DOCKET FILE COPY ORIGINAL

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

MAILED
FEB - 2 2011
FCC Mail Room

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

THIRD REPORT AND ORDER AND FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING

Adopted: January 25, 2011 **Released: January 26, 2011**

Comment Date: [45 days after publication in the Federal Register]
Reply Comment Date: [75 days after publication in the Federal Register]

By the Commission: Chairman Genachowski and Commissioners Copps, McDowell, Clyburn, and Baker issuing separate statements.

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 1
II. BACKGROUND 2
III. THIRD REPORT AND ORDER 5
A. A Common Technology Platform for the Nationwide Public Safety Broadband Network 7
B. Enabling Public Safety Broadband Interoperability 13
IV. FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING 15
A. Technical Rules for the Public Safety Broadband Network 17
1. Architectural Framework 17
2. Architectural Guiding Principles 18
3. Open Standards 27
4. Technology Platform and System Interfaces 29
5. System Identifiers 32
6. Roaming Configurations 35
7. Roaming Authentication and Interworking Functions 37
8. Interconnectivity of Regional or Tribal Broadband Networks 38
9. Prioritization and Quality of Service 43
10. Mobility and Handover 47
11. Out-of-Band Emissions and Related Requirements 51
12. Applications 55
13. Interconnection With Legacy Public Safety Networks 58
14. Performance 59
15. Network Capacity 63
16. Security and Encryption 65

17. Robustness and Hardening 70
18. Coverage Requirements 71
19. Coverage Reliability 74
20. Interference Coordination 76
21. Incumbent Narrowband Operations 80
B. Public Safety Roaming on Public Safety Broadband Networks 85
1. Prioritization and Quality of Service to Support Roaming 90
2. Applications to Be Supported 93
3. Public Safety-to-Public Safety Roaming Rates 94
4. Volume of Roaming Traffic 97
5. Proposed Model Agreement 98
C. Federal Use 100
1. Section 2.103 100
2. Roaming 104
D. Testing and Verification to Ensure Interoperability 106
1. Conformance Testing 106
2. Interoperability Testing 109
3. Interoperability Verification 116
E. Other Matters Relevant to Interoperability on Public Safety Broadband Networks 117
1. Network Operations, Administration and Maintenance 117
2. Reporting on Network Deployment 118
3. Devices 119
4. In-Building Communications 123
5. Deployable Assets 127
6. Operation of Fixed Stations and Complimentary Use of Fixed Broadband Spectrum 129
7. Compliance with the Commission's Environmental Regulations 132
8. Public Safety Broadband and Next-Generation 911 Networks 133
F. Section 337 Eligible Users 134
V. PROCEDURAL MATTERS 141
A. Regulatory Flexibility Act 141
B. Paperwork Reduction Act of 1995 142
C. Other Procedural Matters 143
VI. ORDERING CLAUSES 148
APPENDIX A—Final Rules
APPENDIX B—Proposed Rules
APPENDIX C—Final Regulatory Flexibility Certification
APPENDIX D—Initial Regulatory Flexibility Analysis

I. INTRODUCTION

1. In this *Third Report and Order* and *Fourth Further Notice of Proposed Rulemaking (Third R&O and Fourth Further Notice)*, we adopt rules and propose further rules to create an effective technical framework for ensuring the deployment and operation of a nationwide interoperable public safety broadband network. It has been almost ten years since the tragic events of September 11, 2001, and more than five years since Hurricane Katrina devastated the Gulf Coast. During those horrific events, and others, it became clear that the lack of a nationwide interoperable public safety network hampered rescue efforts and the overall effectiveness of public safety operations. Our action today takes an important step towards remedying the lack of such a network by establishing initial rules for a nationwide technical interoperable framework for the first nationwide broadband network for public safety.

II. BACKGROUND

2. The public safety spectrum band at issue in this proceeding is designated for public safety

broadband communications (763-768 MHz and 793-798 MHz).[1] This band is licensed on a nationwide basis to the Public Safety Broadband Licensee.[2] In 2007, the Commission recognizing the difficulties in funding and the need for an interoperable nationwide public safety broadband network, created a mandatory public-private partnership to facilitate these goals.[3] The Commission's plans did not come to fruition because Auction 73 failed to produce a winning bidder to participate in the partnership.[4]

3. The Commission subsequently issued both a *Second*[5] and *Third Further Notice of Proposed Rulemaking*[6] seeking comment on options to achieve the goal of an interoperable nationwide public safety network in light of this failure.

4. After the *Third Further Notice* was issued, a number of public safety jurisdictions filed petitions for waiver of the Commission's rules to allow them to deploy broadband networks in the public safety broadband spectrum.[7] The *Waiver Order* granted twenty-one public safety entities conditional waivers to pursue early deployment of statewide or regional broadband networks within their jurisdictions.[8] The *Waiver Order* imposed on the waiver recipients an initial set of technical requirements, which were subsequently supplemented by Order of the Bureau, in consultation with the Emergency Response Interoperability Center (ERIC).[9] The *Interoperability Waiver Order* sets forth the requirements to ensure that a 700 MHz broadband network deployed by the waiver recipients, and integrated into the national network, is interoperable on a nationwide basis.

III. THIRD REPORT AND ORDER

5. In its report on the events of September 11, 2001, the bipartisan 9/11 Commission cited the events of that day as "strong evidence that compatible and adequate communications among public safety organizations at the local, state and federal levels remains an important problem."[10] In this order,

---

[1] *See* Service Rules for the 698-746, 747-762 and 777-792 Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, WT Docket No. 06-150, PS Docket No. 06-229, *Second Report and Order*, 22 FCC Rcd 15289, 15406 ¶ 322 (*Second Report and Order*).

[2] *See id.*

[3] *Id.* at 15428 ¶ 386.

[4] *See id.*; *see also* Auction of 700 MHz Band Licenses Closes, *Public Notice*, DA 08-595 (rel. Mar. 20, 2008) (*700 MHz Auction Closing Public Notice*). http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=73; Auction of the D Block License in the 758-763 and 788-793 Bands, AU Docket No. 07-157, *Order*, 23 FCC Rcd 5421, ¶ 5 (2008) (*D Block Post-Auction Order*).

[5] *See* Service Rules for the 698-746, 747-762 and 777-792 Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, WT Docket No. 06-150, PS Docket No. 06-229, *Second Further Notice of Proposed Rulemaking*, 23 FCC Rcd 8047 (2008) (*Second Further Notice*).

[6] Service Rules for the 698-746, 747-762 and 777-792 Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, WT Docket No. 06-150, PS Docket No. 06-229, *Third Further Notice of Proposed Rulemaking*, 23 FCC Rcd 14301 (2008) (*Third Further Notice*).

[7] *See* Public Safety and Homeland Security Bureau Seeks Comment on Petitions for Waiver to Deploy 700 MHz Public Safety Broadband Networks, DA 09-1819 (rel. Aug. 14, 2009) (*700 MHz Waiver Public Notice*).

[8] *See* Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks, PS Docket 06-229, *Order*, 25 FCC Rcd 5145, 5147 ¶ 7 (2010) (*Waiver Order*).

[9] *See* Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks, PS Docket 06-229, *Order*, DA 10-2342 (rel. Dec. 10, 2010) (*Interoperability Waiver Order*).

[10] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 397 (2004) (9/11 Commission Report). *See also* Statement of Former 9/11 Commission Chair Thomas H. Kean and Former 9/11 Commission Vice Chair Lee H. Hamilton on the Federal Communication Commission's Approach to Interoperable Communications Capabilities for Public Safety, Mar. 18, 2010, *available at* http://blog.broadband.gov/?entryId=297238 (Kean and Hamilton Statement); Statement of Former 9/11 Commissioners Jamie (continued....)

we take significant steps to address this problem by adopting rules to guide development of a nationwide interoperable public safety broadband network. First, to ensure nationwide interoperability, we mandate that all public safety broadband networks adopt LTE as a common technology platform. Second, in light of significantly changed circumstances since the unsuccessful attempt to implement a mandatory public/private partnership in 2008, we stay certain of our existing mandatory partnership rules in order to provide certainty during the pendency of this proceeding.

6. The approach adopted here is consistent with the Plan's public safety recommendations, which Chairman Thomas Kean and Vice-Chairman Lee Hamilton of the 9/11 Commission have described as offering "a clear roadmap" for achieving interoperable public safety communications.[11] The approach we embrace in this order, and develop further in our *Fourth Further Notice* below, will "provide public safety users throughout the country with access to wireless broadband capabilities that will enable them to communicate effectively across departments and jurisdictions, while encouraging public safety to partner with commercial providers and leverage the investments they already have made."[12]

A. A Common Technology Platform for the Nationwide Public Safety Broadband Network

7. In the *Second Report and Order*, we mandated that the shared network incorporate, among other technical specifications, "a broadband technology platform that provides mobile voice, video and data capability that is seamlessly interoperable across agencies, jurisdictions and geographic areas" and that also includes "current and evolving state-of-the-art technologies reasonably made available in the commercial marketplace with features beneficial to the public safety community (*e.g.*, increased bandwidth)."[13] We reiterated this baseline requirement in the *Third Further Notice*, where we tentatively concluded that "the shared wireless broadband network must provide for fixed and mobile voice, video and data capability"[14] and that the network "must use a common air interface."[15] Although we further concluded that "there [did] not appear to be a basis for a determination regarding the viability of any particular technology for shared network at [that] time," we clarified that "the record support[ed] a conclusion that two next generation technologies in particular, WiMAX and LTE, provide the most likely options to provide the necessary broadband level of wireless service to public safety entities."[16]

8. There is substantial support for our proposal to require use of a common air interface on the public safety broadband network. U.S. Cellular, for example, states that "an interoperable network of networks providing advanced public safety applications requires a common air interface,"[17] while NPSTC contends that "[v]arying technology platforms [would] present challenges to efficient and effective interoperability."[18] Moreover, Motorola argues that, "[b]y requiring a common technology from the start, the Commission would avoid migrations that are costly, time consuming, and ultimately unnecessary."[19] We agree with these commenters and therefore adopt our tentative conclusion to mandate adoption of a

(Continued from previous page)
Gorelick and Slade Gorton on the Federal Communication Commission's Approach to Interoperable Communications Capabilities for Public Safety, Mar. 15, 2010, *available at* http://4.21.126.217/?entryId=268708.

[11] *See* Kean and Hamilton Statement.

[12] *See id.*

[13] *Third Further Notice* at 14336-37 ¶ 95.

[14] *Id.* at 14340 ¶ 106.

[15] *Id.* at 14342 ¶ 110.

[16] *Id.* at 14341 ¶ 108.

[17] U.S. Cellular Reply Comments on *Third Further Notice* at 15 (Nov. 12, 2008).

[18] NPSTC Reply Comments on *Third Further Notice* at 5 (Nov. 12, 2008).

[19] Motorola Reply Comments on *Third Further Notice* at 6 (Nov. 12, 2008).

common air interface for the nationwide public safety broadband network. Adoption of a common air interface will provide the first building block to ensure nationwide interoperability of the public safety broadband network. While this is only a small step in achieving the critical goal of interoperability, it is an important, widely supported first step.

9. Recently, a strong consensus has emerged in support of a particular technology platform, namely Long Term Evolution (LTE), as a common technology platform for the public safety broadband network.[20] APCO, for example, states that "public safety entities have been unanimous in their support of LTE."[21] The adoption of LTE for the public safety broadband network has also drawn support from wireless carriers and other stakeholders, such as AT&T, which urges the Commission to establish "technological standards and minimum system requirements" for public safety broadband networks "and ensure that all networks adopt the LTE radio technology and infrastructure."[22] Citing "broad support in the record for specifying LTE," we required in the *Waiver Order* that waiver recipients adopt the LTE air interface—specifically "at least 3GPP Standard, Evolved Universal Terrestrial Radio Access ('E-UTRA'), Release 8 ('LTE'), and associated Evolved Packet Core ('EPC')"—for their early deployments.[23] In setting this condition, we emphasized that we "[did] not impose a technical standard in the present case lightly,"[24] but that such condition was necessary "to provide a clear path for initial deployment and evolution" and to ensure "interoperability and roaming among these systems."[25]

10. Given the overwhelming record support for LTE among public safety organizations and other stakeholders, and the importance of ensuring that all public safety broadband networks adopt a common air interface in order to establish an important building block for interoperability, we will require that all networks deployed in the 700 MHz public safety broadband spectrum adopt LTE, specifically at least 3GPP Standard E-UTRA Release 8 and associated EPC.[26] We recognize that this requirement departs from the Commission's traditional posture of technological neutrality, which we believe has served the public interest well—including in the mobile wireless sector, where the flexibility for providers to choose their technology path has led to robust competition and innovation to the benefit of consumers. While we continue to believe in the importance of technological neutrality as a policy, we believe that, in the instant case, establishing a common air interface for 700 MHz public safety networks is necessary to achieve our critical goal of a nationwide interoperable public safety wireless broadband network. We reiterate our observation from the *Waiver Order* that "our overriding consideration here is to provide a reasonable and clearly defined path towards public safety interoperability, a goal that has proven previously to be elusive in the public safety narrowband context."[27] Our requirement simply

[20] *See, e.g.*, APCO Comments on *National Broadband Plan Public Notice* #8 at 11 (Nov. 12, 2009); AT&T Comments on *National Broadband Plan Public Notice* #8 at 2 (Nov. 12, 2009); Verizon and Verizon Wireless Comments on NBP PN #8 at 6 (Nov. 12, 2009); Public Safety Spectrum Trust Comments on *700 MHz Public Safety Broadband Networks Waiver PN* at 11 (Aug. 4, 2009).

[21] APCO Comments on *National Broadband Plan Public Notice* #8 at 11; *see also* PSST Comments on *700 MHz Waiver Public Notice* at 11.

[22] AT&T Comments on *National Broadband Plan Public Notice* #8 at 2; *see also* Verizon and Verizon Wireless Comments on *National Broadband Plan Public Notice* #8 at 6. In recognition of this gathering consensus, the NBP recommends that the Commission consider designating LTE as the technology standard for the network. *See* National Broadband Plan at 316.

[23] *Waiver Order* at 5157-58 ¶ 38.

[24] *Id.*

[25] *Id.*

[26] The uniform deployment of Release 8 (or subsequent releases) is necessary to ensure backwards-compatibility. *See* UMTS Forum, *Mobility Broadband Evolution: the roadmap from HSPA to LTE*, Feb. 2009; 3G Americas, *3GPP Release 8 and Beyond, HSPA+, SAE/LTE and LTE-Advanced*, Feb. 2009.

[27] *Waiver Order* at 5158 ¶ 40.

acknowledges the fact that, at this stage, "LTE has become the technology of choice for the 700 MHz band."[28] This is not a decision we make lightly, but one that we believe is appropriate to provide the first building block to ensure nationwide interoperability of the public safety broadband network. In the *Fourth Further Notice* below, we seek comment on how to address the use of future technolgy platforms that may arise to ensure that they are interoperable and backward compatible with the LTE requirements designated in this *Third Report and Order* or in subsequent orders.[29]

11. We will require that any releases after Release 8 ensure backward compatibility between all subsequent releases from Release 8 and onwards. By imposing this requirement on the network operator, we will ensure that the technical baseline for interoperability is preserved.

12. Further, we also determine, consistent with this decision, and based on the record and our technical analysis of LTE reference architecture[30] that certain Release 8 (LTE) interfaces must be supported.[31] The required interfaces include:

- Uu- LTE air interface
- 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

The first four of these interfaces are important for achieving interoperability when roaming across networks while the rest are necessary to ensure multi-vendor interoperability for equipment and devices operated on the same network. In order to promote both multivendor interoperability and interoperability

[28] Moreover, given the breadth of support for LTE—both in the public safety community and in the commercial wireless sector—we disagree with the comments of Clearwire and Sprint Nextel that "a mandated single air interface would preclude public safety from seeking bids from many service providers." *See* Joint Comments of Sprint Nextel and Clearwire Corp. on *National Broadband Plan Public Notice #8* at 14.

