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

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
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100

To: The Commission

COMMENTS OF THE

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association (TIA) hereby submits comments to the Federal Communications Commission (Commission) in the above-captioned proceeding.[1] TIA appreciates the opportunity to provide technical input on the structure of a nationwide interoperable broadband public safety network.

TIA represents the global information and communications technology (ICT) industry through standards development, advocacy, tradeshows, business opportunities, market intelligence and world-wide environmental regulatory analysis. For over 80 years, TIA has enhanced the

[1] Service Rules for the 698-746, 747-762 and 777- 792 MHz Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, Amendment of Part 90 of the Commission's Rules, WT Docket No. 06-150, PS Docket No. 06-229, WP Docket No. 07-100, *Third Report and Order and Fourth FNPRM* (2011) (Third R&O and Fourth FNPRM).

business environment for broadband, mobile wireless, information technology, networks, cable, satellite, and unified communications. TIA is accredited by the American National Standards Institute (ANSI).

SUMMARY

TIA congratulates the Commission on the critical progress made toward the creation of a public safety nationwide broadband network. While TIA is a long-time supporter of the Commission's technology neutrality principle, and urges the adherence to this fundamental doctrine, TIA supports the Commission's conclusion to initially mandate LTE for use in the public safety nationwide broadband network, based on the unique circumstances. Moving forward, TIA recommends that the Commission adhere to its technology neutrality principle in all possible circumstances.

As LTE development occurs, LTE Releases 9 and 10 will incorporate improved voice and data capabilities that will improve public safety communications. However, TIA notes that the public safety community must first assess their specific needs, and ensure that capabilities adopted are appropriate given spectrum, financial, and other resource concerns. Capability-specific studies should be employed to effectuate this policy.

TIA believes that the Commission's concern regarding compatibility between LTE releases is valid. However, backward compatibility is built into every 3GPP release, and have been addressed in these standards. Further, with regard to IPv4 and IPv6 compatibility, transition mechanisms exist that can be used amongst network occupants to streamline interoperable communications. Therefore, the Commission need not adopt technical requirements to address this concern; however, to facilitate an efficient transition, the Commission should encourage new

networks to utilize IPv6, while allowing IPv4 networks adequate time to migrate their uses to IPv6.

TIA fully concurs with the Commission's conclusion that open standards will best support interoperability between devices and providers. The establishment of baseline standards that must be met for interoperability are critical, and will allow for network occupants to, if they choose to do so based on unique needs, exceed these baselines. Using an open standards- and market-based approach will ensure that investment and development in the 700 MHz nationwide public safety broadband network is not inhibited by lack of competition.

TIA further agrees with the Commission that all network occupants should be required to support home-routed roaming baseline configuration. Due to the characteristics of local breakout configuration TIA urges the Commission to carefully balance the benefits and harms of adopting this configuration as it progresses in this matter.

TIA believes that LTE will provide the needed level of prioritization and quality of service. TIA believes that, in LTE Release 8, a higher access class should be assigned to public safety in order to ensure that appropriate prioritization of service occurs when a public safety user roams onto a commercial network. The Commission is also encouraged to specify a quality of service framework across the entire network using the LTE Policy and Charging Rules Function due to the complexity of related policy rules and address resolution protocol parameters between networks across the country. If a unified standard framework is set in place, the proper prioritization for public safety traffic can be ensured.

As the Commission considers adopting policies related to handover issues, TIA urges for the Commission to maintain as flexible a policy as possible. While using X2 handovers will afford benefits such as less disruption for real-time handovers, S1 handovers are more beneficial for

interactions between inter-operator networks. For different situations, one or the other (or both) may be the most beneficial method(s) for handovers; therefore, TIA urges maximum flexibility in the selection of handover method.

While TIA supports the adoption of a requirement for support of particular applications to facilitate roaming across networks, the Commission is strongly encouraged to provide adequate definitions for each before finalizing related rules. While some are defined, TIA notes that a "status or information 'homepage'" is only defined at a high level, and practical use (and benefit) will only result from support of this application if more detail is provided in its definition. The Commission should also ensure that applications required to be supported be standardized towards ensuring support across the public safety broadband network.

Finally, TIA, in supporting the dire need to ensure that narrowband systems can interoperate with broadband systems in the network, urges the Commission to utilize LTE's Access Point Name technology. This technology is capable of incorporating legacy data networks, and thereby allows infrastructure and applications currently in use to be leveraged. TIA notes that physical equipment will be a necessity to effectuate gateways between legacy systems and LTE systems. Through the use of such means as an IP backbone, existing VoIP interfaces can interoperate with VoIP uses over LTE, valuable resources can be conserved, and interface standards supported. With adequate funding and operational plans, the integration of the existing P25 system into the public safety nationwide broadband network can be accomplished.

