should consider using a similar procedure here, naming one or more clearinghouses for the various functions to be performed; viz., authentication, interconnectivity/peering, device registry and charging.

[7] TV White Spaces Order, 26 FCC Rcd at 555, 556, 559; *Second Report and Order and Memorandum Opinion and Order*, in ET Docket No. 04-186, 23 FCC Rcd 16807 (2008) (¶222).

The clearinghouses could propose their business models in response to either a formal solicitation or a public notice as was done by the OET in the TV Bands proceeding.[8] The authorized clearinghouses would have a defined function and should be required to be tested/approved before beginning service and seeking customers. This would give the Public Safety community a competitive choice of clearing house vendors that compete on platform, services and price.

The authentication mechanisms for roaming will depend on the authentication mechanisms required within any jurisdiction. As noted above, Telcordia supports the use of open standards for the provision of services whenever possible including those for AAA functions.

Interconnectivity of Regional/Tribal Networks (¶¶ 38-42)

Telcordia supports the establishment of a clearinghouse(s) to manage the interconnectivity links. The selection of the third party clearinghouse(s) could be done by competitive bid and follow the model discussed above for Roaming Authentication and Internetworking Functions.

As for the other interconnection options, Telcordia suggests that the Internet should NOT be used as a vehicle to interconnect between components of the national public safety network. The Internet is a Best Effort network with inadequate reliability and security capabilities for public safety especially during emergency events.

Prioritization and Quality of Service (¶¶ 43-46)

The FNPRM provides a good explanation of the differentiation between priority access (when connecting to the network) and QoS (assigned class of service once the user connects to

[8] *See Public Notice*, "Office of Engineering and Technology Invites Proposals from Entities Seeking to be Designated TV Band Device Database Managers," 24 FCC Rcd 14136 (2009).

the network).[9] Telcordia believes that there is much work to be done by the FCC and partner agencies in defining the priority access levels and the governance structure to promote consistent implementation by the operators of public safety networks and by commercial network operators when users may roam across networks.

The NPRM cites an excellent example where priority treatment and QoS may be independently assigned to users whereby a user is allowed entry into the network at times of network congestion due to his/her "high" priority access privileges.[10] However, the same user may not get access to an application because of the QoS class assigned to the user. Telcordia encourages the FCC to develop detailed guidelines on QoS and priority access treatment in the network and when roaming to other public safety and commercial networks. These guidelines should be revisited periodically to accommodate the availability of new services and applications.

Specifically, for LTE priority mechanisms Telcordia supports the use of Allocation Retention Priority (ARP), QoS Class Identifier (QCI), and Access Class Barring (ACB) as specified in 3GPP LTE. However, unlike the public telecom network where pre-emption is not implemented for voice calls, the ARP capability allows some bearers such as guaranteed bit rate (GBR) to preempt non-GBR services. In the public safety dedicated network, the capability of enabling pre-emption of low priority calls by high priority calls is required.

Mobility and Handover (¶¶ 47-50)

Telcordia agrees with the FCC's conclusion that the LTE based public safety broadband network must support seamless handover within and across coverage regions.[11] However, the

[9] FNPRM, 26 FCC Rcd at 746-47 (¶¶ 43-46).
[10] *Id*. at 747 (¶ 45).
[11] *Id*. at 747 (¶ 47).

definition of smooth and seamless handovers needs further clarification.[12] Telcordia believes the FCC needs to support a minimum performance requirement for mobility and seamless handover while within or across a local, regional or tribal network. The handover performance specification should be defined based on public safety requirements and within the performance range achievable by the 3GPP LTE/EPC standards. For example, X2-based handover would be more efficient, but links between eNodeBs is an additional expense. Indirect handover via the core (S1-based) will be applicable in some cases, and must be further evaluated.

