



Emergency Response Interoperability Center

Public Safety Advisory Committee (PSAC)

Considerations and Recommendations for Interoperability of Public Safety Broadband

Interoperability Work Group Subcommittee Report

May 24, 2011

Acknowledgements

The following individuals contributed to the creation of this report:

Jacqueline Miller, State of New Mexico, (Chair)

Douglas Aiken, International Municipal Signal Association, (Co-Chair)

Ajit Kahaduwe Nokia Siemens Networks, (Vice Chair)

Mike Beckstrand, CalEMA

Steven Cumoletti, NYS

Brian Fontes, NENA

Mark Grubb, Delaware

Kenneth Hughes, New Orleans

Ray Lehr, NGA

Vonya McCann, Sprint Nextel

Harlin McEwen, IACP

Byron Neal, Syniverse

Robert Nelson, Intra-Tribal Council of California

Steve Noel, OR

Art Prest, RTG

Roger Quayle, IP Wireless

Michael Simpson, Texas DPS

Terry Sult, Sandy Springs PD

Charles Werner, SAFECOM

Table of Contents

1	Executive Summary.....	5
1.1	Introduction.....	6
2	Charter and Approach.....	6
2.1	Charter	6
2.2	Approach.....	6
3	Governance Assumptions	7
3.1	FCC.....	7
3.2	Governance Body	8
4	Technical Rules for Public Safety Broadband Networks	8
4.1	Open Standards	8
4.2	Technology Platform and System Interfaces	9
4.3	System Identifiers	10
4.4	Roaming Configurations and Authentication and Interworking Functions	10
4.5	Interconnectivity of Regional or Tribal Broadband Networks	11
4.6	Performance and Quality of Service	11
4.7	Mobility and Handover.....	11
4.8	Out of Band Emissions	12
4.9	Applications.....	12
4.10	Interconnection with Legacy Public Safety Networks.....	12
4.11	Performance and Network Capacity	12
4.12	Security and Encryption	13
4.13	Robustness and Hardening.....	13
4.14	Coverage Requirements and Reliability	13
4.15	Interference Coordination	14
4.16	Incumbent Narrowband Operations.....	14

5	Public Safety Roaming on Public Safety System Broadband Networks	14
5.1	Prioritization and Quality of Service to Support Roaming.....	15
5.2	Applications to Be Supported for Roamers	15
5.3	Public Safety-to-Public Safety Roaming Rates, Volume of Roaming Traffic, and Proposed Model Agreement	15
6	Testing and Verification to Ensure Interoperability	15
7	Other Matters Relevant to Interoperability on Public Safety Broadband Networks.....	16
7.1	Network Operations, Administration and Maintenance	16
7.2	Reporting on Network Deployment.....	16
7.3	Devices	16
7.4	In-Building Communications	17
7.5	Deployable Assets	17
7.6	Operation of Fixed Stations and Complementary Use of Fixed Broadband Spectrum	17
7.7	Compliance with the Commissions Environmental Regulations.....	17
7.8	Public Safety Broadband and Next Generation 911 Networks.....	18

1 Executive Summary

The Interoperability Working Group (IWG) of the Public Safety Advisory Committee (PSAC) to the Emergency Response Interoperability Center (ERIC) has developed this report to identify and discuss issues related to the interoperability of the nationwide public safety broadband network initiative.

There are significant benefits in beginning this discussion of the issues at the inception of the network and during the planning phase. The difficulties arise when we begin to discuss options and variables that are still being defined. The report is structured to allow for quick reference back to the *Fourth Further Notice of Proposed Rulemaking*¹ that focuses on the technical and interoperable aspects of the development and implementation of an effective, efficient and sustainable public safety broadband network nationwide.

In the IWG discussion of the technical rules for the public safety broadband network, several topics came to the forefront that needed to be addressed in a certain order. The development of a national architecture based on open standards and determining the interfaces and identifiers will impact the way other issues are addressed. For example, roaming cannot be determined without first knowing how the networks will be structured. In discussion, the term roaming begged for clarification. This document maintains roaming as it is known to be today in the commercial wireless environment and defines the movement of public safety users and/or LTE enabled equipment outside of their area of normal operation as transient operations. Each of the technical components is addressed in the document identifying the items that are within the scope of the interoperability working group.