[29] *See infra* Section IV.A.4.

[30] *See* 3rd Generation Partnership Project, "General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," 3GPP TS.23.401 (2007).

[31] *See, e.g.*, Alcatel-Lucent Ex Parte Filing, PS Docket 06-229 at 3 (filed Aug. 18, 2010) ("Public Safety Broadband Interoperability Recommendations: FCC Interoperability Vendor Meeting").

when roaming, we will require that all public safety broadband networks be capable of supporting each of the aforementioned LTE Release 8 interfaces from day one of service operation. We also believe it is critical that the support of these interfaces be demonstrated. Accordingly, we will require each public safety broadband network operator to submit to the Bureau before deployment a certification that it is instituting the required interfaces in compliance with Release 8 or higher of 3GPP standards prior to the date it achieves service availability.[32]

B. Enabling Public Safety Interoperability

13. As outlined in the background above, we note that some of the rules for deployment of the public safety broadband spectrum are premised on the existence of a mandatory partnership with a D Block licensee. Since the D block auction produced no winning bid, the rules have never become operative. Moreover, we find that these rules no longer serve their intended purpose and may in fact constrain the optimal public safety use of this spectrum.[33] Further, in order to enable full consideration of rules that will most effectively lead to the nationwide interoperability of the public safety broadband network, and to ensure that any actions that might otherwise be taken under the existing regulatory framework do not undermine the implementation of a more effective regime, we find it in the public interest to stay certain of the partnership rules during the pendency of this proceeding.[34]

14. We also note that while we are staying these partnership rules, public safety entities seeking early deployment authorization during the pendency of this proceeding will still need to file a waiver petition with the Commission.[35] For those entities currently undertaking deployment pursuant to our previously granted waivers, their activities remain subject to existing technical rules, the requirements of the *Waiver Order* and *Interoperability Waiver Order*, and the new requirements adopted in this *Third Report and Order*, and future rules that may be adopted in this proceeding.[36]

IV. FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING

15. In the *Third Report and Order* above, we adopted LTE as the common technology platform for a nationwide public safety broadband network. In this *Fourth Further Notice*, we consider and propose additional requirements to further promote and enable nationwide interoperability among public safety broadband networks operating in the 700 MHz band. This *Fourth Further Notice* addresses interoperability from a technological perspective. It considers interoperability at various communication

[32] For purposes of this *Third Report and Order* and *Fourth Further Notice*, "service availability" is achieved when the system is being used on a day-to-day basis for operational functions by at least fifty users.

[33] In May, the Commission granted twenty-one requests from public safety jurisdictions seeking waivers to proceed with early deployment of public safety broadband networks. *See Waiver Order*. Approximately twenty-five additional such requests have since been submitted, and the Bureau has solicited comment on these in a series of public notices. *See* Public Safety and Homeland Security Bureau Seeks Comment on Petitions for Waiver to Deploy 700 MHz Public Safety Broadband Networks, PS Docket No. 06-229, *Public Notice*, DA 10-1748 (PSHSB 2010) (*Second Round Waiver Public Notice*); *See* Public Safety and Homeland Security Bureau Seeks Comment on Additional Petition for Waiver to Deploy 700 MHz Public Safety Broadband Networks, PS Docket No. 06-229, *Public Notice*, DA 10-1796 (PSHSB 2010) (*Texas Waiver Public Notice*); *See* Public Safety and Homeland Security Bureau Seeks Comment on Petitions for Waiver to Deploy 700 MHz Public Safety Broadband Networks, PS Docket No. 06-229, *Public Notice*, DA 10-2278 (PSHSB 2010) (*Third Round Waiver Public Notice*).

[34] For purposes of this order, we stay the following rules: 47 C.F.R. § 90.1403(b)(1), (2), (3), (5), (8); 90.1405-90.1430; and 90.1435.

[35] In this respect, we note that regardless of our decision to stay certain rules, there remains no mechanism, absent a waiver, for regional or Tribal public safety entities to obtain access to the spectrum, *e.g.*, through a lease or other permitted mechanism with the PSBL.

[36] *See id.*

layers, namely the physical layer, network layer and application layer.[37]

16. As an initial matter, we seek comment on the definition of "interoperability" for purposes of the public safety broadband network in the 700 MHz band. Part 90 of Commission rules defines interoperability as "an essential communication link within public safety and public service wireless communications systems which permits units from two or more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results.[38] The Department of Homeland Security (DHS) Office of Interoperability and Compatibility (OIC), however, defines interoperability as "the ability of public safety agencies to talk to one another via radio communications systems – to exchange voice and/or data with one another on demand, in real time, when needed and when authorized."[39] We propose to amend the Commission's definition of interoperability in Part 90 to harmonize it with DHS's because we believe that the broader definition is the true definition of interoperability we seek to achieve (i.e., ensuring that the public safety community, whoever and wherever they are, is able to communicate with one another). We seek comment on our proposal. Interoperability should allow any user while at home or while roaming to be able to access any regional or tribal public safety network in order to reach any other users and any services at home network or at visited network. Interoperability can only be achieved by defining common sets of features and parameters at various communication layers,[40] on every device or node in all networks. Interoperability between devices and network nodes is achieved when all communication layers function with the same corresponding protocols, or simply speak the same language. We also seek comment on whether this definition should apply only to broadband communications, or should be extended to cover narrowband communications as well. If not, we seek comment on the correct definition for narrowband and broadband communications.

A. Technical Rules for the Public Safety Broadband Network

1. Architectural Framework

17. As an initial matter, we consider the architecture of the public safety broadband network which is critical to ensure nationwide interoperability. We believe that the development of a uniform, nationwide architectural framework will promote a comprehensive understanding of interoperability and the steps that must be taken to achieve that objective. Below, we propose a set of high-level principles to guide development of the network in a manner that ensures interoperability. We seek comment on each of these principles. Do these principles capture all of the services and capabilities that the network must be capable of supporting to ensure interoperability? Do they reflect a realistic understanding of how the network will evolve over time? Should the Commission endorse these principles, or others, as a guide for development of the network? Should the Commission adopt these principles through the rulemaking process and codify them as enforceable rules? Are there entities other than the Commission that are better situated to establish an architectural framework for the network and keep the framework current? If so, who are these other entities and how would they achieve this? Do they adequately represent public safety interests?

[37] The concept of layering that first introduced by ISO provides OSI layers consisting of seven layers of functional capabilities within each device or network node. The follow up developments in the industry produced lower number of layers, and in fact, based on needed requirements, various organizations introduced various number of layers based on their needs. We selected 3 layers for practical reasons. Layer 2 of OSI is collapsed into Layer 1 and dubbed as the Physical layer, Layer 3 stays intact as being the Network layer, and Layers 4, 5 and 6 all merge into layer 7, the Application layer.

[38] 47 C.F.R. § 90.7.

[39] *See* SAFECOM, http://www.safecomprogram.gov/SAFECOM/about/default.htm.

[40] For the purpose of this *Third Report and Order* and *Fourth Further Notice* the term "communication layers" includes the Physical Layer, Network Layer, and Application Layer.

2. Architectural Guiding Principles

18. *Components of the Nationwide Network.* The nationwide interoperable broadband network will comprise a set of interoperable, regional or tribal all-IP LTE networks operating in the public safety broadband spectrum; a nationwide IP backbone network; and additional network and service platforms at the national level.

19. *Regional or Tribal Network Characteristics.*[41] The regional networks need to support and maintain certain common characteristics in order to ensure interoperability among them. There are certain other characteristics that pertain to individual networks and serve only the local needs. The common characteristics are:

- Support of all-IP LTE technology platform, particularly 3GPP standard, Universal Terrestrial Radio Access (E-UTRA), Release 8 (LTE), and associated Evolved Packet Core (EPC) as adopted in this order.
- Support of Network Identification schemes, specifically the use of Public Land Mobile Network Identifiers (PLMN IDs), as proposed in this notice.
- Support of certain LTE interfaces to ensure interoperability.
- Support of baseline applications such as those proposed in this FNPRM.
- Support of roaming capabilities such as Home-Routed and Local-Breakout.
- Support of a nationwide framework for Quality of Service and Priority Access.
- Support of security schemes such as those proposed in this FNPRM.
- Support of a minimum level of spectrum efficiency.
- Support of a minimum level of coverage reliability (95%).
- Support for interference mitigation schemes.
- Support for device capabilities as proposed in this FNPRM.
- Test verifications for interoperability (i.e., conformance and interoperability testing).

20. *Supporting Voice and Data Communications.* As the LTE standard progresses, the network must become capable of supporting both mission-critical voice and data communications. Support for both is necessary to ensure a baseline level of operability and interoperability across the country.

21. *Roaming Authentication and Internetworking Functions – Clearing House.* Roamers will need to be authenticated in the visited network as they would be in their own networks. Additionally, user traffic needs to flow between these networks to enable roaming. Roaming between public safety broadband networks requires certain technical and operational arrangements to include interconnectivity among many interfaces, security arrangements and many other roaming arrangement and agreements. As the number of regional or tribal networks grows, the number of such arrangements grows rapidly.[42] The NPSTC BBTF Report recommends the establishment of a common clearing house for the purpose of roaming. The third party clearing houses would provide internetworking functions as well as additional functions, such as roaming authentication and clearing functions.

22. *Nationwide Backbone Network.* Regional or tribal public safety broadband networks will

[41] "Regional or tribal networks" refer to the subset of networks in the network of networks model.

[42] For "n" regional or tribal networks, the number of such agreements and arrangements is "(n(n-1))/2".

need to be securely interconnected utilizing sufficient capacity in order to form a nationwide network. Such interconnectivity is needed for instance, to support the end-to-end interoperable connections traversing multiple regional or tribal networks and to support roaming connections. We believe a number of possible solutions for interconnectivity of regional broadband networks exist, as we discuss at Section 8 *infra*. While these solutions should have sufficient capacity (being fast and able to carry sufficient data) they should also be timely (low delay), reliable, secure and cost-effective. One such alternative is to use the third party network operators to provide high-performance, reliable and secure interconnectivity links. The establishment of a clearing house, as mentioned earlier, could also provide interconnectivity among all public safety regional or tribal networks on a nationwide basis through secure and private networks using Internetwork Packet Exchange (IPX) protocol.

23. *Nationwide Services and Capabilities.* For the network to be truly interoperable on a nationwide basis, certain services, applications and capabilities must be available through each network and to each user to support nationwide interoperability. The implementation of these services may be accomplished either nationally through a set of national core capabilities or locally through capabilities offered by regional or tribal networks. Some instances of these services are authentication services and directory services to mention a few. We envision that the operation of these services, if opted to be implemented nationally, could be accomplished by clearing houses.

24. *Evolution.* It is imperative that the public safety broadband network evolve as new technologies become available. While the current baseline for LTE technology is Release 8, new releases of this standard will offer capabilities that further enhance public safety communications. The evolution of technology and standards should provide support for voice and mission critical voice and ensure that the public safety network and its operation evolve and keep pace with the competitive commercial marketplace. Further, backwards compatibility is essential if the network is to be fully interoperable across the nation.

25. We seek comment on whether we should establish guiding principles for public safety broadband network architecture and, if so, whether the principles summarized above are the principles that should serve as the basis for this vision. Are there are other principles we should consider? For example, should we be looking at how to best maximize network efficiencies by sharing network resources such as core networks? Should shared infrastructure also be encouraged through such a vision in order to reduce costs of network deployment?

26. We tentatively conclude that we should adopt such a framework for the architectural vision. We seek comment on this tentative conclusion. We also seek comment on how we can ensure that this architectural framework evolves to reflect the continued evolution of the network and its underlying technology. Is this a framework the Commission should adopt and manage, or is another entity better suited for this role? For example, should the Commission review these requirements on a regular basis, such as every two years? Is there another entity that would be better suited to address these principles? Could this be a role for the Emergency Response Interoperability Center Public Safety Advisory Committee (PSAC)? What should such a review process include and how can we ensure it will take into account technological advances on a timely basis? Are there third parties that might be better suited and how do we ensure that they have the technical capability to keep up with the pace of technology to ensure the framework evolves?

3. Open Standards

27. Open standards enable vendors to build to common parameters. In the *Competition Public Notice*, the Bureau asked whether the implementation of open standards for public safety broadband and narrowband equipment could increase competition in these markets and hence, increase

interoperability.[43] Commenters were generally supportive of this proposition. ARINC, for example, stated that "[o]pen standards will increase competition,"[44] while the Arlington County Information Technology Advisory Commission argued that "[o]pen standards could offer a more competitive landscape, reduced costs, would foster a better chance for reduction of any interoperability problems and ensure a broader dissemination of equipment to a far larger number of responders."[45] The APCO Project 25 Steering Committee cautioned, however, that any implementation of "open standards" must accommodate the use of patented technologies that may be "the best technologies to support particular applications."[46]

28. In our *Third Report and Order* we require all 700 MHz public safety broadband networks to adopt LTE, a 3GPP standards-based technology, as a common technology platform.[47] We seek comment on whether we should take additional measures to encourage public safety broadband network operators to adopt technologies that employ open standards and if so, what should these be? What are the potential dangers to interoperability associated with the use of devices and equipment that employ proprietary technologies? How do we ensure that any such use does not negatively impact nationwide interoperability?

4. Technology Platform and System Interfaces

29. In the *Third Report and Order*, we require that public safety broadband networks adopt the LTE technology platform, particularly 3GPP standard, E-UTRA, LTE, associated EPC, and that they support specified interfaces.[48] Are there any additional capabilities within the LTE technology platform that we should require public safety broadband networks to support in order to ensure interoperability? We note that, as LTE technology evolves, the 3GPP standard will develop new releases of the technology that exceed the capabilities of Release 8. Should we adopt rules to ensure that public safety agencies upgrade their networks to incorporate newer releases of LTE on a timely basis? We seek comment on the future evolution of the LTE technology platform and how it will support forward and backward compatibility and interoperability with Release 8. Further, we seek comments on the features of Release 9 and Release 10 that are necessary for applications such as real-time voice/video communications, location-based services, multicasting/broadcasting voice/video services, and other emergency preparedness related services. Could interoperability be maintained if we permitted use of multiple 3GPP releases within different networks? How do we ensure that all communications available over any network (*i.e.*, voice and data) are available across the nation? Is it necessary to mandate that as voice communications are supported, networks must be upgraded within an appropriate time frame? If voice is not required, what does this do for nationwide interoperability across the network? What are the costs of such an approach and do the benefits from having a truly interoperable network outweigh these costs? We further seek comment on how to address the use of future technology platforms that arise to ensure that they are interoperable and backward compatible with the LTE requirements designated herein? How can the Commission best accommodate these technologies to ensure continued innovation for the public safety broadband network?

---

[43] *See* Public Safety and Homeland Security Bureau Seeks Comment on Increasing Public Safety Interoperability by Promoting Competition for Public Safety Communications Technologies, PS Docket 10-168, *Public Notice*, DA 10-1556 (rel. Aug. 19, 2010) (*Competition Public Notice*).

[44] ARINC Comments on *Competition Public Notice* at 6 (Sept. 20, 2010).

[45] Arlington County Information Technology Advisory Commission Comments on *Competition Public Notice* at 1 (Sept. 13, 2010).

[46] APCO Project 25 Steering Committee Comments on *Competition Public Notice* at 10-11 (Sept. 20, 2010).

[47] *See supra* Section III.A.

[48] *See id.*

30. We also recognize that LTE currently allows the use of both IP version 4 (IPv4) and version 6 (IPv6). Would the use of both versions in various components of the nationwide network create obstacles to achieving interoperability, either now or in the future? Should the entire network be based on IPv6 from day one? What are the benefits and challenges of launching an all IPv6 network? What are the key advantages and disadvantages of having certain core network elements with IPv4 (capable of upgrading to IPv6 in future) while the rest of the network is based on IPv6? Would there be any time at which we should require all public safety broadband networks to migrate to IPv6? What would be the impact to application interoperability, particularly for real-time voice/video applications, should both versions coexist as networks transition to IPv6? We also seek comments on dual stack in order to support both IPv4 and IPv6. Should devices be required to support dual stack? Should any network element be required to support dual stack? Would such a requirement create any significant cost increase or added complexity? What are the costs of such requirements and how should they be borne?