Applications (¶¶ 55-57)

In general Telcordia supports the FCC's tentative conclusion on adopting a common set of applications including the interoperability with Land Mobile radio and PSTN voice. [13] Interoperability should also be required with the NGN Priority Services in the public commercial NGNs, as specified by the National Communications System (NCS). Mission critical voice will be transported over the non-LTE based networks for some time in the near future. Hence, we encourage the FCC to develop guidelines for gateway functionality across wireline and legacy wireless technologies to provide interoperability with the public safety broadband network. The guidelines must address interoperability from the perspective of priority access, performance, reliability and security. A complementary governance structure that ensures consistent implementation by public safety network operators must be established.

Interconnection with Legacy Public Safety Networks (¶ 58)

To enable a device designed for a legacy network (in multiple bands) to work in a 700 MHz public safety broadband coverage area, software-defined-radio base stations and gateways

[12] *Id*. (¶ 47, 49-50).
[13] *Id*. at 749-50 (¶¶ 55-56).

are needed to convert the wireless signal and data over the air from the legacy device to the EPC of the 700 MHz public safety broadband network and vice versa.

Telcordia suggests that focus groups within public safety standards bodies working in conjunction with the PSAC should develop interconnection guidelines between public safety and legacy networks.

Performance (¶¶ 59-62)

Telcordia supports the establishment of formal procedures for certification of network performance (*i.e.*, measured data rates) and suggests re-certification periodically after Initial Operating Capability (IOC). A set of key performance metrics for public safety broadband networks should be developed. These metrics should be measureable, testable (before deployment), and tunable (after deployment).

Security and Encryption (¶¶ 65-69)

Telcordia supports the FCC's tentative conclusion that all three security features for network access, as specified in 3GPP TS 33.401 should be required.[14] The security functions should include integrity protection and verification of data, ciphering/deciphering of data, and security for meta/operational data. Additionally, Telcordia suggests that the FCC establish requirements for a minimum set of network domain security features as well as features for visibility and configurability of security.[15] Telcordia strongly suggests that security requirements be assessed on an end-to-end basis including the full suite of devices, networks, services and applications.

[14] *Id*. at 752-53 (¶¶ 65-66).

[15] In addition to protecting the network from threats originating both externally and internally, security and access control must also protect the communications of a particular user group from unnecessary access by other user groups.

Robustness and Hardening (¶ 70)

Telcordia suggests that the FCC establish the requirement of at least 24 hours of back-up power at each eNodeB site within a public safety broadband network. Compliance with the backup power requirement should be determined by self-attestations filed with the Commission. Each network operator should certify within 30 days of its service availability that its eNodeB sites are capable of achieving the backup power requirement.

Telcordia's NEBS (Network Equipment – Building System) SR3580/GR-63-CORE/GR-1089-CORE)[16] testing requirements can be used as a basis for testing the robustness and hardening of public safety broadband network equipment. The NEBS requirements specify testing criteria for personnel safety, protection of property, and operational continuity in the presence of natural disasters such as earthquakes and thunder storms, and for physical and electrical protection.

<u>Public Safety Roaming on Public Safety Broadband Networks</u>

Public Safety Roaming on Public Safety Broadband Networks (¶¶ 85-89)

Telcordia proposes that the admittance of roamers should depend on user priority particularly during network overload conditions. In addition, intra-system roaming is important for many Public Safety personnel who have a national concern or have to help out in another jurisdiction during an emergency. As noted above, Telcordia supports the proposal that third party clearinghouses could be leveraged to support this function.

[16] Telcordia, under its previous name Bellcore, created this U.S. industry standard.

Prioritization and Quality of Services to Support Roaming (¶¶ 90-92)

Telcordia proposes the use of third party clearinghouse(s) to support call setup for support of roaming of Public Safety devices. The priority mechanisms and setup process will depend on the priority and access policy used by the visited region/jurisdiction.

To ensure interoperability, Telcordia suggests the establishment of a nationwide agreement on call priority levels such that these priorities will be honored in all public safety networks.