Interoperability is the concept that supports and enables public safety broadband users to move around the nationwide network with a design that minimizes roaming issues (and costs) and provides robust, reliable service to all regions. The actual need for roaming and roaming agreements will depend on network architecture. Prioritization and quality of service should be determined through technical and operational procedures developed at the network administrator level within the network architecture and governance rules. Public safety users will need access to their home networks and applications specific to their organization but also will need access to nationwide network applications. Additionally, a basic set of requirements will need to be determined to assure that applications are supportable, secure and reliable.

The existing recommendation of LTE as the technology solution for the nationwide public safety broadband network is the baseline for development of standards and testing for hardware to assure we are meeting the needs and expectations of the user community. While existing testing in the commercial wireless environment exists, it needs to be modified to address the needs and requirements of the public safety environment. Quality of service, performance and prioritization will require some additional testing requirements. Assuring open interfaces and interoperable hardware will need to be addressed but may be at a lower level. We need to learn from our challenges in land mobile radio to assure that interoperability is not only recommended, but also measurable and tested.

¹ See Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket 06-229, *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, 26 FCC Rcd 733 (2011) (*Third Report and Order* and *Fourth FNPRM*, respectively).

Administration and operations of networks should remain the responsibility of the implementing organization within the confines of a nationwide and local governance structure to assure a minimum standard of performance and support. Some local or regional systems will be more robust and may have added features; however, the maintenance of a basic service offering should be the focus of the nationwide governance structure. Many variables that are outside the scope of the Interoperability working group and even the PSAC will impact current and future recommendations. We remain diligent and dedicated to the ongoing process of supporting the development of the deployment and operation of a nationwide interoperable public safety broadband network. This report reflects the views of the membership with the understanding that there are many variables and decisions out of scope that may change recommendations.

1.1 Introduction

An important element of the FCC's policies surrounding development of a nationwide public safety broadband network is establishment of a framework that will enable public safety officials to leverage the technological advancements that regularly occur in the wireless industry. The FCC, in choosing Long Term Evolution (LTE) from the Third Generation Partnership Project (3GPP), establishes an interoperability framework which leverages a global ecosystem of infrastructure and devices along with commercial wireless.

By choosing LTE and its associated network technology, Public Safety systems should be able to stay at the forefront of technology trends and have the ability to incorporate features which are found on commercial networks.

2 Charter and Approach

2.1 Charter

The mission of the Interoperability Working Group is to develop and provide interoperability recommendations for the Public Safety broadband network to assure that first responders nationwide have the ability to take advantage of evolving technologies to support their mission.

Interoperability is imperative to a successful implementation of a Nationwide Public Safety Broadband Network. In partnership with all working groups derived from the PSAC, the Interoperability Working Group will work towards identifying issues and areas of focus that will support interoperability and develop guiding principles for implementing interoperable networks. Risks to successful interoperability implementation will be noted and a mitigation plan will be recommended. The Interoperability Working Group includes a goal to provide a recommendation to advocate minimum standards and partnerships with commercial service providers to maximize usage and coverage. Consideration for solutions to assure new systems are interoperable with legacy public safety networks will be provided as the architecture is more clearly defined.

2.2 Approach

In the effort to answer the short term question below, the Interoperability Working Group will evaluate topics from the *Fourth Further Notice of Proposed Rulemaking*.

- **What rules or policies must be implemented to ensure that public safety broadband networks are interoperable with other public safety networks, (both narrowband networks and broadband networks)?**

For the following topics the working group will discuss the need to develop policies and/or rules by the FCC or if is better to wait until the nationwide governance, network structure and funding are known. The discussion of the need for rule or policy development is the basis for the recommendations the group has submitted to the full PSAC for review and discussion.