31. We also note that, although the prevalent tunneling protocol in LTE is GTP-based, a PMIP-based tunneling protocol has also been specified in 3GPP Release 8. This protocol is necessary in order to implement certain LTE interfaces. Supporting this protocol would require the adoption of an additional interface, namely Gxc (interface between SGW and PCRF when PMIP is used on S5 or S8). Should we require that public safety broadband networks adopt, in addition to the interfaces specified in the *Third Report and Order*, PMIP and the corresponding additional interface, Gxc? What are the potential costs and benefits of implementing such a requirement?

5. System Identifiers

32. Compliance with 3GPP standards requires that public safety broadband networks be assigned network identification numbers.[49] As we noted in the *Technical Public Notice*,[50] the NPSTC BBTF Report identifies two alternatives for assigning network identification numbers to the regional or tribal networks: (1) use of a single PLMN ID for the entire public safety network, or (2) use of a different PLMN ID for each regional or tribal network.[51] We also noted the NPSTC BBTF Report's claim that, because of the limited availability of network numbers, only one-hundred or fewer network identification numbers may be assigned.[52] We sought comment on whether this proposed limitation could hamper implementation of the second approach.[53]

33. In comments responding to the *Technical Public Notice*, Alcatel-Lucent, Motorola and DC propose a hybrid scheme in which one separate PLMN ID would be assigned to each regional or tribal network and a single PLMN ID would be assigned for the overall nationwide network.[54] The PSCR has also expressed support for such a scheme.[55] These parties assert that assignment of a separate ID for each network is compliant with the 3GPP standards, and the assignment of a single ID for the whole

[49] *See, e.g.*, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Sharing; Architecture and functional description (Release 9), 3GPP TS 23.251 at 4.2.1 (2009).

[50] *See* Public Safety and Homeland Security Bureau Seeks Comment on Interoperability, Out of Band Emissions and Equipment Certification for 700 MHz Public Safety Broadband Networks, PS Docket 06-229, *Public Notice*, 25 FCC Rcd 5486 (PSHSB 2010) (*Technical Public Notice*).

[51] *See* NPSTC BBTF Report at 6.3.1.

[52] *See id.*

[53] *See Technical Public Notice* at 5487-88.

[54] For example, if there are 55 regional and tribal networks operational, there should be 56 PLMN IDs, one for each region, and one virtual one for the overall network. *See* Alcatel-Lucent Comments on *Technical Public Notice* at 7-8 (July 19, 2010); District of Columbia Comments on *Technical Public Notice* at 7 (July 16, 2010); Motorola Comments on *Technical Public Notice* at 19 (July 19, 2010).

[55] *See* Public Safety Communications Research Program, NAWG Meeting #2 Slide Presentation at 10, http://www.pscr.gov/projects/broadband/700mhz_demo_net/NAWG-meeting2-v2.pdf (last visited Dec. 13, 2010).

nationwide network facilitates roaming to other regional or tribal public safety networks and to commercial networks. We seek comment on this proposed hybrid scheme for the assignment of PLMN ID numbers. What are the benefits and disadvantages of such an approach? Were we not to adopt this approach, would the use of a single nationwide PLMN ID be adequate to support the envisioned network-of-networks architecture?

34. We also seek comment on the mechanism by which PLMN IDs for the public safety broadband network should be acquired and assigned. Commercial mobile network operators obtain PLMN IDs through a process, managed by the IMSI Oversight Council (IOC), which requires them to be members of the GSM association.[56] We seek comment on how we can enable public safety network operators to acquire these IDs without incurring the burdens associated with the IOC process. Is this a role that the PSBL could support? Would this be an appropriate role for NIST? Are there other entities that could apply for these IDs on behalf of all the regional or tribal network operators and, if so, how would they be enabled? How should the costs of obtaining these IDs be allocated and who should be responsible for payment?

6. Roaming Configurations

35. The 3GPP LTE standards set two categories of roaming: home-routed and local breakout. In home-routed roaming, the roamer's traffic is routed back to the home network to enable the use of home resources, while in local breakout roaming, the roamer utilizes the resources of the host network for desired services. The *Waiver Order* required the waiver recipients to support both methods.[57] We tentatively conclude that all public safety broadband networks should have the ability to support both categories of roaming. We seek comment on this tentative conclusion.

36. In the Plan, a recommendation was also made to require certain broadband commercial carriers to accommodate roaming by public safety broadband users. If, in a separate proceeding outside the scope of this item, we pursued such a requirement for commercial operators, are there any requirements that we should then impose on public safety broadband operators in this proceeding to ensure that their networks can interoperate with commercial broadband operators? Should the Commission take efforts in this proceeding to better enable public safety agencies to enter voluntary roaming agreements with commercial operators? If so, what should these incentives be?

7. Roaming Authentication and Internetworking Functions

37. As previously described, roamers will need to be authenticated in the visited network as they would be in their own networks. In the absence of a clearing house, these authentication functions and any additional clearing functions between regional or tribal public safety networks could impose significant technical, administrative, and cost burdens on each network operator. Therefore, we tentatively conclude that within the context of public safety broadband networks, there would be significant efficiency gains if such functions were performed by third party clearing houses rather than by each network operator. We seek comment on this tentative conclusion. To what extent such clearing houses can perform the functions stated here? Do they provide the performance, reliability and security that are required for public safety networks? Is this solution cost effective? Should there be a single third party clearing house or multiple of them? If multiple, what is the right number? Who should select the clearing houses and what should be the selection criteria? How should these clearing houses be compensated?

---

[56] "The IOC is an open industry committee of telecommunications companies and other organizations with a direct interest in the management of IMSI codes. An IMSI is a 15-digit number used within mobile phones that allows service operators to identify mobile terminals, for purposes of international roaming. The IOC is responsible for overseeing the management of IMSI codes that have been assigned to the United States and its possessions as authorized by the U.S. Department of State since 1996." IMSI Oversight Council, http://www.atis.org/ioc/index.asp.

[57] *See Waiver Order* at 5160 ¶ 45.

8. Interconnectivity of Regional or Tribal Broadband Networks

38. The anticipated set of regional or tribal broadband networks will not serve as a nationwide interoperable broadband network unless they are interconnected with adequate capacity to support the end-to-end interoperable connections traversing multiple networks and to support roaming connections. A number of alternative solutions for interconnectivity of regional or tribal broadband networks exist. While each of these solutions should have sufficient capacity, it is also important that any interconnectivity solution be timely (low delay), reliable, secure, and cost-effective. Three alternatives are outlined here for consideration, and we seek comment on each.

39. Direct interconnectivity provides direct dedicated connectivity between any two regional or tribal networks. This alternative can provide a high-performance, reliable, and secure solution; however, it cannot scale for a large number of networks, since a large number of interconnectivity links would be needed.[58] While this solution can be implemented in certain situations where high volume of traffic between two regional broadband networks warrants the associated cost of dedicated links, we tentatively conclude that this solution is not scalable and hence, not cost-effective. We seek comment on this tentative conclusion.

40. The public Internet can serve as an interconnection hub if all regional broadband networks are connected to it. We seek comment on this alternative. Does this solution meet the performance requirements of interconnectivity links? Is it reliable and secure for public safety needs? Is it cost effective? Can it be part of the solution complementing some other alternative? What would be that alternative?

41. Third party network operators can provide high performance, reliable and secure interconnectivity links with adequate capacity. The NPSTC BBTF Report recommends the establishment of a common clearing house for the purpose of roaming. While the topic of roaming and associated functions is addressed elsewhere in this notice, we seek comment here on the establishment of clearing house(s) for interconnectivity links. Such clearing house(s) can provide interconnectivity among all public safety regional networks on a nationwide basis through secure and private networks using IPX protocol. We seek comment on these matters. To what extent can such clearing houses perform the function stated here? Do they provide the performance, reliability and security that are required for public safety networks? Is this solution cost effective? For the purpose of interconnectivity, should there be a single third-party provider or multiple providers? If multiple, what is the right number? Should the PSBL or the network operators select the providers? What should be the selection criteria?

42. In addition to these three alternatives for interconnectivity of the regional broadband networks, we seek comment on whether there are any other alternatives that would meet public safety's performance, reliability, and security requirements in a cost-effective manner? How much will these approaches cost and how should these approaches be paid for? How should responsibility for such interconnection be handled?

9. Prioritization and Quality of Service

43. We seek comment on how public safety broadband networks should support both prioritization and quality of service among connections as well as applications over these connections. Prioritization is the network's ability to determine which connections have priority over others in connecting to the network at times of emergency and network congestion. Quality of service (QoS) is the network's ability to assign classes to different applications based on certain performance attributes and objectives, and maintain the network performance for the application (i.e., QoS) within the acceptable range. Thus, prioritization deals with the connection to the network while QoS deals with the treatment

[58] The number of interconnectivity links grows exponentially with the number of interconnected networks. If the number of networks is "n", the number of links connecting them would be "(n-1)n/2".

of traffic after the connection is established.

44. In a broadband network when users attempt to establish a connection, certain administrative actions take place. In addition to authentication, authorization and some other administrative procedures, the network through a Connection Admission Control (CAC) function will also determine whether it has sufficient resources to accept a new connection. These resources include bandwidth, processing power, codes and other operational elements within the system. During an emergency, networks may be unavailable for a number of reasons. This is when the Priority Access mechanism plays a role.

45. Prioritization within a public safety broadband network ensures users of high priority can establish connections with higher level of certainty relative to users of low priority. In general, priority levels for connections can be defined and assigned based on various criteria including user's role (or user priority), user application types, incident type, etc. As a matter of principle, for a given application type, connections initiated by users with higher user priority take priority over the connections initiated by users with lower user priority. However, such priority may not hold if the application types are different. For example, a priority scheme may choose not to provide a connection priority to a higher priority user with video application rather than to a lower priority user with voice application. The determination of connection priority levels and its mapping to user priority, application type and other attributes is a matter that hinges upon both the public safety needs and the technology supporting it.

46. LTE provides priority mechanisms through capabilities such as Allocation Retention Priority (ARP), which assigns fifteen levels of priority with two bits to flag preemption capability and vulnerability for a connection, QoS Class Identifier (QCI), which assumes nine levels of prioritization for various application types, and Access Class barring, which would allow any fourteen levels of the access classes to be barred from the network at times of congestion. We seek comments on these capabilities. Which features specific to QOS and Priority Access in the December 2009 freeze of 3GPP LTE Release 8 are currently being developed for implementation in LTE equipment? Are these adequate to support a solid framework for public safety needs relating to priority access and interoperability? Are they all to be used for such framework or should we look at different approaches?

10. Mobility and Handover

47. As users move within a network operator's coverage area, their communication sessions need to continue without any interruption. In other words, when a user moves from one cell coverage area with an eNodeB that serves that user to another cell coverage area with a different serving eNodeB, its connecting link need to be handed off from the old eNodeB to the new eNodeB in a smooth and seamless manner. LTE supports this feature, and hence, we tentatively conclude that each operator's network must support seamless handover within its coverage region. We seek comment on this tentative conclusion.

48. LTE supports two methods of handover, one is through direct links between source eNodeB and target eNodeB, called X2 based handover, and the other one through indirect links between eNodeBs through the core, called S1 based handover. We seek comment on viability and availability of each option. What are advantages and disadvantages of each one? Should we require one method and not the other one, or should we require both, or should we require neither? Is there any impact on interoperability depending on the solution we select?

49. Additionally we seek comment, and raise the same questions as above, for the case where handover occurs between two eNodeBs from two different neighboring networks. This would be considered roaming. How is seamless handover possible in this situation?

50. LTE supports mobility across the cellular network while maintaining a minimum level of performance, and supporting seamless handover. Do we need to set up support for a minimum speed (in mph) for mobility and seamless handover while within a regional or tribal network? Similarly, do we need to set up support for a minimum speed for mobility and seamless handover while crossing

neighboring networks (roaming)?

11. Out-of-Band Emissions and Related Requirements

51. It is imperative that the networks that comprise the public safety broadband network are protected from interference from adjacent and near operations or nationwide interoperability could be harmed. Accordingly, in the *Waiver Order*, we noted that "[a] number of measures can be considered to reduce the impact of interference to mobile wireless systems" and that "[a]gencies should use mutually agreed upon practical solutions for eliminating Out-of-Band Emissions (OOBE) or other interference, such as software parameter changes, site configuration modifications, ensuring a reasonable distance of site equipment beyond the border or the reduction of transmitter power levels towards the border."[59] As a waiver condition, we required that, for operations in the 763-768 MHz band and the 793-798 MHz band, the power of any emission outside the lessee's frequency band(s) of operation shall be attenuated below the transmitter power (P) within the licensed band(s) of operation, measured in watts, in accordance with the following:

- On any frequency outside the 763-768 MHz band, the power of any emission shall be attenuated outside the band below the transmitter power (P) by at least 43 + 10 log (P) dB; and
- On any frequency outside the 793-798 MHz band, the power of any emission shall be attenuated outside the band below the transmitter power (P) by at least 43 + 10 log (P) dB.[60]

52. We further noted that "[c]ompliance with the provisions of paragraphs above in this section is based on the use of measurement instrumentation employing a resolution bandwidth of 100 kHz or greater."[61] We clarified, however, that "in the 100 kHz bands immediately outside and adjacent to the frequency block, a resolution bandwidth of at least 30 kHz may be employed."[62] In addition, we observed that "OOBE standards are already in place with respect to the public safety narrowband spectrum" and that "the 700 MHz public safety spectrum allocation already includes a guard band between the public safety broadband and narrowband allocations."[63] Our analysis demonstrates that compliance with these interference requirements will protect against interference into adjacent or near operations for the public safety broadband network.

53. In the *Technical Public Notice*, we sought comment on "the benefits of [the OOBE limit adopted in the *Waiver Order*], or of any proposed alternative specification, for the public safety broadband network in protecting and promoting the use of both the Public Safety Broadband (PSBB) Block and the D Block and minimizing interference."[64] We also inquired whether, "[i]f more stringent OOBE limits were applied to the PSBB Block, [it would] be possible to attenuate signals outside the band without a guard band between D Block and the PSBB Block."[65]

54. Most of the parties that commented on the OOBE limit specified in the *Waiver Order* expressed support for it.[66] We therefore tentatively conclude to adopt this limit for the nationwide public

---

[59] *Waiver Order* at 5159 ¶ 43.

[60] *Id.* at 5159 ¶ 44. The *Waiver Order* also noted that 47 C.F.R. § 90.543(e) remains in effect. *See id.*

[61] *See id.*

[62] *See id.*

[63] *See* id. (*citing* 47 C.F.R. § 90.543(e)).

[64] *See Technical Public Notice* at 5489.

[65] *See id.*

[66] *See* Alcatel Lucent Comments on *Technical Public Notice* at 12 (July 19, 2010); AT&T Comments on *Technical Public Notice* at 18-19 (July 19, 2010); Bay Area Comments on *Technical Public Notice* at 6 (July 19, 2010); Ericsson Comments on (continued....)

safety broadband network. Our analysis demonstrates that these parameters provide protection against harmful interference for the public safety broadband network and will further advance interoperability across the network. We seek comment on this tentative conclusion.

12. Applications

55. One means of facilitating roaming across public safety broadband networks is to ensure that users of each network have access to a common set of applications. In the *Waiver Order* we required, as a waiver condition, that each early deployed network support five applications recommended in the NPSTC BBTF Report: (1) Internet access; (2) Virtual Private Network (VPN) access to any authorized site and to home networks;[67] (3) a status or information "homepage;"[68] (4) provision of network access for users under the Incident Command System;[69] and (5) field-based server applications.[70] We sought comment on this list in the *Technical Public Notice*, and the comments received in response were generally supportive of the list.[71] We therefore tentatively conclude that we should adopt these as a common set of applications that must be fully supported by each public safety broadband network and that this is appropriate to advance interoperability. To further our ability to specify interoperability requirements, we here delve deeper into the technical characteristics of these five applications. Should Internet access enable fully transparent use of any Internet-based application (e.g., using different transport and application protocols) or just a restricted subset? Does VPN access imply client-based VPNs and if, so, is any network support required? If the network does not allow all protocols, what kinds of VPN protocols should be allowed, such as IPSec, PPTP or L2TP? Does this application imply a requirement for the network to operate such a server and how should it be identified? Does the support for field-based server applications imply support for specific protocols or simply the ability to reach a web server via HTTP and HTTPS? In general, should users of the public safety broadband network expect that the network allows all applications or restricts the user to certain protocols, ports and applications, either in their home network or while roaming?