<u>Testing and Verification to Ensure Interoperability</u>

Conformance Testing (¶¶ 106-108)

Telcordia supports the FCC's requirement on performing conformance testing on every user device to ensure compliance to 3GPP LTE Release 8 and higher standards. We propose that the FCC consider adding "for every release without exception" to the requirement. Based on our experience in testing and certification of user devices for the telecommunications market we note that any change in the hardware, firmware or software of the device could potentially create a problem with the previously functioning features. Telcordia believes that conformance testing performed by certified independent commercial test laboratories should be encouraged. The certified test labs have a significant competencies and expertise to provide service in this area. The PTCRB[17] has the appropriate administrative structure in place to support the needs of the public safety networks and should be leveraged for authorization of laboratories and certification of public safety user devices.

Major commercial network providers have extensive lab testing infrastructures to test equipment that is deployed in their network. They have rigorous testing programs that include

[17] PTCRB is the independent organization that provides the evaluation process for GSM/UMTS Type Certification for mobile network operators. *See* FNPRM, 26 FCC Rcd at 762-63, 762 n. 109 (¶¶ 107-108).

compliance testing, pair-wise interoperating, integration testing, solution testing, network readiness testing, first office application testing and acceptance testing in the field on a per site basis. For LTE infrastructure equipment every component of the network is subject to all the phases of a test program. The testing in each phase is very comprehensive to include testing in the following areas: protocol, feature/functionality, performance, reliability, security, billing/usage and operations and maintenance. Telcordia believes that the LTE infrastructure equipment for public safety networks should undergo similar levels testing and certification.

A commercial network provider may choose to deploy infrastructure equipment from only two or three infrastructure equipment providers. Hence, they can target their testing programs to ensure interoperability among a small set of vendors. This may not be the case for the public safety network, since any infrastructure equipment provider could offer their equipment for testing and certification to be deployed in the public safety networks. This will certainly increase the complexity of in the administration and operation of a certification program.

Telcordia believes that to support the goal of an interoperable public safety network every component of the network must be subject to a conformance certification process. Any equipment non-conformance could create potential problems in the field when the public safety practitioners are providing life saving services. This risk, coupled with the fact that some of the public safety network operators will not have the resources to invest in test programs and must rely on a central administration for the certification process, makes it imperative that the FCC create a certification requirement for LTE infrastructure equipment.

The FCC should provide consideration for different business and operation models for the certification labs for LTE infrastructure equipment. The FCC should continue to leverage the work being performed at the Department of Commerce Public Safety Communications Research

(PSCR) program and their test infrastructure for proof of concept and early deployments. As the program grows the FCC should consider broadening the program in which the ERIC could take a larger role in the certification process by performing testing, being the central administrator and providing the oversight for a certification program, developing a public-private partnership to leverage the certification and testing in commercial network operator's commercial labs.

In the near term a practical approach would be for the ERIC in partnership with NIST to provide the central administration for the certification process. Open competitive bids for certification labs to participate in the program should be considered. As part of the central administration and oversight function, the ERIC would maintain the guidelines for the certification program and use the PSAC for periodic review of the programs.

Interoperability Testing (¶¶ 109-115)

Based on our experience in providing conformance testing, interoperability testing (IOT) and integration testing for the telecommunications industry we strongly believe that IOT is essential to ensure that the end-to-end services and applications perform as intended to by design. Additionally, for the public safety networks to provide the services that are needed by the public safety practitioners in times of crises we believe that self-certification provided by the equipment vendors needs to be augmented by formal certification performed by an independent organization. The current work being performed under the Public Safety Research Program (PSCR) should be leveraged to build and expand the base of the certification test facilities.

Many commercial test facilities, including Telcordia, have extensive test bed infrastructures, test tools, testing competencies and experience in running certification programs for the telecommunication industry that should be leveraged. Incremental, moderate investments will be required to get the infrastructures to support IOT for public safety networks. The

commercial certification clearinghouses could work with the FCC to leverage the work done by the government and define the appropriate certification programs and business models to promote a self-sustaining eco-system for the public safety networks.

Interoperability Verification (¶ 116)

In addition to conformance testing and IOT, the commercial telecommunication industry uses several important additional testing and verification steps to reduce risk and provide the necessary high confidence that equipment and solutions will operate properly when deployed in the field.