The Interoperability WG will identify whether or not the working group should provide comment or recommendation using a four level scope classification to the discussion topics in the *Fourth Further Notice of Proposed Rulemaking*:

- WG – Item to be addressed by WG (something the I WG and FCC should be involved in)
- NetAd – Area left to whatever Network Administration is established (not be addressed by FCC) at the national level
- NetLo – Item which should be left to individual network (not to be addressed by FCC) at the local level
- NetAd/NetLo – NetAD and NetLO coordinate on items which effect the network

Funding has a significant impact at all levels to interoperability and to the breadth and depth achievable in Public Safety systems. With the uncertainty of the funding source, amount, and timing the recommendations by the Interoperability WG made recommendations where the NetAd or NetLo funding levels will be determined outside of this working group.

3 Governance Assumptions

The discussion of governance is ever-present as we discuss not only interoperability, but also every aspect of the implementation of the Nationwide Public Safety Broadband Network. To enable the working group to have productive discussion the working group made the following assumptions regarding governance.

[Note: There may be Federal legislated language that will enable the creation of a federally chartered not-for-profit organization that will hold the single nationwide public safety broadband license (now held by the Public Safety Spectrum Trust) and will become the Nationwide Network Governing Entity (NNGE) we have referred to as the NetAd.]

3.1 FCC

The IWG recommends that the FCC support a Nationwide Network Governing Entity (NNGE) through the adoption of rules that would allow the NNGE to guide network design and governance input from ERIC and the PSAC. This will establish governance over aspects of the network and its implementation that require enforceable rules and policies.

3.2 Governance Body

The development of a NNGE has been identified as a priority. While it is out of scope to make recommendations on the makeup or responsibilities of that group, the following are assumptions made by the Interoperability Working Group regarding the structure and accountability of the yet to be identified Governance Body.

Input and representation from all four of the levels of scope classifications defined in the approach section of this document is an element essential to assure that the needs of the user community are addressed. Defining and supporting the implementation of interoperability solutions must represent the diverse organizations, geographic challenges as well as funding streams. Evaluation of existing commercial systems and deployments are lacking in some elements critical to Public Safety networks. The input from NetAd and NetLo classifications should be used to enhance and complement commercial solutions. By including all stakeholders, structures can be developed to assure compatibility and cost effective use of technologies and equipment. The involvement of the NetAd and NetLo also will support the resolution of disputes between organizations managing separate networks.

Funding oversight should be an element addressed through governance structures. With the assumption that there will be funding streams unique to individual networks and organizations implementing those networks comes the need to provide guidance on how funds are managed when implementing local, regional and state systems as part of the nationwide Public Safety Broadband Network.

Development and support of a national architecture will help to support interoperability efforts. That architecture needs to be flexible enough to account for many variables in implementation ranging from funding to topography and application support while maintaining a minimum performance level. Sustainability of both the network and the governance structure should be defined and outlined in the national architecture and should include a clear definition of goals and objectives.

4 Technical Rules for Public Safety Broadband Networks

4.1 Open Standards

Open standards have fueled the development of commercial wireless systems. “Openness” in standards allow multiple stakeholders including public safety to influence the direction of standards development which reflects an inclusive set of market requirements for development by the industry.

The open standards approach opens the door for competition amongst vendors of wireless network equipment and devices which in turn creates a larger number of equipment choices and a competitive marketplace for public safety systems.

Recommendations:

The Interoperability WG agrees with the use of the 3GPP Rel-8 Baseline as a starting point for Public Safety systems. Further enhancements from the baseline 3GPP release to incorporate feature from Rel-9 or subsequent releases (Currently 3GPP is finishing Rel-10) should be determined by the NetAD / NetLo in a coordinated manner nationally and not the FCC.

As standardized interfaces are important to ensure interoperability between network elements and between systems, the main interfaces of the LTE radio and core network system should be identified for interoperable support.