DISCUSSION

I. THE COMMISSION SHOULD, TO THE EXTENT POSSIBLE, CONTINUE ITS POLICY OF TECHNICAL NEUTRALITY AND FLEXIBILITY.

TIA has long supported the Commission's regulatory support for technology neutrality, and urges the Commission to embrace this policy to the extent feasible in the context of the nationwide interoperable public safety broadband network. TIA recognizes the reasonable conclusion of the Commission to mandate LTE for the public safety 700MHz broadband network, and applauds the Commission's recognition that this decision is not one made lightly and is a departure "from the Commission's traditional posture of technological neutrality, which we believe has served the public interest well [and] has led to robust competition and innovation to the benefit of consumers."[2]

TIA agrees with this position, and urges the Commission, as it finalizes the full complement of interoperability requirements, to take a minimalist regulatory approach in setting additional mandates. The focus of the Commission's requirements must be limited to achieving initial nationwide interoperability and should accommodate market flexibility in technology choice for future upgrades once the interoperability is achieved.

[2] *Id.* at ¶ 10.

II. FUTURE LTE RELEASES WILL HAVE ENHANCED VOICE AND OTHER CAPABILITIES WHICH SHOULD BE ASSESSED AS REQUIREMENTS FOR THE PUBLIC SAFETY NETWORK.

In its proposed "Architectural Guiding Principles," the Commission makes clear that, as LTE develops, both voice and data must be supported.[3] TIA agrees that the current capacity of LTE Release 8 to deliver data to first responders must be complemented by voice capacity in future LTE releases. LTE Release 9 has most of the requirements needed for voice capability, and some operators are making plans to deploy voice over LTE in Release 9. LTE Release 10 will add even more features that will improve on the voice capabilities of Release 9, and those will be further refined in Release 11. These new capabilities will facilitate emergency sessions and position location enhancements for requirements such as E911.

In addition to these enhancements, LTE Releases 9 and 10 contain important features that will improve communications operations for first responders. For example, Multimedia Broadcast and Multicast Services (MBMS) will be available, and control plane location services will supplement existing location technologies. However, before those new capabilities are adopted for public safety, the specific function must meet needs of first responders. Further, it must be determined that the selected capability is mature enough in both specifications and implementations and that deploying it represents a best use of spectrum, financial, and other resources. Moreover, it must be ascertained through sufficient testing that the capability meets reliability needs of public safety. Accordingly, the Commission should evaluate studies, specific to each new capability, before issuing regulations mandating support of the particular capability arising from LTE Release 9 and higher.

[3] *See id.* at ¶ 20.

III. BACKWARD COMPATIBILITY IS A REQUIREMENT OF EACH LTE RELEASE WHICH WILL MAINTAIN INTEROPERABILITY.

The Commission seeks comments on whether interoperability can be maintained if multiple 3GPP Releases are used within different networks.[4] Backward compatibility is a requirement of each 3GPP release; the specification development process in 3GPP ensures backward compatibility between communicating subsystems. During operations, information obtained via signaling and/or from configuration databases assures that all subsystems are capable of identifying the release level of other subsystems. That, combined with the ability of systems to handle errors gracefully, provides an additional layer of protection and interworking. Thus synchronizing LTE releases across disparate networks is not strictly necessary, as the integrity of those systems is not endangered by communications with systems using older or newer releases. Further, LTE Advanced will support enhanced data rates to support advanced services and applications. LTE Advanced will also include Carrier Aggregation for a proscribed set of bands.

IV. IPv6 IS NOT BACKWARD COMPATIBLE WITH IPv4, BUT IPv4 AND IPv6 CAN COEXIST IN THE SAME NETWORK.

The Commission inquires as to whether the use of both IPv4 and IPv6 in various components of the nationwide network creates obstacles to achieving interoperability.[5] TIA notes that IPv6 is not backwards-compatible. Thus, users with IPv4 addresses will not be able to access IPv6 services or communicate with IPv6 host, and vice versa, without the support of the appropriate transitions mechanisms that have been developed. However, these transition mechanisms,

[4] *See* Third R&O and Fourth FNPRM at ¶29.
[5] *See id.* at ¶ 30.

including dual-stack implementations, tunneling, and translation, allow existing IPv4 systems to co-exist and interoperate with IPv6 systems. Therefore, there is no need for a technical requirement that IPv6 should be used exclusively in the public safety network. Moreover, the transition from IPv4 to IPv6 for end user traffic will likely take a significant amount of time due the need to support, and ultimately migrate, legacy systems and services that are currently IPv4-based. While existing networks using IPv4 should be afforded this time, it is advisable for new networks to utilize IPv6 from the initial deployment