(Continued from previous page)
Technical Public Notice at 5 (July 19, 2010); IP Wireless Comments on *Technical Public Notice* at 5 (July 20, 2010); Motorola Comments on *Technical Public Notice* at 30 (July 19, 2010); Sprint Comments on *Technical Public Notice* at 8 (July 19, 2010); T-Mobile Comments on *Technical Public Notice* at 7 (July 19, 2010); TIA Comments on *Technical Public Notice* at 2 (July 19, 2010).

[67] "The regional operator and commercial networks operating in conjunction with the PSBL shall be required to allow establishment and use of VPN connections by roaming users on their networks to other networks." NPSTC BBTF Report at Section 6.2.2.

[68] "Public safety or public/private partnership network operators shall provide a universal method to obtain a "home page" for visitors to the system. This "home page" will facilitate access to and distribution of available applications, alerts, incident-specific information, system status information, and information that the operator deems important to share with visitors to the system." NPSTC BBTF Report at Section 6.2.3.

[69] "First responders, emergency response support, and all other mutual aid responders managed under ICS structure of a requesting agency served by a public safety broadband network shall be provided access to that network to carry out incident objectives and communicate with their home networks." NPSTC BBTF Report at Section 6.2.5. For purposes of our proposed rules, *see infra* app. B, we tentatively adopt a definition of "Incident Command System" used by the Federal Emergency Management Agency (FEMA). *See* FEMA, http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm.

[70] "The regional systems shall support the use of field-deployed server applications. This requirement includes the need for client devices to consistently and continuously reach each server-based system from any other location on the Internet. The capability is not required for every subscriber device on the broadband network but is limited to a subset of the users that actually require such a feature." NPSTC BBTF Report at Section 6.2.7.

[71] *See* Bay Area Comments on *Technical Public Notice* at 1 (July 19, 2010); District of Columbia Comments on *Technical Public Notice* at 2-3 (July 16, 2010); Harris Comments on *Technical Public Notice* at 3 (July 19, 2010); Motorola Comments on *Technical Public Notice* at 7 (July 19, 2010). Because we believe that interoperability must be achieved at all layers of communications, including at the applications layer, we disagree with the claim that mandating a minimum set of applications would "add costs and complexity" without providing "any concomitant benefits." *See* AT&T Comments on *Technical Public Notice* at 6 (July 19, 2010).

56. We also seek comment on whether other applications should be added to our proposed list of required applications. We seek comment on how to best ensure this list of required applications is current. The NPSTC BBTF Report recommends that in addition to the five applications specified in the *Waiver Order*, two other applications should be required to be supported by public safety broadband networks: the remaining two are (1) Status/Information "SMS-MMS Messaging" and (2) Land Mobile Radio (LMR) Gateway Devices. We seek comment on whether to require public safety networks to support these applications as well. In addition, we note that the NPSTC BBTF Report also identifies four "desired" applications: (1) Location Based Data Capability; (2) One-to-Many Communications across all Media; (3) LMR Voice; and (4) Public Switched Telephone Network (PSTN) Voice. We seek comment on whether we should also require, or encourage, public safety broadband systems to be capable of supporting any or all of these "desired" applications. What is the potential for each of these additional applications to contribute to nationwide interoperability? Are these applications capable of being supported at the present stage of technology and standards development? If not, when would they be ready? Are there any other applications whose adoption should be mandatory or that the Commission should consider mandating or encouraging for adoption in the future? What would be the costs associated with any such mandate?

57. The Commission anticipates that an all-IP wireless broadband LTE network will enable public safety agencies to select from a diverse array of evolving applications and services to support their communications needs, including real-time voice and video communications. We seek comment on how we can promote the interoperability of key applications that are not included among the set of common applications that all public safety networks will be required to support. What interfaces impact application interoperability? Should we require that public safety networks support additional interfaces essential to maintaining application interoperability?

13. Interconnection With Legacy Public Safety Networks

58. Capabilities exist for the support of public safety communication services across both narrowband and broadband networks. The interconnection of broadband networks with co-existing narrowband networks will enable public safety agencies to better integrate their communications and avoid the unnecessary stranding of assets. We seek comment on how to address the interconnection of existing narrowband public safety networks (both voice and data) in multiple bands (Legacy Networks) with the public safety broadband network in the absence of the Public/Private Partnership called for in the *Second Report and Order*. What are the advantages and disadvantages of using the gateways between Legacy Networks and public safety broadband networks? What are the current and future capabilities and availabilities of gateways between Legacy Networks and public safety broadband networks? Can these gateways between Legacy and public safety broadband networks offer both voice and data services? What are the costs of imposing such requirements and how are these costs best allocated? How can the public safety community cover such costs? What is the appropriate time frame for achieving such interoperability?

14. Performance

59. We recognize the importance of ensuring that public safety broadband networks have adequate capacity, spectral efficiency, QoS and overall performance to achieve nationwide interoperability. Spectrum is a valuable public resource and the Commission is committed to ensuring that this resource is used efficiently. Moreover, we believe that imposing baseline operability requirements on public safety broadband networks ensures that disparate networks are capable of interoperating. We tentatively conclude that in order to ensure baseline operability and to ensure the efficient use of the radio frequency resource, it is appropriate to adopt performance requirements for public safety broadband networks. We seek comment on this tentative conclusion.

60. The radio access network is essential in providing public safety with wireless communications between user devices and the network operator antennas on the other end. Radio

network planning and baseline operability requirements are key to achieving high spectral efficiency and coverage in order to deliver broadband services to a largest possible number of users. If public safety networks are not built with baseline operability requirements and high spectral efficiency, both operability and interoperability may fail in an emergency when the demand for communications is greatest. This baseline set of operability requirements needs to start at the Radio Access part of the LTE network. The basic requirements for any advanced cellular network are to meet coverage and quality targets. These requirements are also related to how the end user experiences the network. Coverage first targets the mean of the population or geographic area the network is covering with agreed upon location availability, *i.e.* the availability to get service. The requirements furthermore specify the signal strength values that need to be met inside the different area types. The quality targets are related to factors such as QoS and the success of call completion. Therefore it is imperative that a minimum set amount of requirements to ensure access to applications and other communications tools will enable interoperable public safety broadband networks nationwide, something that has never materialized to date for public safety.

61. Accordingly, we tentatively conclude that we should require public safety broadband networks to provide outdoor coverage at minimum data rates[72] of 256 Kbps uplink (UL) and 768 Kbps downlink (DL) for all types of devices, for a single user at the cell edge.[73] We further tentatively conclude that as part of its initial design, each network must provide the minimum data rates base on a sector loading of seventy percent throughout the entire network.[74] Finally, we tentatively conclude to require each public safety network operator to certify, within thirty days of its date of service availability, that its network is capable of achieving these data rates. Such certification will need to be based on a representation of the actual "as-built" network and accompanied by UL and DL data rate plots that map specific performance levels. This approach would ensure a minimum level of performance across the network. We seek comment on these tentative conclusions. We also seek comment on the potential costs for such a requirement? We also seek comment on the appropriate geographic areas for making these measurements and the time frames for compliance. We tentatively conclude that these requirements should be met prior to the date that a network achieves service availability.[75] Finally, to the extent that commenters recommend that we not impose such a requirement, how will this impact interoperability? If there is not a baseline level of service available on a network wherever public safety users have access to the broadband network, how is interoperability achieved?

62. Furthermore, we seek additional comments on these technical specifications. Are there additional requirements that should be included to ensure access to applications and other communications tools, which will enable interoperable public safety broadband networks nationwide? Should the minimum cell edge Spectral Efficiency be required on the UL or DL or both? Should an average, instead of a minimum, cell edge data rate be used, and if so, what should that requirement be? To generate average spectral efficiency and cell edge spectral efficiency levels, should we assume a mix of applications and usage scenarios, with users evenly distributed throughout the coverage area? Should we define the certification (UL and DL data plots) more specifically, *i.e.*, define all the specific map performance levels required on the plots? Should the plots be computer simulation or based on actual drive test data of the actual "as-built" network? Should coverage maps be accompanied with information giving site locations? Should coverage maps be provided for each Phase of network build? Is it

[72] The data rate in this context is measured and defined as the physical layer provided rate with less than or equal to a 10% block error rate. A 5+5 MHz system typically uses twenty percent overhead on the DL and about twelve percent overhead on the UL.

[73] In 3GPP TR 36.913, the metric used for the cell edge assessment is the 5-percentile user throughput, which is obtained from the cumulative distribution function (CDF) of the user throughput. *See* 3rd Generation Partnership Project, "Requirements for Further Advancements for E-UTRA (LTE Advanced) (Release 8)," 3GPP TR 36.913 (2008), *available at* http://www.3gpp.org/ftp/Specs/html-info/36913.htm.

[74] Seventy-percent loading per sector indicates that the sector is loaded to this level of traffic.

[75] *See supra* note 32.

acceptable to use seventy percent loading per sector (both UL and DL)? Should we use Section 3.2 of the NPSTC Statement of Requirements document as a reference for assumed traffic loading for various applications?[76] Should it be possible for one user, at the cell edge, to achieve 768 kb/s DL or multiple users and 256 kb/s UL? Should the Commission require periodic reports and updates on coverage maps, actual usage and traffic data, in order to access and/or modify the spectral efficiency requirements? Finally, we seek comment on the costs and benefits for the additional requirements.

15. Network Capacity

63. As commercial technologies become increasingly efficient, it is important to ensure that public safety broadband networks are able to capture these efficiency gains. The network capacity of a cellular system in terms of supporting user traffic is the "maximum achievable aggregate data rate" in bits per second.[77] This capacity largely depends on the locations where potential users would receive service (distance from the cell tower, and being indoor / outdoor), available bandwidth, technology/communications protocols, transmitter, both user equipment and base stations, powers and noise, among other environmental factors.[78]

64. The capacity of a system within a cell site is initially set to provide a minimum level of service quality for the coverage area. As the number of users grows, the capacity is added or alternatively, resources are added, to maintain the service quality. Among these resources are eNodeB backhaul capacity and core capacity. We seek comment on the adequacy of these resources and whether we should ensure they are adequate to support public safety requirements. Should we set a minimum level of capacity for backhaul and core? For instance, for a three sector cell site or eNodeB with an average of 1.8 bits/Hz spectrum efficiency throughout the site, the total capacity is twenty-seven Mbps. Should we consider rules for backhaul links that can handle this amount of traffic? Should we consider any other suggestions for backhaul capacity? Should we consider similar assessments for the capacity of the core, or should this type of assessment be left to local design considerations? To what extent, if at all, could interoperability be impaired if we leave capacity considerations to localities? What are the cost implications of such requirements being imposed?

16. Security and Encryption

65. Secure communications are of vital importance to public safety and are needed to encourage increased usage and reliance on the network. It is crucial to maintain a reliable communication and to protect public safety user traffic from intentional and unintentional intrusion attacks. Security schemes are implemented at various levels and segments of the network to achieve an end to end reliable and secure communications. According to LTE specifications, "five security feature groups are defined. Each of these feature groups meets certain threats and accomplishes certain security objectives.

- Network access security (I): the set of security features that provide users with secure access to 3G services and which, in particular, protect against attacks on the (radio) access link;
- Support all of IP-LTE technology platform, particularly the 3GPP standard, Universal Terrestrial Radio Access (E-UTRA), Release 8 (LTE), and associated Evolved Packet Core (EPC) as required by the *Third Report and Order* above.

[76] *See* National Public Safety Telecommunications Council, Public Safety 700 MHz Broadband Statement of Requirements at Section 3.2 (2007).

[77] When user service profiles are known, and all users have the same service profile and environmentally bear the same condition, the capacity can also be measured as the "maximum number of users" that the system can support. A user service profile is a set of applications with the frequency of use.

[78] These factors along with a fair scheduling scheme at the cell tower (dividing bandwidth among users) will determine the data rate for each user. Capacity is then the aggregate data rate of all users that are scattered within an area transmitting and receiving (over forward and reverse link) at their maximum available data rate.

- User domain security (III): the set of security features that secure access to mobile stations;
- Application domain security (IV): the set of security features that enable applications in the user and in the provider domain to securely exchange messages;
- Visibility and configurability of security (V): the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature."[79]

66. Each aspect of security as defined above is specified in various standards. For example, network access security is specified in 3GPP TS 33.401, and network domain security is specified in 3GPP TS 33.210. The NPSTC BBTF Report required the optional security layer features specified in 3GPP TS 33.401. The *Waiver Order* adopted these features to be technologically supported with additional specifics to follow in the future. More specifically, the NPSTC BBTF report required security features for three protocol layers as specified in 3GPP TS 33.401. They are LTE signaling layer security features over the Radio Resource Control (RRC) protocol layer (UE and eNodeB), EPC signaling layer security features over the Non Access Stratum (NAS) protocol layer (UE and MME) and user data/control layer security features over the Packet Data Convergence Sublayer (PDCP) protocol layer (UE and eNodeB). We tentatively conclude that all three security features for the network access security, as specified in 3GPP TS 33.401, should be fully required.[80] Are these appropriate security features to ensure the security of the public safety broadband network? We seek comment on this tentative conclusion. Is this sufficient to ensure network access security? Does the public safety community require additional security? If so, what is this and what are the costs incurred to achieve this?

67. We recognize that 3GPP TS 33.210 provides specifications for network domain security. Should we adopt rules for network domain security? If so, what should they be? Do the optional features specified in 3GPP TS 33.210 fully serve the purpose of network domain security? Are they sufficient? Which optional features should be selected? Would there be any interoperability issues should the commission choose not to require network domain security features, or not to select them?[81]

68. Application domain security as stated above and as specified in 3GPP TS 33.102 and TS 31.111 is an optional feature. Application domain security overall enhances network security. Should the Commission adopt rules for application domain security? Do the optional features specified in these standard specifications fully serve the purpose of application domain security? Are they sufficient? Which optional features should be selected? Would there be any interoperability issues should the Commission choose not to require application domain security features, or not to select them?

69. Visibility and configurability of security as stated above and as specified in 3GPP TS 33.102 and TS 22.101 is an optional feature. Should the Commission adopt rules for visibility and configurability of security? Are these necessary to ensure the operability and interoperability of the public safety broadband network? Do the optional features specified in these standard specifications fully serve the purpose of visibility and configurability of security? Are they sufficient? Which optional features should be selected? Would there be any interoperability issues should the Commission choose not to require visibility and configurability of security features, or not to select them? What are the cost implications of such requirements?

---

[79] 3rd Generation Partnership Project, "3GPP System Architecture Evolution (SAE); Security Architecture", 3GPP TS 33.401 (2008), *available at* http://ftp.3gpp.org/specs/html-info/33401.htm.

[80] Two aspects of security features namely, "integrity protection and verification of data" and "cyphering/decyphering of data" should be supported for signaling. In addition "cyphering/decyphering of data" should be supported for user traffic.

[81] User domain security as stated above is a mandatory feature according to 3GPP TS 33.102 for the operation of the LTE network. *See* 3rd Generation Partnership Project, "3G Security; Security architecture (Release 8)," 3GPP TS 33.102 (2009). Therefore, the public safety broadband network must support it and it is not the subject of this notice.