- Uu- LTE Air Interface
- S6a MME to Home HSS
- S6a – Visited MME to Home HSS
- S8 – Visited SGW to Home PGW
- S9 – Visited PCRF to Home PCRF for dynamic policy arbitration
- S10 – MME to MME support for Category 1 handover support
- X2 – eNodeB to eNodeB
- S1-u – beween eNodeB and SGW
- S1-MME – between eNodeB and MME
- S5 – between SGW and PGW
- S6a – between MME and HSS
- S11 – between MME and SGW
- SGi – between PGW and external PDN
- Gx – between PGW and PCRF (for QoS policy, filter policy and charging rules)
- Rx – between PCRF and AF located in a PDN
- Gy/Gz – offline/online charging interfaces

It is premature to assign a responsible entity or methods used to determine interoperability at this time prior to knowing funding, governance, and network architecture or deployment scenarios.

4.2 Technology Platform and System Interfaces

The FCC in the *Third Report and Order and Fourth Further Notice of Proposed Rulemaking* required all public safety broadband networks to adopt LTE as the technology platform based on the 3GPP Rel-8 standard including the Air Interface “E-UTRA” and core network “Evolved Packet Core” and specified interfaces.²

3GPP standards account for compatibility between releases and versions of each release so backwards compatibility is built-in.

Recommendation:

The Interoperability WG encourages the public safety broadband system to maintain high levels of interoperability both within and between systems with common interfaces and feature sets. The decision to use specific 3GPP Release 8 features, additional interfaces, and upgrades to subsequent 3GPP releases should be left to the NetAD working with relevant stakeholders to determine the criteria for upgrades and the timing. Funding models play an important role in determining “what”, “when” and “if” to upgrade.

² See *Third Report and Order*, 26 FCC Rcd at 738 ¶ 10.

4.3 System Identifiers

3GPP systems are required to use system identifiers better known as the Public Land Mobile Network Identifier (PLMN ID). There are many design, architectural, governance considerations which need to be accounted for to determine the best use of an identifier(s) for the Public Safety broadband network.

The choices for the number of PLMN IDs range from a single national PLMN ID to multiple PLMN IDs which can be assigned based on regional/sub-regional or tribal levels. There are benefits and disadvantages to all approaches which can change the number of PLMN IDs depending on the variables used.

Recommendation:

The Interoperability WG sees the benefits of adopting a single National PLMN ID in order to have operationally a system where public safety users can move freely throughout the nation. In addition, single PLMN ID would reduce complexity and roaming management.

At the same time, the WG suggests that due to the number of currently known open variables, it is too early for the FCC to decide on the number of PLMN IDs. This decision is best left to a later date by the NetAD once more is known about the funding, administration, governance, etc of the Public Safety broadband network.

4.4 Roaming Configurations and Authentication and Interworking Functions

3GPP standards for LTE allow for two types of data traffic backhaul for public safety transient users (users who are operating out of their normal area of operation):

- Home routed where all data traffic is routed back to the transient user's home network
- Local breakout where the transient user is able to access the visited network directly for services.

Transient users do need to be authenticated in a visited network which in commercial systems is handled bi-laterally or through a third party clearing house.

The final definition of a transient user within the public safety network cannot be determined yet as there is no network design, network governance model or network administrator.

Recommendation:

The Interoperability WG supports the need for transient operation within the network to allow coordinated regional or national incident response and general mobility of public safety users.

The Interoperability WG believes that it is premature to make any decisions on roaming configurations within the public safety domain, to pursue requirements with commercial operators, or to determine the need for a third party clearing house.

As expressed earlier, the need for different roaming configurations comes first from deciding the number of PLMN IDs; and then, from the network architecture which would be deployed amongst other

things. The NetAD and NetLO are logically the entities to decide once more is known about the actual network deployment and configuration.

4.5 Interconnectivity of Regional or Tribal Broadband Networks

Interconnectivity between local, regional, and statewide public safety systems with the nationwide network allows different regional systems and the nationwide network to interoperate. The actual number of network peering points and methods for interconnection within the public safety network or to non-public safety networks is unknown at this time.

Recommendation:

The Interoperability WG supports the need for interconnection between regional or tribal networks.

The Interoperability WG believes that it is premature to make any decisions regarding the method for interconnectivity or the use of clearing houses. The NetAD and NetLO are logically the entities to decide once more is known about the actual network deployment and configuration.