These additional testing/verification steps include:

- Solution testing, also referred to as network readiness testing: This is comprehensive end-to-end testing of the solution with new or enhanced network components from a user perspective. Every aspect of the service is addressed in the testing, including provisioning of the user device and network components, features and functionality in the presence of back up traffic, exercising the maintenance capabilities for both sunny day and rainy day scenarios, reliability, security, and also service restoration in the event a problem is identified.
- First office application: This testing consists of "soaking" the solution at a single site or for friendly users for an extended period of time (a week or month, say) to assess the performance over a relatively long period of time. All aspects of the features are exercised to identify any outstanding issues that might appear only after repeated use in the field or as an interaction with other capabilities and circumstances that occur seldom or under limited configurations.

- Period solution regression testing: This consists of testing over pre-defined intervals of time for solutions that were deployed earlier and are expected to continue to function properly in the field. The scope and duration of the testing and verification is influenced by the nature of capabilities that are being tested.

Telcordia encourages the FCC to take into consideration these additional test phases as they define the overall testing and verification program for the nationwide public safety network. These testing activities lend themselves readily to 3rd party testing houses that perform audit testing to ensure that services and applications are performing as designed and needed in the field. Given the complexity of the public safety network environment, diverse operators, and multi-vendor infrastructure, we believe that adding these additional testing steps will provide significant benefits.

Other Matters Relevant to Interoperability on Public Safety Broadband Networks

Network Operations, Administration and Maintenance (¶ 117)

Telcordia agrees with the Commission that network operations, administration and management (OA&M) is fundamental and critical to the operation and maintenance of all public safety services. A set of basic OA&M service capabilities should be adopted nationwide.

In-Building Communications (¶¶ 123-126)

While Distributed Antenna Systems are important for in-building communications, Telcordia expects the future wide spread deployment of femtocell and picocell technologies will have a greater impact on in-building wireless. These small cell technologies substantially improve in-building coverage and performance at affordable cost. The LTE standards support femtocells and will evolve to support other microcell technology. There are some important

open issues such as planning, deployment and management of an LTE network with both macro and femtocells so as to avoid interference from femtocells that could cause coverage holes in the macrocells. Interference risks are impacted by the large power disparity between the macro and femtocells and the generally unplanned locations of femtocells.

For public safety, there are some policy and technical issues associated with femtocells, which can be provisioned to support only users in a closed subscriber group (CSG). When a first responder enters a building under terrorist attacks, he needs to gain access to the CSG-provisioned femtocell in the building even though he is not in the CSG. Enhancements are needed to current standards so that a public safety user's device can be authenticated and authorized to connect to the femtocell in that building.

Public Safety Broadband and Next-Generation 911 Networks (¶ 133)

Regional/tribal public safety networks must interface with NG911 networks through the IP-based Emergency Services IP Network (ESInet) and Public Safety Answering Points (PSAPs) for dispatch calls and transferring information, such as caller location and call back.[18] Interoperability analysis and testing for key interfaces (*e.g.*, call routing and control) between NG911 and public safety LTE networks are critical.

As with NG911, Telcordia suggests FCC oversight to address potential data overload of end systems and users during normal and major national emergencies conditions. Some policy and technical issues related to priority access and resource control for 911 calls, inter-public-safety-personnel calls, and NS/EP calls need to be clarified and resolved.

[18] The networks also will have to function via the PSAPs with the legacy circuit-switched E911 networks throughout the nation as they evolve to NG911.

CONCLUSION

Telcordia urges the FCC to consider our comments and recommendations as set forth above. In adopting these recommendations, we believe that the Commission can specify the architecture necessary to create a nationwide, interoperable, broadband wireless network in the 700 MHz band that will provide public safety users with access to wireless broadband capabilities that will improve their effectiveness and enable them to communicate effectively across departments and jurisdictions nationwide.

Respectfully submitted,

TELCORDIA

By: _____

Brenton C. Greene, President
Advanced Technology Solutions
TELCORDIA
One Telcordia Drive
Piscataway, New Jersey 08854
(732) 699-8013

April 11, 2011