17. Robustness and Hardening

70. As many public safety entities and organizations have stated in their comments, it is critical that public safety have available to it a resilient and reliable public safety broadband network.[82] Many of the comments acknowledge public safety's need for sites equipped with generator and battery backup power.[83] Accordingly, we seek comment on whether we should require more or less than eight hours of back-up power to each eNodeB site within a public safety broadband network? Should the Commission require more or less than eight hours of back-up power to specific eNodeB sites within a pre-defined area of the public safety broadband network, such as high traffic areas or urban areas? Should the Commission require less than eight hours of back-up power to each eNodeB site located on building rooftops, apartments or similar structures? Besides the use of batteries for back-up power at each eNodeB site, are there other alternatives such as solar power?[84] Should the requirement include at least eight hours for all of the network equipment located at the RAN site location? How would compliance with backup power requirement be determined? Should there be a requirement to file something with the Commission for verification (*e.g.*, self-certification, etc.)? Should the Commission propose to require each public safety network operator to certify, within thirty days of its date of service availability, that its eNodeB sites are capable of achieving the backup power requirement? What are the costs of such requirements and how should they be borne? Are there other ways to achieve the same results?

18. Coverage Requirements

71. Coverage is an important consideration in ensuring that the public safety broadband network is interoperable on a nationwide basis. Accordingly, we tentatively conclude that we should impose coverage and performance requirements on the networks that will comprise the nationwide public safety broadband network. We seek comment on this tentative conclusion. Additionally, we seek comment on whether the Commission should impose either a population- or geographic-based build-out requirement and whether such a requirement should also include interim benchmarks for the percentage of population or geographic area covered. We seek comment on the advantages and disadvantages of adopting either method as well as on how to structure the percentage requirements to maximize coverage while preserving the economic viability of a nationwide network. Also, we seek comment on whether the Commission should require each public safety network operator to certify, within thirty days of achieving service availability, its compliance with any coverage requirements we adopt, and whether there should there be ongoing certification requirements.

72. One approach we can take is to require that the public safety broadband networks cover a certain population or geographic benchmark. Such requirements could impose costs on public safety but could ensure that an increased percentage of the nation benefits from the public safety broadband network and hence, is interoperable. Is this an appropriate requirement to impose on public safety? If so, what percentage of population-based or geographic coverage benchmark should we adopt for the public safety broadband network? Should coverage requirements be implemented over a fifteen-year period? If a fifteen-year period were implemented, should the Commission require that the network achieve 40 percent coverage within four years, 75 percent within ten years and 99 percent within fifteen years?[85]

---

[82] *See, e.g.*, APCO Comments on *Third Further Notice* at 15 (Nov. 3, 2008); Joint Public Safety Commenters Comments on *Third Further Notice* at 13 (Nov. 3, 2008); NATOA Comments on *Third Further Notice* at 15-16 (Nov. 3, 2008); NPSTC Comments on *Third Further Notice* at 17-18 (Nov. 3, 2008).

[83] *See id; see also* New York City Comments on *Third Further Notice* at 11 Nov. 3, 2008; PSST Comments on *Third Further Notice* at 20-21 (Nov. 3, 2008); RPC 20 Comments on *Third Further Notice* at 7-8 (Nov. 3, 2008); TIA Comments on *Third Further Notice* at 11 (Oct. 31, 2008).

[84] *See* Emergency Response Interoperability Center Technical Advisory Committee Filing, PS Docket 06-229, at 6-7 (Oct. 31, 2010) (ERIC TAC Filing).

[85] In evaluating public safety broadband networks' compliance with such requirements, we would refer to the most recently available U.S. Census Data.

Would significant population, as required for the waiver recipients, be more appropriate? Also, are their other coverage benchmarks that might be reasonable and ensure nationwide interoperability? If we do not impose such requirements, how do we ensure that coverage of the network is extensive enough to meet the needs of public safety? What would be the costs of such approaches?

73. We recognize that commercial providers often have economic incentives to concentrate their network deployments in high population areas but that public safety broadband users will require coverage availability even in highly rural areas. In order to promote better coverage in rural areas, should the Commission require that the coverage area of the network reach major highways and interstates? In lieu of a population or geographic benchmark in rural areas, should the Commission propose a different benchmark, such as vehicular traffic counts on major highways and interstates? Finally, we seek comment on whether other requirements should be imposed to ensure that public safety broadband networks achieve a sufficient baseline of operability, even in rural areas, to enable the development of an interoperable nationwide network.

19. Coverage Reliability

74. While geographic coverage of a network is important, network availability is another critical factor. An unreliable network is inoperable, and therefore not interoperable. Areas of poor performance and inadequate coverage must be identified as well as assessed to adequately maintain the operability and interoperability of the nationwide network.

75. We seek comment on whether to impose coverage reliability requirements on public safety network operators. In particular, we tentatively conclude that the network should provide outdoor coverage reliability at a probability of coverage of 95 percent for all services and applications throughout the network that is a standard commonly used today by the Land Mobile Radio and cellular industries. We seek comment on this tentative proposal. Is this a stringent enough approach? What are the costs of such an approach? Should the broadband network be designed to meet 95 percent coverage reliability on all named streets within the service area (not including in-building coverage)? If not 95 percent probability, what percentage of outdoor reliability should be used? Should the service area be defined geographically, by the county boundaries, if not by what boundary? What should the time frame be for meeting this requirement? Are there methods to increase the probability of coverage with less or more spectrum, without adding eNodeB sites, repeaters, distributed antennas systems (DAS) or In-Building systems? Should the proposed 95% Probability of Coverage requirement apply only to outdoor environments? Is a different percentage requirement appropriate for indoor environments?

20. Interference Coordination

76. In the *Waiver Order* we noted the importance of providing "a solid mechanism for ensuring efficient, interference-free implementation and evolution of regional or tribal, statewide or local early-deployed networks."[86] Accordingly, we required as a condition of deployment, that prior to deployment each waiver recipient "coordinate and address interference mitigation needs with any adjacent or bordering jurisdictions that also plan deployment." We further required waiver recipients to memorialize these agreements in writing and submit them to ERIC within 30 days of their completion. In addition, we required "that parties provide ERIC with notice of any changes or updates within 30 days" and provided that, "[s]hould the parties be unable to reach an agreement within 90 days after coordination begins, they may submit the dispute to the Bureau for resolution."

77. It is critical as we move forward that networks are coordinated with one another to protect against harmful interference and ensure interoperability. Accordingly, we tentatively conclude that we should require that, ninety days prior to deployment, a public safety broadband network operator must notify any adjacent or bordering jurisdiction of its plans for deployment. Each notified jurisdiction

[86] *See Waiver Order* at 5159 ¶ 42.

would then have the opportunity to request that the parties negotiate a written coordination agreement. We would require that any such agreement be submitted to the Bureau within thirty days of its execution. Parties unable to reach an agreement within ninety days could refer their dispute to the Bureau for resolution. We seek comment on this tentative conclusion.

78. We also observe that public safety broadband networks should employ interference mitigation techniques that will avoid signal/spectral efficiency degradation issues within a region and between overlapping with adjacent regions. Should the Commission impose such requirements and what are the costs and benefits of such an approach? Should the Commission require eNodeB features such as Static Inter-cell Interference Coordination (ICIC) for interference mitigation?[87] Are there eNodeB or other features, either currently available or being studied within 3GPP, that are superior or better suited for interference coordination and mitigation? Should the Commission require the eNodeB feature Semi-static ICIC?[88] What benefit would Semi-static ICIC offer compared to Static ICIC? Should the Commission require the eNodeB feature Semi-static ICIC? How would compliance with these eNodeB feature requirements be determined? Should there be a requirement to file something with the Commission for verification (*e.g.*, self-certification, etc.)? What other techniques or features are currently available for the eNodeB, that can be implemented immediately using the existing functionality for interference mitigation or coordination, besides typical network planning techniques?[89]

79. In addition, as both commercial and public safety 700 MHz networks add eNodeB sites in subsequent phases to address coverage, capacity, and spectral efficiency issues that may arise once more bandwidth intensive applications are added to the system, the possibility exists that performance of one network could be negatively impacted by another network operating in adjacent spectrum. This possibility is increased if networks are built according to different site topologies and densities. Given this possibility, we seek comment on whether we should require public safety broadband networks to coordinate with operators in adjacent spectrum, as commercial operators do, and take any steps necessary to ensure that the performance of the public safety network is not degraded below the required levels due to interference from spectrally adjacent networks.

21. Incumbent Narrowband Operations

80. In the *Second Report and Order*, the Commission recognized that in realigning the 700 MHz public safety spectrum to create a consolidated broadband allocation, certain incumbent public safety narrowband operations in the lower portion of the public safety band (TV Channels 63 and 68, and the upper 1 megahertz of TV Channels 64 and 69) would need to be relocated to the new consolidated public safety narrowband allocation.[90] The Commission adopted a plan that would require the D Block auction winner to fund that relocation at a capped amount, with the PSBL administering the process.[91] Due to the auction failure, this relocation funding mechanism was never put into effect, and these

[87] Within the 3GPP, several techniques have been proposed for inter-cell interference coordination (ICIC). The Static ICIC feature is intended to minimize inter-cell interference by providing a fixed, static method of allocating resource blocks between cells within the system. Static ICIC method relies exclusively on information contained in each eNodeB, and as such does not require the use of messaging across the X2 interference between eNodeBs nor does it require any kind of dynamic coordination between eNodeB scheduler processes.

[88] Semi-static ICIC is another feature proposed within the 3GPP. This feature is intended to minimize intercell interference by making use of 3GPP standardized messaging across the X2 interference between eNodeBs. Measurement reports exchanged between eNodeBs over the X2 interface can be used to support interference coordination in both the downlink and uplink. Semi-static ICIC relies on three types of measurement reports between eNodeBs.

[89] Typical network planning techniques include: selecting appropriate antenna patterns, adjusting the individual sector antenna tilts or power levels, and selecting optimal site locations and site separation distances.

[90] *Second Report and Order* 22 FCC Rcd at 15409, 15410 ¶¶ 329, 332.

[91] *Id.* at 15411-14 ¶¶ 336-344.

incumbent narrowband operations continue to operate in the public safety broadband spectrum.

81. In the *Waiver Order*, we accounted for these incumbent narrowband operations, by requiring waiver recipients either to protect the incumbents through appropriate engineering measures or geographic exclusion, or to relocate them at their own expense.[92] For waiver recipients proposing to protect an incumbent by engineering measures, we required the waiver recipient to obtain the consent of the narrowband system operator to its proposed method of protection[93]. Further, we required waiver recipients to protect public safety narrowband deployments on the former narrowband channels present in adjacent regions.[94] We took these actions subject to further consideration of relocation issues in this proceeding, but declined at that time to address the costs for such relocation or any potential reimbursement. [95]

82. We remain committed to providing for the relocation of narrowband incumbents from the public safety broadband spectrum in order to ensure that the public safety broadband spectrum can be fully utilized to support nationwide broadband interoperability. We seek comment on how best to facilitate such relocation. For example, should prospective broadband operators be required to include plans for narrowband relocation as part of their deployment proposals? If broadband operators incur relocation expenses, should they be entitled to reimbursement in the event that the Commission adopts a relocation funding mechanism?

83. In the interim, we seek to ensure that narrowband incumbents who continue to operate temporarily in the broadband spectrum will be protected from potential harmful interference until they are relocated. Therefore, we tentatively conclude that as an interim rule, pending future disposition of relocation and reimbursement issues, we will require all public safety broadband operators to abide by the same conditions relating to narrowband incumbents that were imposed in the *Waiver Order*, *i.e.*, each broadband operator must protect any potentially affected narrowband incumbent by technical measures or geographic separation, or must relocate the incumbent at its own expense. We seek comment on this tentative conclusion. Are other technical rules needed to protect these incumbent narrowband operations from harmful interference? If so, what should be the basis of these technical rules (e.g., distance separation, contour overlap etc.)? If a broadband operator relies on geographic separation, should we adopt signal strength, antenna height, or other technical restrictions for the "borders" between these operations?

84. We also tentatively conclude that, as in the *Waiver Order*, each public safety broadband operator should be required to notify and obtain the consent of the potentially affected narrowband incumbent as to its proposed method of protection. We seek comment on this tentative conclusion. Should we adopt procedural rules to govern the notification process, *e.g.*, by requiring notification to the incumbent narrowband operator within a specified time period? What should the notification include? If we require consent from the incumbent narrowband operator, should we adopt a time period for such consent (*e.g.*, 60 days), and if consent is not received within that time period, should we there be a path for elevating the issue to the Bureau or Commission? If so, what should that path be and what should the time requirements be?

[92] *Waiver Order*, 25 FCC Rcd at 5168, ¶¶ 72-73.

[93] *Id.*

[94] *Id.*

[95] *Id.*

B. Public Safety Roaming on Public Safety Broadband Networks

85. In an effort to enhance the utility of the public safety broadband networks recently authorized by early build out waivers[96] and to foster the continued evolution towards a national public safety broadband network in the 700 MHz band, we now seek to establish technical requirements and a regulatory framework to govern public safety roaming on 700 MHz public safety broadband networks (intra-system roaming).[97] We expect that this framework will enhance interoperability in both day-to-day and emergency situations.

86. As an initial matter, we note that this *Fourth Further Notice* deals exclusively with roaming by public safety users on broadband networks operating in the existing 700 MHz public safety broadband spectrum, *i.e.*, where a 700 MHz public safety broadband user travels to another region and logs into another public safety network using the 700 MHz public safety broadband spectrum. We do not here address issues related to public safety roaming on commercial spectrum. These issues will be addressed separately.[98]

87. *Nomenclature*. We propose to define a 700 MHz public safety roamer in our Part 90 rules as "A mobile station receiving service from a station or system in the public safety broadband network other than one to which it is a subscriber." We seek comment on this tentative definition. In addition, as a way to develop a common nomenclature to guide this and future discussions we broadly divide intra-system public safety roamers into three categories based on the nature of their mission:

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

We seek comment on this categorization. Would such categorization facilitate technical and operational aspects of the roaming? Are there any other categorization schemes that render better results? What are these schemes and have they been used in other places?

88. In order to ensure interoperability it is critical that public safety users can gain access through roaming to other public safety networks across geographies. Accordingly, we tentatively conclude that all 700 MHz public safety broadband users should be able to roam on all other 700 MHz regional public safety broadband networks. Under this tentative conclusion, a public safety broadband provider (*i.e.*, any operator of a public safety broadband network) will have an obligation to enter into roaming arrangements with other public safety broadband providers on reasonable terms and conditions,

---

[96] *See Waiver Order.*

[97] Roaming for 700 MHz public safety users can occur in two circumstances: (1) when a public safety user travels to another region and logs into another public safety network using the same public safety band in 700 MHz spectrum, or (2) when a public safety user either travelling to another region or within his or her own region faces a situation in which either there is no coverage for public safety band or there is not sufficient capacity at the time, and hence, the user roams on to a commercial band. We adopt the nomenclature used in the NPSTC BBTF Report, which terms the first circumstance "intra-system roaming"—where public safety roams into another public safety network within the same band. The second circumstance is termed "inter-system roaming"—where public safety roams into commercial networks in another band. The scope of this *Fourth Further Notice* is limited to the issues concerning the intra-system roaming, and the issues concerning the inter-system roaming are to be addressed separately.

[98] Separately, we will also address the argument that the Commission should clarify whether E911 and the requirements of Section 255 of the Communications Act apply to public safety devices that are capable of roaming onto commercial networks. *See, e.g.*, AT&T Comments on *Technical Public Notice* at 8-9.

when requested. We tentatively conclude that the obligation to provide public safety roaming extends to all 700 MHz public safety broadband providers in order to ensure nationwide interoperability among public safety broadband networks. Additionally, we tentatively conclude that this roaming obligation should extend to all three categories of public safety roamers described above. We propose, however, that public safety broadband providers can admit different categories of public safety roamers onto the host network on different priority bases if needed. We seek comment on this tentative conclusion.

89. We believe that enabling public safety users to roam on multiple public safety broadband networks is an important step on the path to a nationwide interoperable public safety network. We believe that establishing an obligation for technologically compatible networks to allow for intra-system roaming will provide public safety with increased interoperability. We seek comment on our proposals and analysis, as well as on the issues discussed below.