4.6 Performance and Quality of Service

Prioritization is the ability to determine which connections have priority over other ones during times of congestion while Quality of Service (QoS) is the ability to maintain a set level of performance for the duration of the connection or session. 3GPP networks have a set of tools at different levels of the network to support prioritization and QoS in 3GPP Release 8 for LTE.

Recommendation:

The Interoperability WG supports the need for a consistent and flexible use of priority and QoS within the public safety broadband network allowing for nationwide and local requirements.

The Interoperability WG believes that it is too premature to make any decisions whether the prioritization and QoS mechanisms are adequate for public safety before use cases are defined. In addition, the NetAD and NetLo should be responsible for defining a performance and QoS framework at the national and/or local level.

4.7 Mobility and Handover

The LTE system supports user mobility through the use of handovers between different sectors of the same site or between sectors of different sites. There are multiple mechanisms which can be invoked for a handover by the network depending on the network topology and administrator preference.

Recommendation:

The Interoperability WG supports the need for mobility through the use of 3GPP handover mechanisms.

The Interoperability WG believes that it is too premature to make any decisions on mandating the types of handovers which are used in an operational public safety broadband system. The NetAD and NetLo

should be responsible for determining what kind of handover and performance is necessary for the network.

4.8 Out of Band Emissions

Due to the mission critical nature of public safety systems it is of the highest importance to protect them from Out-of-Band Emissions (OOBE) from adjacent operations. There are multiple methods used in the wireless industry which can help mitigate OOBE.

Recommendation:

The Interoperability WG encourages the FCC to determine the appropriate level for OOBE to protect public safety systems as the main priority and to ensure public safety systems OOBE support co-existence. In addition, the FCC should use both analytical as well as lab testing to ensure that public safety systems in operation are not impacted by OOBE.

4.9 Applications

There are different kinds of applications which may be used within local systems and across the nationwide public safety broadband network. Short Message Service (SMS), Multimedia Messaging Service (MMS), and Voice Calls are some of the core applications to cellular systems. Other applications are field or operation applications such as email, incident response, etc.

Recommendation:

The Interoperability WG supports the need for interoperability between applications within the public safety broadband network and to other networks. The definition of these applications is not in the WG scope and is handled by the Applications WG.

4.10 Interconnection with Legacy Public Safety Networks

Interconnection between the public safety broadband network and legacy land mobile public safety narrowband networks can enhance interoperability communications.

Recommendation:

The Interoperability WG recommends the NetAD and especially the NetLO are best able to determine what systems need to be interconnected in the legacy networks due to the numerous and varying legacy systems in the field today.

4.11 Performance and Network Capacity

The performance of the network depends on its capacity, efficiency, QoS, and many other factors. The actual performance of the network and the needs for a particular area will vary from area to area based on the population density as well as the geographical and network topology.

Recommendation:

The Interoperability WG supports the development of a robust and reliable public safety broadband network or networks and that public safety broadband systems meet the needs of its mission critical nature and users.

The Interoperability WG recommends the NetAD and the NetLO, not the FCC, determine the level of network performance and capacity. A one size fits all model would appear to be impractical with the significant variation across the United States in population, geography, network requirements, etc.

4.12 Security and Encryption

The security of communication over public safety systems is critical to its integrity. In addition, public safety broadband systems need to be hardened against intrusions which compromise reliability or security.

Recommendation:

The Interoperability WG supports the need for robust security for public safety broadband network using interoperable mechanisms. The definition of the appropriate level of security and mechanisms is not in the Interoperability WG scope and is handled by the Security WG.

4.13 Robustness and Hardening

The resilience and reliability of public safety systems are important for the day-to-day operation as well during emergency situations.

Recommendation:

The Interoperability WG supports the need for public safety broadband systems to be robust and reliable to serve its mission critical nature and users.

The Interoperability WG recommends the NetAD and the especially the NetLO, not the FCC, determine the level of network performance and capacity. While a one-size-fits-all model may create requirements which are impractical or prohibitively costly to build, minimum standards, with the provision for exceptions, should be managed by NetAD.