V. OPEN STANDARDS THAT ESTABLISH A REFERENCE ARCHITECTURE WILL ENSURE INTEROPERABILITY AND SPUR INNOVATION.

In the Fourth FNPRM, the Commission discusses the importance of utilizing open standards and explores possible dangers to interoperability associated with the use of devices and equipment that employ proprietary technologies.[6] Open standards are necessary to support interoperability between manufacturers and between device and infrastructure providers and to provide functionality related to policy control, QoS, charging, packet transport, network, security, and a host of other services. TIA also agrees with many stakeholders that the prudent application of open standards can attract investment and innovation and deliver economies of scale that can quickly drive prices of devices and infrastructure down, enabling more feature-rich services for the same amount of investment. However, the use of open standards must be carefully balanced to encourage innovation while still ensuring compliance with all standards necessary to ensure interoperability. Thus, open standards provide a reference architecture – a "tool box" of

[6] *See id.* at ¶ 28.

capabilities – and a functional foundation from which to implement market-specific product features.

VI. HOME-ROUTED ROAMING MUST BE A BASELINE CAPABILITY; THE COMMISION SHOULD CONSIDER LOCAL BREAKOUT.

The Commission proposes that all broadband public safety networks have the ability to support both home-routed and local breakout roaming.[7] TIA agrees that home-routed roaming should be required as a baseline roaming configuration, as this is a general-purpose configuration which can be used to support most, if not all, applications. Thus, while local breakout may be used for minimizing bearer path latencies, it is not needed for basic interoperable service. Local breakout is a special-purpose configuration that is designed to minimize bearer path latencies for certain applications. It requires agreements among roaming partners, such that well-known local breakout APN's are defined and configured in each network, for applications intended to use local breakout. Further, each network is required to support identical local breakout applications located in a separate and dedicated data network. As a result, a compromised or improperly implemented device can enable data routing between security domains, comprising the APN networks. Further, accessing applications from the visited system bypasses home agency proxies, firewalls, antivirus measures, home network logging, and activity tracking. As it evaluates requiring local breakout roaming, the Commission should balance these potential harms to the functionality of the network with the overall benefits local breakout roaming provides to first responders.

[7] *See id.* at ¶ 35.

VII. LTE WILL PROVIDE EFFECTIVE PRIORITIZATION AND QUALITY OF SERVICE.

The Commission inquires on how public safety broadband networks can and should support priority access and quality of service (QoS).[8] To enable Public Safety responder's timely connectivity to the broadband network there is a need to prioritize public safety user's initial access priority to the network. LTE Release 8 includes "Access Class Barring," a method to prevent congestion of the control channel at busy Evolved Node Bs (eNBs). Higher access classes (e.g., access class 14) should be reserved for public safety first responders. This will provide significant benefit if and when public safety LTE devices roam onto commercial carrier networks. For this to be effective, the appropriate access classes (e.g., access class 14) should be reserved for public safety usage on both commercial and public safety networks.

Further, a QoS priority framework needs to be specified that is deployed across the public safety broadband network. This framework utilizes LTE standards-based QoS attributes including QoS Class Identifier (QCI) and related parameters as well as address resolution protocol (ARP). The Public Safety broadband network should implement the LTE Policy and Charging Rules Function (PCRF) function. Complex QoS policy rules that vary between public land mobile networks (PLMNs) or across regions under a single PLMN may also be needed, requiring a PCRF. For these reasons, all public safety LTE deployments should include a PCRF. In addition, the nature of incidents may require priority of applications and devices to be modified in real-time for the incident. Public Safety's PCRF should provide QoS policy for responder devices (when at home or roaming). The public safety broadband network should utilize the LTE interface for signaling the needed QoS level. Once a request has been received by the LTE

[8] *See id.* at ¶ 35.

broadband network, there must be an admission control process by which the requested network resources are evaluated based on ARP parameters. The QoS priority framework defines a set of ARP values to enable priority admission for Public Safety responders. For the nationwide public safety system, standardization of the ARP value insures appropriate priority for public safety and insures LTE resources are available especially for life threatening situations.

VIII. THE COMMISSION SHOULD ALLOW FLEXIBILITY IN HANDOVER METHOD USE.

The Commission inquires as to the advantages and disadvantages of X2 handover and those of S1 handover.[9] Both X2 and S1 handovers can be used simultaneously. X2 handovers have the advantage of not losing data buffered in the eNodeB while performing the handover. X2 handovers also mandate S1 relocation, both S1-MME and S1-U. The Commission also inquires whether it should require one method and not the other, or both.[10] This decision will depend on the application; for absolute real-time handovers, X2 handovers have the advantage of less disruption. However, S1 handovers will be effective for most handover scenarios. TIA notes that X2 handover will likely be the most common method for intra-vendor links, while S1 handover will likely be the most common method used for inter-operator links. Accordingly, it may not be necessary to specify the handover method required. Both X2 and S1 handovers have use in certain deployment scenarios, yet some deployments may not require both types. Further, there may be future handover types which will be better suited for future deployments. The Commission should allow flexibility in selecting the handover methods – current and future – best suited in different scenarios.