1. Prioritization and Quality of Service to Support Roaming

90. We seek comment on public safety needs and standards for prioritization in the context of public safety intra-system roaming. Should there be a standard nationally-applicable prioritization scheme for all regional public safety broadband networks? Who should determine this prioritization scheme? Does this have any impact on interoperability of these networks? Alternatively, should we establish a prioritization framework within which regional networks could define and set their own priority schemes? Would such an approach still achieve our goal of nationwide interoperability? What criteria would need to be specified in the framework to ensure a baseline level of nationwide capability for interoperability purposes, while still providing flexibility for regional control? How would roamers be treated in such a framework? Is there any standardized configuration for various categories of roamers to acquire and maintain an appropriate prioritization within a visited network?

91. Similarly, we seek comment on when a prioritization scheme should be triggered. Should there be a standard nationally-applicable prioritization trigger mechanism for all regional public safety broadband networks? Who should determine the timing of this trigger mechanism? Independent of the trigger mechanism, we seek comment as to who should be able to initiate prioritization generally within networks or portions thereof. Should there be a sliding scale of authority based upon the extent of the network being put under a prioritization scheme (*e.g.*, should it require less authority to initiate prioritization on a single cell than a larger area such as an entire city)?

92. Similarly as related to QoS, we seek comment on the adoption of a standardized QoS scheme for all regional networks. Should such scheme be required for nationwide interoperability and roaming? Would a simple QoS framework be adequate for all regional networks with sufficient flexibility embedded for individual regional control over the QoS? How should various roamers acquire and maintain a minimum level of QoS capability?

2. Applications to Be Supported for Roamers

93. Broadband technologies can advance public safety and homeland security by improving the operability, interoperability, and usability of public safety communications. In particular, public safety applications could seamlessly be available to all users at home and while roaming during day to day tasks as well as in times of emergency. Recognizing these benefits of broadband technologies to public safety, we have tentatively concluded in Section A.16 above to adopt five common applications that must be fully supported by each public safety broadband network. In order to further advance interoperability across networks, we extend this tentative conclusion here by proposing that all networks support this same set of applications for the purpose of roaming. Therefore, we tentatively conclude that public safety broadband networks must support the following five applications to intra-system roamers: (1) Internet access; (2) VPN access to any authorized site and to home networks; (3) a status or information "homepage;" (4) access to responders under the Incident Command System; (5) and field-based server applications. We seek comment on this tentative conclusion. Are there additional applications that should be supported for roaming purposes?

3. Public Safety-to-Public Safety Roaming Rates

94. We recognize that providing intra-system roaming support may add some costs to the operations of any network that is subject to roaming requirements. We seek comment on the nature of these potential costs and how significant they might be. We note that public safety entities currently absorb interoperability costs for their existing systems. Thus, as a threshold issue we ask whether public safety broadband network operators anticipate absorbing intra-system roaming costs generated by other public safety users as an operational cost or whether they expect to use roaming rates or charges to recover these costs. Is there a threshold level of roaming above which costs should no longer be absorbed but need to be recovered? Should public safety intra-system roaming cost recovery functions be based on any existing commercial roaming models, or are there cost and cost recovery elements that are unique to public safety? Parties should also address how roaming costs associated with shared resources such as clearinghouses or databases should be apportioned or recovered.

95. Parties supporting the establishment of intra-system roaming charges or rates should comment on whether there are steps we should take to ensure or facilitate reasonable charges or rates for public safety intra-system roaming. In this regard, we seek to provide, within the scope of our authority, sufficient incentives for public safety to make use of negotiated roaming arrangements. Since intra-system roaming would involve reciprocity and the same set of public safety entities providing roaming to one another, we seek comment on whether adjudicating disputes on intra-system roaming charges or rates on a case-by-case basis though a complaint process is likely to be the best approach or whether some other approach would better serve the public interest in this context.[99] Are there unique factors related to facilitating public safety intra-system roaming that warrant the Commission taking steps to facilitate reasonable intra-system roaming rates for public safety? Does the goal of nationwide interoperability in the public safety context necessitate and justify significantly increased Commission oversight? We seek comment on other factors that may impact the need for Commission action to facilitate reasonable rates in this context.

96. To the extent that action is necessary, we seek comment on what steps the Commission could take to facilitate reasonable rates for intra-system roaming. If we decide not to determine rates on a case-by-case basis, but instead adopt a nationwide intra-system roaming rate, we seek comment on the appropriate methods to determine such a rate. For example, in the *Third Further Notice,* the Commission proposed a service charge of $48.50 per user per month as a benchmark rate for 700 MHz public safety broadband users.[100] The Commission based this amount on a survey of contracts presently offered to governments and public safety authorities for wireless voice and data services.[101] We seek comment as to whether using this method and this amount would be reasonable in the intra-system roaming context. What other methods are available to determine a nationwide intra-system roaming rate for public safety? We seek comment as to whether a sunset strategy would be appropriate here if we adopted an initial nationwide intra-system roaming rate.

4. Volume of Roaming Traffic

97. We make no assumptions about the amount of intra-system roaming that will occur. Rather, we seek comment on what the anticipated demand for intra-system roaming is likely to be. We also seek comment on how roaming traffic will be distributed amongst the three categories of roamers

[99] *See* Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers and Other Providers of Mobile Data Services, WT Docket 05-265, *Report and Order and Further Notice of Proposed Rulemaking*, 22 FCC Rcd 15817, 15832-33 ¶¶ 37-40. *See also* Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers and Other Providers of Mobile Data Services, WT Docket 05-265, *Order on Reconsideration and Further Notice of Proposed Rulemaking*, 25 FCC Rcd 4181, 4223-24 ¶ 91.

[100] *Third Further Notice*, 23 FCC Rcd at 14427 ¶ 392.

[101] *Id.* at 14425 ¶ 391.

described above, *i.e.*, "itinerant roamers", "interoperability roamers" and "response roamers." To this end, we seek comment on how the anticipated volume of public safety-to-public safety roaming traffic will impact interoperability and the cost and design of each public safety broadband network.

5. Proposed Model Agreement

98. In the *Waiver Order*, we provided a "Standard Lease" to govern the spectrum leasing arrangement between the PSST and waiver recipients.[102] We required use of this lease because of the nascent nature of deployment in the public safety broadband spectrum, the novel nature of the relationship between the PSST and the waiver recipients, and the unique licensing scheme adopted by the Commission in the *Second Report and Order* in which we provided for a single nationwide public safety broadband licensee.[103]

99. We seek comment on whether we should similarly provide a "Standard Roaming Agreement" for public safety intra-system roaming. Would such a standardized agreement help facilitate roaming on public safety broadband spectrum during initial and subsequent phases of deployment, help facilitate nationwide interoperability, and reduce the administrative burden on public safety network operators? We seek comment on whether such an agreement would be useful, and if so, what terms this agreement should contain. Are there minimum provisions that should be standardized on a nationwide basis? Should we allow for some local or regional variation in roaming agreements? Would such variation enhance emergency response or hinder it? Who should develop the standardized agreement? Should the PSBL or other national entity serve as a clearing house for facilitating local or regional agreements?

C. Federal Use

1. Section 2.103

100. In the *Second Report and Order*, the Commission determined that Section 337 of the Act does not bar Federal government public safety entities from using the 700 MHz band under certain conditions.[104] Specifically, the Commission determined that, while Section 337 of the Act does not expressly indicate that Federal government entities should be eligible, such "omission simply reflects the fact that the Commission does not license Federal stations."[105] In the *Waiver Order*, we determined to retain the existing rule that allows Federal use of this spectrum for the purpose of the waivers granted by the order.[106]

101. We believe it is worthwhile to re-examine this rule to ensure that it is consistent with the current approach to ensuring nationwide interoperability. We also note that the current rule could arguably be construed to allow direct leasing of spectrum for Federal use (*e.g.*, "Federal stations may be authorized..."), as opposed to merely allowing Federal users access to the network as subscribers.

102. Accordingly, we seek comment on whether the existing rule remains the appropriate vehicle for Federal access in light of the revised network-of-networks approach. If the PSBL is to retain a central role in determining access by Federal entities, should it be obligated to consult with the regional and tribal public safety network operators to ensure that capacity is not adversely impacted? Should there be other safeguards to ensure that regional and tribal networks needs are not harmed? Alternatively, should Federal access be granted at the regional or tribal level with a national clearing house to address a

[102] *See Waiver Order* at 5153-54 ¶¶ 25-27.

[103] *Id.*

[104] *See Second Report and Order*, 22 FCC Rcd at 15427 n.822; *see also* 47 C.F.R. § 2.103(b)).

[105] *Second Report and Order*, 22 FCC Rcd at 15427 n.822; *see also Waiver Order* at 5155-56 ¶ 34; 47 C.F.R. § 2.103

[106] *See Waiver Order* at 5155-56 ¶ 34; 47 C.F.R. § 2.103.

standard or common access agreement, allowing for local schedules? If so, who should fill the role as a clearing house?

103. We also seek comment on whether a capacity "leasing" option for Federal users is an appropriate approach in light of our determination to require the use of LTE for the public safety broadband network, and the bandwidth that this standard requires. Alternatively, would a subscriber access model be preferable to a leasing or capacity sharing model? In either scenario, should there be constraints on fees paid by Federal users, to whom such fees are paid, or the apportionment of such revenues? Should there be constraints on how such revenues are spent, *e.g.*, in support of the public safety broadband network? How would this be monitored or enforced? How would either model impact the costs of Federal use? If a subscribership model is more appropriate, does this impact whether a centralized or state/local access model is preferred for Federal users?

2. Roaming by Federal Users

104. In light of these concerns, we also seek comment on the appropriate regime for allowing Federal users to roam onto state or local public safety broadband systems. We tentatively conclude to extend eligibility for intra-system roaming to all Federal entities whose "sole or principal purpose" is "to protect the safety of life, health or property" and who meet the remaining requirements of Section 337(f). We anticipate that networks would enforce any eligibility requirements via network access. We seek comment as to whether Federal users should be assigned a different priority level than non-federal users.

105. In addition, if Federal government users are allowed to operate on this spectrum under the leasing option discussed above,[107] we propose that Federal agencies would also be eligible to use intra-system roaming. We seek comment on this tentative conclusion. We also seek comment from potential Federal users as to what their anticipated use of these networks would be, and on the anticipated costs (both financial and in terms of network traffic) of Federal roaming on public safety broadband networks. As above, we also seek comment on whether the use of a clearinghouse or other nationwide model roaming agreement would facilitate Federal roaming, and how such a mechanism would function, and whether any revenues generated from any roaming arrangements should be directed towards the construction and maintenance of the network.

D. Testing and Verification to Ensure Interoperability

1. Conformance Testing

106. Interoperability requires that user devices and network equipment comply with relevant standards specifications. Conformance testing, a process generally planned and developed by industry organizations and conducted by certified labs,[108] is a mechanism that could be used to ensure that devices and network equipment that are deployed in the public safety broadband spectrum are compliant with the 3GPP LTE Release 8 and higher standards. We therefore tentatively conclude that we should require that all user devices be subject to conformance testing and seek comment on this tentative conclusion.

107. While ordinarily it would be appropriate to require conformance testing in advance of network deployment, we note that a conformance testing and certification process for user devices operating in LTE Band Class 14—which includes the public safety broadband spectrum—may not be developed as of the release date of this *Fourth Further Notice*. However, the PTCRB[109] is expected soon to complete development of such a process. We propose to require that six months following the

[107] *Id.*; *see also* 47 C.F.R. § 90.175(g).

[108] 3rd Generation Partnership Project, http://www.3gpp.org/conformance-testing-ue; PTCRB, http://www.ptcrb.com/; Global Certification Forum (GCF), http://www.globalcertificationforum.org/WebSite/public/ home_public.aspx.

[109] PTCRB is a global organization created by Mobile Network Operators to provide an independent evaluation process where GSM / UMTS Type Certification can take place. *See* PTCRB, http://www.ptcrb.com/.

Commission's release of a public notice announcing the availability of the PTCRB testing process for Band 14, each public safety broadband network operator must certify to the Commission that the operating devices have gone through and completed this process.[110] We further propose that in its certification to the Commission, each network operator must also commit to any future testing called for within the certification process. We seek comment on this proposed conformance testing requirement. Do the benefits of conformance testing outweigh the costs associated with our proposal?

108. We also seek comment on conformance testing for LTE infrastructure equipment. Is there any known conformance testing with some formal certification process for LTE infrastructure equipment, namely EPC, including eNodeB, MME, SGW, PGW and PCRF? To what extent is such process used by commercial network providers? Would the benefit of such certification outweigh the possible costs associated with creating a certification requirement for public safety broadband network infrastructure equipment? Finally, we seek comment on who should represent public safety at PTRCB? Should it be the PSST, NIST or another entity? Could it be a combination of entities working in partnership? What is the cost of such a requirement?

2. Interoperability Testing (IOT)

109. In the *Waiver Order*, we required waiver recipients to self-certify their performance of IOT on specified LTE interfaces.[111] We sought comment in the *Technical Public Notice* on whether our final rules should require only self-certification, or whether we should establish a more formal mechanism for ensuring compliance with any interoperability testing requirements adopted in our final rules. Motorola recommends "self-certification relying on test suites developed specifically for public safety use of Band Class 14."[112] Meanwhile, Harris argues that "a self-certification process is adequate in the near term, particularly for systems constructed under the waiver process because final network technical specifications are still being finalized."[113] The District of Columbia, however, contends that, "[t]hough self-certification may be sufficient initially, vendors' desire to differentiate themselves in the marketplace can create incentives that run counter to the goal of interoperability" and "[i]n time, demonstrated interoperability on key interfaces will probably be necessary."[114]

110. IOT is an important mechanism for ensuring that public safety broadband networks are technically capable of supporting roaming. We therefore tentatively conclude that we should require that public safety broadband networks perform IOT for the LTE roaming interfaces identified in the *Third Report and Order* above. To this end, we tentatively conclude that we will require that network operators perform IOT, prior to deployment of any RAN equipment, on the following LTE interfaces:[115]

- Uu – LTE air interface
- S6a – Visited MME to Home HSS
- S8 – Visited SGW to Home PGW
- S9 – Visited PCRF to Home PCRF for dynamic policy arbitration

[110] Device manufacturers have their devices tested and certified through PTCRB certified labs. *See* PTCRB, http://www.ptcrb.com/.

[111] *Waiver Order* at 5161 ¶47. The specified interfaces are S1-MME (interface between eNodeB and MME); S1-u (interface between eNodeB and SGW); and U_u- LTE air interface. *Id.*

[112] Motorola Comments on *Technical Public Notice* at 18 (July 19, 2010).

[113] Harris Comments on *Technical Public Notice* at 6 (July 19, 2010).

[114] District of Columbia Comments on *Technical Public Notice* at 6 (July 19, 2010).

[115] These are the roaming interfaces that our *Third Report and Order* requires public safety broadband networks to support for the purpose of enabling roaming. *See supra* Section III.A.

111. We seek comment on this tentative conclusion. What are the costs and benefits of IOT on roaming interfaces? Have we identified an appropriate list of interfaces on which IOT is necessary to ensure roaming capability among public safety broadband networks? Are there interfaces that should be added to this list, and if so, what would be marginal costs associated with requiring IOT for such interfaces?

112. Commercial network operators rely on IOT to ensure multi-vendor interoperability for devices and equipment that operate on their networks. The LTE interfaces relevant to multi-vendor interoperability include:

- S1-u – between eNodeB and SGW
- S1-MME – between eNodeB and MME
- S5 – between SGW and PGW
- S6a – between MME and HSS
- S10 – between MMEs
- S11 – between MME and SGW
- SGi – between PGW and external PDN
- X2 – between eNodeB and eNodeB (for intra-network handover)
- 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

113. Should the commission adopt IOT rules to ensure multi-vendor interoperability on public safety broadband networks? What are the potential costs and benefits of such a requirement? Does the preceding list include all of the interfaces on which IOT should be required to support multi-vendor interoperability or are there other interfaces that should be included?