4.14 Coverage Requirements and Reliability

The coverage and coverage reliability of the network depends on a number of factors which include network topology, cell density, cell height, in-building systems, etc., which need to match the population density, building density, and geographical terrain amongst other factors.

Recommendation:

The Interoperability WG recognizes that the public safety broadband systems that will become part of the nationwide network must adequately serve the different users of the network.

The Interoperability WG recommends the NetAD and the NetLO, not the FCC, determine the level of network performance and capacity by setting guidelines. A one size fits all model would appear to be

impractical with the significant variation across the United States in population, geography, network requirements, etc.

4.15 Interference Coordination

Interference coordination between networks prevents harmful interference from degrading interoperability.

There are administrative as well as technical solutions which can be brought to bear to mitigate interference issues between networks.

Recommendation:

The Interoperability WG recommends that the FCC within its mandate facilitate coordination between different systems within the nationwide network. Actual interference mitigation techniques are not specified by 3GPP, so the techniques used within the public safety broadband network should be determined by the NetLo along with the NetAd.

4.16 Incumbent Narrowband Operations

Incumbent operations of users in the lower portion of the public safety band need attention.

Recommendation:

The Interoperability WG does not see this as an issue which is within the scope of our WG.

5 Public Safety Roaming on Public Safety System Broadband Networks

The FCC proposed three types of roammers in the *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*

- “Itinerant roammers” - those on a network while in transit through an area or while in the execution of small scale tasks (such as an extradition or conference attendance).
- “Interoperability roammers”- those who are on the network as part of a long-standing arrangement.
- “Response roammers” - those who are on the network as part of a coordinated response to a large-scale emergency incident.

The act of roaming in a 3GPP network is driven by crossing from the user’s home PLMN to a visited PLMN which the user is able to gain authorization to access.

Recommendation:

The Interoperability WG supports the ability, from an interoperability view, for public safety broadband users to move around the nationwide public safety network with a design that minimizes roaming issues and reduces costs within the public safety nationwide network and provides robust, reliable service to all regions. The actual need for roaming and roaming agreements will depend on the use of PLMN ID and network architecture. The NetAd should determine the requirements and more detailed use cases. It is too premature at this time to determine any specifics.

5.1 Prioritization and Quality of Service to Support Roaming

Standards and practices for prioritization/QoS and its trigger for transient users need to be established to ensure interoperability and deterministic behavior for users.

Recommendation:

The Interoperability WG supports the ability from an interoperability view for public safety broadband transient users to know what framework they will be using when not in their home network. The actual need for this scheme again depends on the use of PLMN ID and network architecture. The NetAd should determine the requirements and more detailed use cases. It is premature at this time to determine any specifics.

5.2 Applications to Be Supported for Roamers

Roamers should be able to access applications in their home network when roaming.

Recommendation:

The Interoperability WG supports the ability from an interoperability view for public safety broadband transient users-to access their home applications as well as nationwide and visited network applications.

The actual need for this scheme depends on the use of PLMN ID and network architecture. The NetAd should determine the requirements and determine what applications should be supported. It is too premature at this time to determine any specifics.

5.3 Public Safety-to-Public Safety Roaming Rates, Volume of Roaming Traffic, and Proposed Model Agreement

Roaming rates, the volume of roaming traffic and any model agreement for handling roaming are part of the discussion items for the business part of roaming in commercial networks. The relevance of this to public safety broadband systems is hard to determine at present.

Recommendation:

The Interoperability WG supports the ability from an interoperability view for public safety broadband roaming (as defined earlier by transient users). There should be no cross charging for the volume of traffic within the public safety broadband network. There is an additional need for roaming with commercial networks which needs to be in place for the nationwide public safety broadband network.

The NetAd should determine the requirements within the network governance model. It is too premature to make any rules regarding roaming rates, volume, or agreements without the knowing more about actual network design and operation.

6 Testing and Verification to Ensure Interoperability

Conformance testing on standards in certified labs is supported by the industry. There are numerous groups worldwide which test conformance for 3GPP devices. Network equipment testing is normally conducted but in a less structured manner especially with regards to interoperability testing.