[9] *See id.* at ¶ 35.
[10] *See id.*

IX. THE PROPOSED APPLICATIONS, IF PROPERLY DEFINED, ARE BASELINE REQUIREMENTS FOR INTEROPERABILITY.

The Commission seeks comment on the need to require the network to support the following applications to facilitate roaming across public safety broadband networks: [11]

1. Internet access;
2. Virtual Private Network (VPN) access to any authorized site and to home networks;
3. A status or information "homepage;"
4. Provision of network access for users under the Incident Command System (ICS); and
5. Field-based server applications.

TIA agrees with the Commission that support for the five listed applications is the minimum requirement for roamers, provided that each are clearly defined. Some of these applications, such as Internet access or agency-controlled VPN access, are already well understood. However, others, such as the status or information "homepage," are not defined beyond high-level requirements, and will not support interoperability until the necessary definitions are developed. The roaming framework (multiple networks) or home access (single network) allows all authorized users under the ICS to have network access provisioned, while the status page can be used to facilitate inter-agency communication. Field-based server applications connectivity using public IP space is well understood, but a framework to enable authentication and authorization to use any applications, for either home or visiting users, still needs to be defined.

Beyond these, for any additional application(s) to be adopted, the application has to have been standardized. Adoption of the application matters to the broadband public safety system if the

[11] *See id.* at ¶ 55.

application places a new transport requirement on the network that the network is currently not capable of handling. Adoption of the application also matters if the service is intended to be partially or fully served by the visited network in a roaming scenario. It is not clear that any applications beyond the defined set are standardized and ready for adoption.

X. WITH PROPER GUIDELINES, INTERCONNECTION WITH LEGACY SYSTEMS CAN BE FACILITATED THROUGH LTE AND NARROWBAND STANDARDS.

TIA agrees with the Commission that it is vital that broadband networks interconnect with narrowband networks to enable public safety agencies to better integrate their communications and prevent sunk costs.[12] Today, public safety agencies have defined private data networks for their legacy state/local data applications. In many cases, public safety agencies also incorporate multicast virtual private network ((M)VPN) technologies in these data networks. Existing data applications, such as Computer Aided Dispatch and local fixed video, can benefit from the advantages of throughput, redundancy, and enhanced coverage provided by LTE. By utilizing LTE's standard Access Point Name (APN) technology, an LTE device can support a legacy "agency APN" which enables routing traffic between the device and the agency's legacy data network. LTE devices can utilize these same legacy agency APN's. This will allow an LTE device to integrate with existing public safety data networks and applications. This strategy also allows an agency to leverage their existing IT infrastructure and applications. To achieve this, guidelines should be established which allow a local agency to:

[12] *See id.*

1. Create and associate an LTE APN to the agency's existing IP space and promote this APN in national DNS applications and the roaming transport service;
2. Associate LTE QoS policy (PCC rules) with existing agency applications within the confines of the national QoS framework; and
3. Limit transport costs associated with deploying legacy data applications by enabling regional and tribal networks to deploy localized PGW/SGW elements and associated IP transport equipment

Regarding gateways between existing public safety networks and Public Safety Spectrum Trust (PSST) LTE, physical equipment will be necessary to provide security and interworking between the agency's legacy data network and the LTE system. It will be possible for the gateways to support both voice and data applications. For example, by leveraging a national IP backbone, an existing agency VoIP private branch exchange (PBX) could interface with a peer agency VoIP PBX in another LTE tribal area, saving the agencies public switched telephone network (PSTN) costs. Many gateways with such capabilities are readily available in industry. Much of the interoperable capabilities in this question require a nationwide IP backbone. This nationwide IP backbone can also support an agency's TIA standard TIA-102.BACA-A (a.k.a. ISSI) interface to another agency on the backbone. This will help facilitate the interconnection of P25 systems. This should be emphasized and established as soon as practical. Once this is in place, data and voice interoperability scenarios will be substantially enabled. A funding and operational plan needs to be created for the deployment and sustainability of this nationwide network.

CONCLUSION

For the foregoing reasons, TIA urges the Commission to take into consideration its views in this proceeding.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: ___/s/_____

Danielle Coffey
Vice President,
Government Affairs

Patrick Sullivan
Director,
Technical and Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

April 11, 2011