114. Although IOT is critical to ensuring that public safety broadband networks are interoperable, it is our understanding that no specific guidelines for conducting IOT between such networks have been developed. Accordingly, we tentatively conclude that, for the interim, each public safety broadband network operator will be required to submit for Bureau review, within six months of its date of service availability,[116] a plan for IOT.[117] The scope of the IOT called for in the network operator's plan would be required to be sufficiently broad to address all LTE capabilities and functions required under the *Waiver Order*, and it should examine all the interfaces needed for roaming to and from other public safety networks. After the Bureau approves its plan, each network provider will be required to certify, within three months, that IOT will be conducted on an ongoing basis with other deployed public safety broadband networks until final IOT testing rules are adopted.

115. We observe that commercial broadband service providers, who perform IOT to ensure interoperability among devices and network infrastructure, generally own or operate laboratories in which they can perform IOT. Because it is similarly important for public safety networks operators to have access to IOT for the purpose of verifying interoperability, we tentatively conclude that certain lab facilities need to be designated for the purpose of IOT. We seek comment on this tentative conclusion. Are there facilities already available for conducting IOT for public safety broadband networks? Are there

[116] *See supra* note 75.

[117] The Bureau may, at its discretion, seek public comment on any network operator's IOT plan.

third party commercial laboratories where public safety broadband network IOT could take place? How about federal lab facilities such as NIST/NTIA (PSCR) facilities, or the Idaho National Laboratory (INL)? How about an arrangement with certain commercial service providers to conduct IOT for public safety in their own lab? How should the lab facility be compensated? Who should pay for the services? Who should set and manage the set of guidelines for IOT? Who should determine the test plans? Is there a role for the PSST in this process? We note that PSCR is developing test plans for its public safety demonstration network.[118] Is it appropriate to use such test plans for IOT? If not, what is an appropriate process for developing test plans for public safety purposes? We seek comment on all of these matters.

3. Interoperability Verification

116. We seek general comment on whether there are other methods, in addition to conformance testing and IOT, of verifying that public safety broadband networks comply with the technology standards adopted for the nationwide network and are technically capable of achieving interoperability. Are any such methods more reliable than IOT and conformance testing for verifying compliance with the technical requirements adopted for the nationwide network? What are the potential costs of implementing any such methods?

E. Other Matters Relevant to Interoperability on Public Safety Broadband Networks

1. Network Operations, Administration and Maintenance

117. The operation of the broadband public safety network involves network management, administration/provisioning, and maintenance. The *Waiver Order* did not address the technological and operational features of network operations, administration and maintenance (OA&M). What operational capability, if any, should be required in order to maintain and enhance interoperability? Are there any specific operational models that would help consistency and interoperability on a local, regional or tribal and nationwide basis?[119] If yes, what are they and what are the cost benefits of the different models? Should ERIC be the entity that standardizes these operational conformance models or is another entity that is better situated to do this?

2. Reporting on Network Deployment

118. In the *Waiver Order*, we noted the importance of ensuring that waiver recipients were diligent in pursuing deployment of their networks. Accordingly, we required them to submit to the Bureau quarterly reports addressing their progress in 3 areas: (1) planning; (2) funding; and (3) deployment. To date, the Waiver Recipients have each filed two quarterly reports, which have provided the Commission with valuable information on the progress of each recipient. We anticipate that as we progress with broader deployment of the nationwide network, it will be useful for the Commission to receive periodic updates on the progress of network deployment. We thus seek comment on whether to impose on public safety network operators a periodic reporting requirement similar to that imposed on waiver recipients. Would it be appropriate to require such reporting on a quarterly basis? Should the reports address matters in addition to those required to be addressed in the quarterly reports filed pursuant to the *Waiver Order*? Should the PSST or another entity serve as the clearing house for these reports?

3. Devices

119. Devices are a critical component of system interoperability, particularly during the early phases of system deployment. In recent months, the Commission has type-approved several LTE devices

[118] The PSCR/DC Demonstration Network will provide an open platform for development and testing of public safety 700 MHz LTE broadband equipment. *See* Press Release, Nat'l Inst. of Standards and Tech., Demonstration Network Planned for Public Safety 700 MHz Broadband (Dec. 15, 2009), *available at* http://www.nist.gov/eeel/oles/network_121509.cfm (last visited Apr. 26, 2010).

[119] *See* ERIC TAC Filing at 9.

that vary in terms of channel bandwidth, frequency bands and 2G/3G technology support.[120] In order to facilitate the development of interoperable public safety LTE networks, we seek comment below on the use of LTE devices on such networks.

120. *Channel Bandwidth Requirement for the Public Safety Broadband Spectrum*: The LTE standard supports operation in 1.4/3/5/10/15/20 MHz of channel bandwidth in Frequency-Division Duplexing (FDD) mode.[121] Given that 5+5 megahertz in the 700 MHz band is presently allocated for public safety broadband communications, we tentatively conclude that we should require public safety LTE devices to support, at minimum, a five megahertz channel bandwidth. We note that certain LTE devices are type-approved for operation in 1.4/3/5 MHz channel bandwidth.[122] We seek comments whether public safety LTE devices should be required to support 1.4/3 MHz channel bandwidth in the public safety broadband spectrum. What would be the advantage/disadvantage of having multiple channel bandwidth support for public safety, such as 1.4/3/5/10 MHz Bandwidth channels? What are the costs for such an approach and do the benefits support the addition of any cost? What would be the potential impacts to device certification and national interoperability? Would there be any operational impacts to the public safety broadband network if 1.4/3 MHz channels were supported by devices but not used? What would be the impact on costs?

121. *Band Class 14 Support*: There are certain LTE devices that are FCC type-approved for 5/10 MHz operation in lower and upper 700 MHz bands.[123] Band Class 14 includes both the 5+5 megahertz D block and the 5+5 megahertz public safety broadband allocation. Should at least one or a subset of public safety LTE devices be required to support five megahertz channel operation in D block or support ten megahertz operation in Band Class 14? What are the potential benefits and costs of such requirements? What are the tradeoffs in terms of cost, complexity and performance in consideration of certification and national interoperability?

122. *Multiple Mode Support*: As LTE networks are built out for public safety and commercial usage, multiple mode devices may provide additional coverage with 2G/3G support.[124] Commercial multiple mode LTE devices are type approved to support either GPRS/EDGE/WCDMA/HSPA platform or CDMA/EVDO platform in various frequency bands. What factors should public safety entities consider when selecting LTE devices? Further, given the coverage limitations of terrestrial wireless networks, what are the possibilities of adding satellite capability to public safety LTE device? Does satellite capability favor any particular 2G/3G/4G technology platform? What, if any, action should the Commission take here?

4. In-Building Communications

123. We recognize that ideally, emergency responder communications should continue to function within a building, maintaining key services and sustaining vital communications support.[125]

---

[120] *See* FCC ID BEJAD600 (850/1900 GPRS/EDGE/WCDMA/HSPA and 700/1700 LTE USB Modem) with Test Report Serial No of Y01004190658.BEJ; FCC ID BEJVL600 (Cellular/PCS CDMA/EVDO and 700MHz LTE USB Wireless Modem) with Test Report Serial No of 0Y1004190658.BEJ; FCC ID A3LSCHR900 (Cellular/AWS/PCS CDMA/EVDO and AWS/PCS LTE Phone with Bluetooth and WLAN) with Test Report Serial No of Y01006211075.A3L.

[121] *See* 3rd Generation Partnership Project, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception (Release 8)," 3GPP TS 36.101 at Section 6.6.1 (2007).

[122] On September 21, 2010, MetroPCS announced the first LTE service in US and introduced Samsung SCHr-900 handset (FCC ID A3LSCHR900) which is FCC type-approved for operation in 1.4/3/5MHz channel bandwidth. *See* Metro PCS, http://www.metropcs.com/presscenter/articles/mpcs-news-20100921.aspx (last visited Dec. 29, 2010).

[123] *See* FCC ID BEJAD600; FCC ID BEJVL600.

[124] *See* ERIC TAC Filing at 14.

[125] *See id.* at 8.

Accordingly, we tentatively conclude that we should adopt a framework to achieve in-building coverage. Traditionally, public safety planning has accounted for this by providing extra margin in RF designs to allow for the building attenuation effects resulting from RF signals having to penetrate walls, floors and other building structures. However, even when such margins are provided, realistic circumstances make them at best, incomplete solutions. It is well known for example, that with practical attenuation margins, very tall buildings present serious challenges to sustainable communications. In addition, deep penetration into the interiors of large buildings may not be achievable. These and other conditions serve to limit the overall effectiveness of in-building penetration margins. Thus, while providing such margins is often a necessary and standard part of a public safety RF network design, such provisions in and of themselves are insufficient for the broad range of circumstances in which the emergency responder may operate.

124. We anticipate that in the future, public safety agencies will come to rely on broadband technologies for mission-critical services including voice services. Should an RF margin therefore be provided as part of a standard design to compensate for building attenuation effects as is presently done for narrowband mission critical voice services? What margin levels should be used? Will the lack of such margins lessen the effectiveness and safety of emergency responders? If building penetration margins are not provided as part of the initial design, will the lack of such margins increase the evolution expense towards mission critical services? Given the fact that even when margins are included, building attenuation effects may limit or block communications in specific circumstances, what other means should be used to support the in-building communication requirements of emergency responders? If increased margins are allowed, what does that do to the cellular architecture of the network and does that impact interference protection criteria between jurisdictions and also between other 700 MHz network operators? We seek comment on the cost of such requirements and the balance between this cost and being able to rely on this network for important in-building requirements.

125. Distributed Antenna Systems are commonly provided within buildings to support commercial wireless services and this will be extended to support the deployment of broadband commercial services. How may public safety best take advantage of Distributed Antenna System approaches? Does the expected evolution of commercial Distributed Antenna Systems represent an opportunity for public safety? Is there anything that the Commission can do to incent the deployment of such systems? What would be the cost of such an approach?

126. Finally, what other approaches may be used to further support the in-building communication needs of public safety users? If in-building requirements are adopted, what certification should the Commission impose to demonstrate that in-building requirements are met if they are required? Should a certification need to be based on a representation of the actual "as-built" network and accompanied by UL and DL data rate plots that map specific performance levels? How would this be achieved? How should new and novel approaches be evaluated? How should criteria be set to determine their overall effectiveness? Given the technical difficulty of comparative evaluations, should specific agencies or governmental organizations be assigned responsibility for testing and evaluation of promising new approaches? Lastly, what technical challenges may be involved in such evaluations? Should we require as part of any future Radio Frequency (RF) engineering assumptions and design objectives a 256 Kbps UL minimum data rate with indoor coverage to the first wall to support mission-critical communications?

5. Deployable Assets

127. The Plan recommends that public safety agencies use deployable equipment, during natural disasters and in other circumstances,[126] to supplement their existing coverage and capacity and to

[126] These deployable assets could also be used for supplementing in-building coverage.

provide a source of redundancy.[127] This equipment may include cells on wheels (COWs) and cells on light trucks (COLTS), which may be configured either as stand-alone base stations[128] or as repeater stations. COWs and COLTs may be deployed during an emergency, for example, to temporarily replace damaged sites or to support surges in traffic.[129] They can also support communications during events that occur at a cell edge, where coverage and capacity may be marginal. In addition to COWs and COLTs, signal repeaters located within public safety vehicles can be used to relay signals from portable user equipment back to a base station.[130]

128. We note that any deployable assets operating in the public safety broadband spectrum would be required to comply with the technical and operational rules established for that spectrum. We seek comment on how to ensure such compliance. Would deployable assets such as COWs and COLTs be capable of operation in conformity with the relevant technical requirements adopted in the *Third and Report Order* and proposed in this *Fourth Further Notice*? Should the Commission require that COWs and COLTs deployed for Public Safety use the 4.9 GHz or Satellite bands for backhaul? Are there additional steps we should take to promote this capability?

6. Operation of Fixed Stations and Complimentary Use of Fixed Broadband Spectrum

129. The 700 MHz public safety broadband spectrum is allocated to mobile use. This allocation was made because of the recognition of the need for discrete spectrum for mobile uses. This band has unique technical characteristics, such as its propagation characteristics that makes it especially well suited for mobile broadband use. In this respect, the Bureau previously determined that, for the Waiver Recipients, achieving operability and interoperability required allowing fixed use on an ancillary basis only.[131] The record indicates requirements for fixed, mobile and nomadic subscriber use cases. However, we tentatively conclude that we should allow public safety to operate fixed services in this band on an ancillary basis. We seek comment on this tentative conclusion. By enabling such ancillary fixed use, we will ensure that the spectrum remains available for its primary purpose, while allowing users appropriate flexibility as long as it does not compromise the primary use of the spectrum for mobile purposes. We note however that mixed use could introduce unacceptable interference, especially at the cell edge, that will impact the network performance. In the event it does, how can a network operator mitigate such interference and is there any specific E-UTRA (LTE) standards that need to be mandated by the Commission?

130. Of course having broadband spectrum available for fixed uses is critical. The Commission recognized this need when it allocated 50 megahertz of spectrum at the 4.9 GHz band to public safety for broadband fixed uses.[132] This spectrum is currently being used by many jurisdictions for many important public safety uses including surveillance and back-haul capacity.

---

[127] *See* National Broadband Plan at 318, Exhibit 16-B: National Safety Network and Solutions; *see also* Cost Model Paper at 3.

[128] Under the 3GPP LTE standard, base stations are referred to as "Enhanced NodeBs", or "eNodeBs".

[129] In mobile data networks higher signal levels above noise and interference level are proportional to available data rates. In addition, introducing bandwidth in a given area allows the introduction of the corresponding capacity to users in that area.

[130] *See* Cost Model Paper at app. A.

[131] *Waiver Order* at ¶ 21. The Bureau received two Petitions for Reconsideration of this provision. *See* Petition for Reconsideration filed by City of Charlotte, NC, District of Columbia, Iowa Statewide Interoperability Communications System Board, State of New Jersey, City of Mesa, AZ, State of New Mexico, State of Oregon, and City of Seattle, WA, , PS Docket No. 06-229 (filed Jan. 10, 2011); Petition for Reconsideration filed by Utilities Telecom Council, PS Docket No. 06-229 (filed Jan. 11, 2011).

[132] *See* The 4.9 GHz Band Transferred From Federal Government Use, WT Docket 00-32, *Second Report and Order and Further Notice of Proposed Rulemaking*, 17 FCC Rcd 3955 (2002).

131. We believe that it is critical that public safety community has the broadband tools it requires to keep America safe. Accordingly, we seek comment on what can be done to ensure that the 4.9 GHz band networks can complement the 700 MHz broadband networks. What can be done to increase this compliment? Can channel plans and power limits current employed for the 4.9 GHz band be adjusted or improved? We also seek comment on the use of different directional antennas with different antenna gains as a means of increasing use of the 4.9 GHz band spectrum. Are there other ways to increase throughput in this band? Should licensees in this band be provided more certainty? How should licensing for the 4.9 GHz band and the 700 MHz band match? Should licensing rules be structured for the two bands to encourage use of the 4.9 GHz band? If so, how?

7. Compliance With the Commission's Environmental Regulations

132. All towers constructed by or for FCC licensees must comply with the Commission's environmental regulations, 47 C.F.R. §§ 1.1301-1.1319. These rules implement federal environmental statutes, including the National Environmental Policy Act of 1969 (42 U.S.C. § 4321 *et seq.*), the Endangered Species Act of 1973 (16 U.S.C. § 1531 *et seq.*), and Section 106 of the National Historic Preservation Act (16 U.S.C. § 470f). The Commission's rules require an Environmental Assessment (EA) prior to construction when a facility may have a significant impact on the environment. In order to determine whether an EA is necessary, applicants are required to ascertain whether their facilities may have nine types of effects specified in Section 1.1307(a) and (b) of the rules.