Recommendation:

The Interoperability WG supports the concept of testing to ensure high levels of interoperability between network elements and devices:

- In terms of UE interoperability certification, the WG recommends that public safety leverage the conformance testing and certification in the commercial 3GPP industry as much as possible, to avoid increasing costs to public safety and only test specific public safety features.
- In terms of network interoperability (between systems and between vendors), where there are informal processes between 3GPP (normally driven by customer needs), the WG recommends that public safety leverage this as much as possible to avoid increasing costs. In the case of any public safety-specific network configurations or vendor combinations that are not covered by normal commercially-driven testing, a public safety oriented laboratory such as PSCR or Idaho National Labs may be used to perform appropriate testing.

The NetAD should be responsible to determine what should be tested based on input from stakeholders and to work with testing groups/houses to ensure interoperability. It is premature to pick labs or determine interoperability needs for certification.

7 Other Matters Relevant to Interoperability on Public Safety Broadband Networks

7.1 Network Operations, Administration and Maintenance

Operational capabilities and models are handled by the network management, administration / provisioning and maintenance systems.

Recommendation:

The Interoperability WG believes it is premature for anyone to provide recommendations on OA&M. The NetAd and NetLo, after receiving inputs from stakeholders and studying the requirements, are better able to determine a course of action.

7.2 Reporting on Network Deployment

Recommendation:

Out of Scope of Interoperability WG

7.3 Devices

Devices which use the public safety broadband network must meet conformance standards in order to assure interoperability.

Recommendation:

The Interoperability WG encourages the FCC to require conformance testing as it does of other devices within its mandate of radio emissions for type approval.

In terms of UE interoperability certification, the WG recommends that public safety leverage the conformance testing and certification in the commercial 3GPP industry as much as possible, to avoid increasing costs to public safety and only test specific public safety features.

Determining additional conformance testing to 3GPP standards and support for additional bands or radio technology modes should be done by the NetAD based on input of stakeholders.

7.4 In-Building Communications

Recommendation:

Out of Scope of Interoperability WG

7.5 Deployable Assets

COW (Cell on Wheels) and COLTs (Cells on Light Trucks) may be deployed by public safety during emergencies. These pieces of equipment are radio transmitters/receivers which support communications for specific use cases within public safety networks.

Recommendation:

The Interoperability WG supports the FCC within its normal mandate to propose rules related to regulating the use of radio equipment and radio frequency characteristics to operate within defined characteristics. The NetAD should be responsible to determine what should be tested beyond radio conformance based on input from stakeholders and to work with testing groups/houses to ensure interoperability. Regarding the use of 4.9GHz or satellite links for COLTS/COWs the Interoperability WG recommends the NetAD / NetLO work with the FCC to determine the best backhaul methods.
Operation of Fixed Stations and Complementary Use of Fixed Broadband Spectrum

7.6 Operation of Fixed Stations and Complementary Use of Fixed Broadband Spectrum

Use of fixed stations and complementary use of fixed broadband and associated rule making is important to maintain interoperability with public safety systems.

Recommendation:

The Interoperability WG supports the FCC within its normal mandate to propose rules related to regulating the use of spectrum and radio frequency characteristics. The Interoperability WG agrees that “fixed” use of spectrum should not be prohibited, but should be allowed only in exceptional circumstances, and then on a secondary and non-interfering basis.

7.7 Compliance with the Commissions Environmental Regulations

Recommendation:

Out of Scope of Interoperability WG

7.8 Public Safety Broadband and Next Generation 9-1-1 Networks

Public safety first responders need to communicate with each other to ensure emergency response is fast, accurate, and efficient. NG 9-1-1 capable PSAPs (Public Safety Answering Points) bring media transfer abilities beyond standard voice such as video, text, and pictures.

Recommendation:

The Interoperability WG supports the interoperability of public safety broadband networks with NG 9-1-1 capable systems in order for first responders to have seamless communication with NG 9-1-1 PSAPs.

The NetAD should work with groups including the Association of Public-Safety Communications Officials (APCO) and the National Emergency Number Association (NENA) to determine interoperability standards and practices between the two networks.