8. Public Safety Broadband and Next-Generation 911 Networks

133. As the broadband public safety network is developed, it expands the potential means for first responders not only to communicate with one another, but also to communicate with and receive data from 911 centers that will assist them in responding to emergencies. This potential will increase even further to the extent that jurisdictions develop Next Generation 911 (NG911) networks that enable the public to transmit broadband data, such as text, photos, and video, to 911 centers.[133] By linking the public safety broadband network with NG911 networks, text and images sent by the public can be processed by 911 centers and retransmitted to first responders in the field, vastly improving their situational awareness and enabling a faster, more focused response. We seek comment on the how best to ensure that the public safety broadband network can interconnect with NG911 networks to support such communication. Are there technical issues that need to be addressed? Are the technical standards that are being developed for NG911 networks compatible with the technical architecture we propose here for the public safety broadband network? How do we ensure continued compatibility as both the public safety network and NG911 networks evolve and acquire new technical capabilities over time?

F. Section 337 Eligible Users

134. Use of the 700 MHz public safety broadband spectrum is governed by Section 337 of the Communications Act. Section (f) defines public safety services.[134] These services are services "the sole or principal purpose of which is to protect the safety of life, health or property."[135] Such services also must be provided by a governmental entity or a non-governmental entity that is authorized by a governmental entity "whose primary mission is the provision of such services," and must not be made commercially available to the public.[136] In the *Second Further Notice* and in the *Third Further Notice*, the Commission sought comment on permissible users of the public safety broadband spectrum.[137] As a

[133] *See* Framework for Next Generation 911 Deployment, PS Docket 10-255, *Notice of Inquiry*, FCC 10-200 (rel. Dec. 21, 2010).

[134] 47 U.S.C. § 337(f).

[135] § 337(f)(1)(A).

[136] § 337(f)(1)(B), (C).

[137] *Second Further Notice* at 8061-63 ¶¶ 30-35; *Third Further Notice* at 14401-07 ¶¶ 312-327.

general matter, the Commission tentatively concluded that utility and critical infrastructure (CI) entities are not eligible for use of the public safety spectrum, in that they fail to meet the "sole or primary use" requirement of 337(f)(1)(A).[138]

135. In further reviewing the statute, we have concerns about the Commission's authority to allow secondary use of the public safety broadband spectrum. However, we recognize the strong desire of many in the public safety community to include secondary users such as utilities, public works and others on their network as a mechanism to coordinate common activities and respond jointly to emergencies, as well as a method to spread costs and capitalize on infrastructure sharing opportunities. This policy goal is worth of pursuit in light of the otherwise uncertain nature of the funding need to ensure nationwide build out of the public safety broadband network.[139]

136. In this respect, we re-examine each of Section 337(f)'s requirements in turn and seek comment. First, we focus on the Section 337(f)(1)(A)'s requirement that public safety services, for which the 700 MHz public safety allocation is designated, must be services "the sole or principal purpose of which is to protect the safety of life, health, or property."[140] Would this requirement be met if the Commission were to adopt a limit on the amount of secondary usage permitted, such that the principal purpose of the network or networks remains for public safety purposes? We previously noted that such an interpretation appears inconsistent with the spirit of the statute.[141] However, in light of the strong interest in permitting such use, we again seek comment on any limits we could place on usage that could satisfy this portion of the statute. If we limit secondary use, how would we measure such usage? Should we address this usage on a nationwide basis, or on some smaller subdivision? Should the secondary usage be required to have some quasi-public safety focus, or some other public safety nexus to qualify? How would this be determined? If secondary users are allowed, should their traffic be afforded a lower priority? Should there be an exception for those communications that qualify for public safety services treatment? Should require such prioritization, or should we limit communications by secondary users to those that protect the safety of life, health or property? How could this be enforced? Are there other methods that could be employed to ensure "principal" use remains for public safety services?

137. With respect to Section 337(f)(1)(B), we recognize that such use would likely be undertaken pursuant to subsection 337(f)(1)(B)(ii) which allow such services to be provided by "nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services."[142] In the *Second Report and Order*, we addressed this element of the statute with respect to the PSBL by requiring that applicants for the license submit evidence of such authorization in the form of letters from qualifying public safety agencies.[143] How should we ensure that such consent is obtained? Should we require new authority to be obtained by the PSBL? Should we adopt mechanisms for a state or local network or prospective secondary user to obtain evidence of such consent? Should a single agency in a particular geography be responsible for managing such authorization? Are there other means to satisfy this statutory element?

138. Next, we consider Section 337(f)(1)(C), which requires that public safety services "are

[138] *Third Further Notice* at 14405-06 ¶¶ 323-326; *see also* State of Illinois, *Order*, 23 FCC Rcd 437 (PSHSB 2008) (rejecting argument that provider of electric and gas utility service was eligible to hold license for or use 700 MHz public safety spectrum)

[139] *See also* New Mexico Comments on *Second Round Waiver Public Notice* at 7 (citing changed circumstances following the failed D Block auction in calling for a re-examination of the Commission's previous tentative conclusions regarding Section 337 eligibility).

[140] 47 U.S.C. § 337(f)(1)(a).

[141] *Third Further Notice* at 14403 ¶¶ 317-18.

[142] 47 U.S.C. § 337(f)(1)(B)(ii).

[143] *Second Report and Order* at 15421-22 ¶ 373.

not made commercially available to the public."[144] If such secondary users are charged a fee for access to the network, is this provision violated? If such a fee is made through in-kind contributions, such as access to infrastructure, does that make a difference? If any revenue generated by such access is limited in terms of how it can be spent, such that it must be put back into the public safety broadband network, can we find this provision satisfied? Is such a requirement a good idea in any event? How would such restrictions be structured and enforced?

139. We also consider Section 337(a), which sets forth the division of the 700 MHz spectrum between commercial uses and public safety services.[145] If some amount of spectrum in the public safety broadband allocation is employed for non-public safety purposes, even if the "principal use" of the network remains for public safety services, is Section 337 violated? If not, why? If all secondary users are required to accept secondary, preemptible status, is this sufficient? What if some communications are afforded primary status?

140. Finally, we seek comment on any other conditions that should be imposed on secondary users in the event such use is found permissible under Section 337, or other policy considerations that the Commission should address. Are usage limits necessary to preserve capacity for traditional public safety use? Should secondary users be permitted only on a secondary, preemptible basis? Who should facilitate access by such secondary users – the PSBL or the regional or tribal network operator? Should a clearing house model be used, or should a model Memorandum of Understanding (MOU) or user agreement be developed? By whom? How should such use be monitored and enforced? Should there be limits on fees for such usage, or constraints on how revenues generated by such secondary use could be employed? Should there be a requirement that such fees be used for construction and operation of the network? How should such fees be allocated, or to whom would these fees be paid? How would this be monitored or enforced?

V. PROCEDURAL MATTERS

A. Regulatory Flexibility Act

141. As required by the Regulatory Flexibility Act,[146] the Commission has prepared a Final Regulatory Flexibility Certification (Certification) relating to the *Third Report and Order* and an Initial Regulatory Flexibility Analysis (IRFA) relating to the *Fourth Further Notice of Proposed Rulemaking*. The Certification is set forth in Appendix C, and the IRFA is set forth Appendix D.

B. Paperwork Reduction Act of 1995

142. *Paperwork Reduction Act of 1995.* This document contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies are invited to comment on the new or modified information collection requirements contained in this proceeding.

C. Other Procedural Matters

1. Ex Parte Presentations

143. The rulemaking shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[147] Persons making oral *ex parte* presentations are reminded that

[144] 47 U.S.C. § 337(f)(1)(C).

[145] 47 U.S.C. § 337(a).

[146] *See* 5 U.S.C. § 604.

[147] 47 C.F.R. §§ 1.200 *et. seq.*

memoranda summarizing the presentations must contain summaries of the substance of the presentations and not merely a listing of the subjects discussed. More than a one or two sentence description of the views and arguments presented generally is required.[148] Other requirements pertaining to oral and written presentations are set forth in Section 1.1206(b) of the Commission's rules.[149]

2. Comment Filing Procedures

144. Pursuant to Sections 1.415 and 1.419 of the Commission's rules,[150] interested parties may file comments on or before the dates indicated on the first page of this document. All filings related to this *Fourth Further Notice* should refer to PS Docket No. 06-229. Comments may be filed using: (1) the Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies.[151]

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://www.fcc.gov/cgb/ecfs/ or the Federal eRulemaking Portal: http://www.regulations.gov. Filers should follow the instructions provided on the website for submitting comments.

    - ECFS filers must transmit one electronic copy of the comments PS Docket No. 06-229. In completing the transmittal screen, filers should include their full name, U.S. Postal Service mailing address, and PS Docket No. 06-229. Parties may also submit an electronic comment by Internet e-mail. To get filing instructions, filers should send an e-mail to ecfs@fcc.gov and include the following words in the body of the message, "get form." A sample form and directions will be sent in response.

- Paper Filers: Parties who choose to file by paper must file an original and four copies of each filing. Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail (although we continue to experience delays in receiving U.S. Postal Service mail). All filings must be addressed to the Commission's Secretary, Marlene H. Dortch, Office of the Secretary, Federal Communications Commission, 445 12th Street, S.W., Washington, DC, 20554.

    1. Effective December 28, 2009, all hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes must be disposed of before entering the building. **Please Note**: The Commission's former filing location at 236 Massachusetts Avenue, NE, Suite 110, Washington, DC 20002 permanently closed on December 24, 2009.

    2. Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

    3. U.S. Postal Service first-class, Express, and Priority mail should be addressed to 445 12th Street, S.W., Washington DC 20554.

[148] *See* 47 C.F.R. § 1.1206(b)(2).

[149] 47 C.F.R. § 1.1206(b).

[150] 47 C.F.R. §§ 1.415, 1.419.

[151] *See* Electronic Filing of Documents in Rulemaking Proceedings, 63 Fed. Reg. 24121 (1998).

145. Parties should send a copy of their filings to: Jennifer Manner, Public Safety and Homeland Security Bureau, 445 12th Street, S.W., Washington, D.C. 20554, or by e-mail to jennifer.manner@fcc.gov. Parties shall also serve one copy with the Commission's copy contractor, Best Copy and Printing, Inc. (BCPI), Portals II, Room CY-B402, 445 12th Street, S.W., Washington, D.C. 20554, (202) 488-5300, or via e-mail to fcc@bcpiweb.com.

146. Documents in PS Docket No. 06-229 will be available for public inspection and copying during business hours at the FCC Reference Information Center, Portals II, Room CY-A257, 445 12th Street, S.W., Washington, D.C. 20554. The documents may also be purchased from BCPI, telephone (202) 488-5300, facsimile (202) 488-5563, TTY (202) 488-5562, e-mail fcc@bcpiweb.com.

3. Accessible Formats

147. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to FCC504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY). Contact the FCC to request reasonable accommodations for filing comments (accessible format documents, sign language interpreters, CARTS, *etc.*) by e-mail: FCC504@fcc.gov; phone: 202-418-0530 (voice), 202-418-0432 (TTY).

VI. ORDERING CLAUSES

148. Accordingly, IT IS ORDERED pursuant to sections 1, 2, 4(i), 5(c), 7, 10, 201, 202, 208, 214, 301, 302, 303, 307, 308, 309, 310, 311, 314, 316, 319, 324, 332, 333, 336, 337, 614, 615, and 710 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 155(c), 157, 160, 201, 202, 208, 214, 301, 302, 303, 307, 308, 309, 310, 311, 314, 316, 319, 324, 332, 333, 336, and 337, that this *Third Report and Order and Fourth Further Notice of Proposed Rulemaking* in PS Docket No. 06-229 IS ADOPTED. The *Third Report and Order* shall become effective upon publication in the Federal Register.[152]

149. IT IS FURTHER ORDERED that the Commission SHALL SEND a copy of the *Third Report and Order* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

150. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of the *Third Report and Order*, including the Final Regulatory Flexibility Certification, to the Chief Counsel for Advocacy of the Small Business Administration.

151. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of the *Fourth Further Notice of Proposed Rulemaking*, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch

Marlene H. Dortch
Secretary

[152] Because the *Third Report and Order* imposes no immediate obligations on any party, we find that good cause exists for making the *Third Report and Order* effective upon publication in the Federal Register. The information collection contained in the *Third Report and Order* will become effective upon approval of the Office of Management and Budget.

APPENDIX A

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 27 and 90 as follows:

PART 27 – MISCELLANEOUS WIRELESS COMMUNICATIONS SERVICES

1. The authority citation for part 27 continues to read as follows:
   Authority: 47 U.S.C. 154, 301, 302, 303, 307, 309, 332, 336, and 337 unless otherwise noted.

PART 90 – PRIVATE LAND MOBILE RADIO SERVICES

2. The authority citation for part 90 continues to read as follows:

   Authority: Sections 4(i), 11, 303(g), 303(r), and 332(c)(7) of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 161, 303(g), 303(r), and 332(c)(7) unless otherwise noted.

3. Section 90.7 is amended by adding the following definitions in alphabetical order to read as follows:

   §90.7 Definitions.

* * * * *

Public Safety Broadband Network Operator. A Public Safety Network Operator is a public safety entity that is authorized by lease or other permitted mechanism under the Public Safety Broadband License to operate a public safety broadband network in the 763-768 MHz and 793-798 MHz bands.

Service Availability. The use of a public safety broadband network on a day-to-day basis for operational purposes by at least fifty users.

Upper 700 MHz D Block license. The Upper 700 MHz D Block license authorizes services in the 758-763 MHz and 788-793 MHz bands.

* * * * *

4. Section 90.203 is amended by adding paragraph (p) to read as follows:

   §90.203 Certification Required

* * * * *

(p) *Equipment certification for transmitters in the 763-769 and 793-799 MHz Bands.* Applications for all transmitters must show support for at least 3GPP Standard E-UTRA Release 8 and associated Evolved Packet Core, which is incorporated by reference. The Director of the Federal Register approves this incorporation by reference in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. Copies may be inspected at the Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554 or National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202–741– 6030, or go to: http://www.archives.gov/ federal_register/code_of_federal_regulations/ibr_locations.html. Copies of the 3GPP Standard E-UTRA

Release 8 can be obtained from 3GPP, http://www.3gpp.org.

* * * * *

5. Section 90.1407 is amended by adding paragraphs (d)-(f) to read as follows:

§90.1407 Spectrum Use in the Network

* * * * *

(d) Public Safety Broadband Network Operators must use at least 3GPP Standard E-UTRA Release 8 and associated EPC Evolved Packet Core (incorporated by reference). The Director of the Federal Register approves this incorporation by reference in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. Copies may be inspected at the Federal Communications Commission, 445 12th Street, SW., Washington, DC 20554 or National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202–741– 6030, or go to: http://www.archives.gov/ federal_register/code_of_federal_regulations/ibr_locations.html. Copies of the 3GPP Standard E-UTRA Release 8 can be obtained from 3GPP, http://www.3gpp.org. Later versions of this standard may be employed by Public Safety Broadband Network Operators provided they are backwards-compatible with this version.

(e) Systems in the network must support the following interfaces: Uu- LTE air interface; 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 – between 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.

(f) A Public Safety Broadband Network Operators must submit to the Chief of the Public Safety and Homeland Security Bureau prior to deployment of any Radio Access Network equipment a certification that it will be in compliance with paragraph (e) of this Section prior to the date its network achieves service availability.

* * * * *

APPENDIX B

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 47 CFR part 90 as follows:

PART 90 – PRIVATE LAND MOBILE RADIO SERVICES

1. The authority citation for part 90 continues to read as follows:

   Authority: Sections 4(i), 11, 303(g), 303(r), and 332(c)(7) of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 161, 303(g), 303(r), and 332(c)(7) unless otherwise noted.

2. Section 90.7 is amended by amending the following definitions in alphabetical order to read as follows:

   §90.7 Definitions.

* * * * *

Field-based Server Applications. Applications that require client devices to consistently and continuously reach server-based systems from any other location (*i.e.*, field locations) on the Internet.

Incident Command System. A standardized, on-scene, all-hazards incident management approach that allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure; enables a coordinated response among various jurisdictions and functional agencies, both public and private; and establishes common processes for planning and managing resources.

Internet Access. Access to the global internet.

Interoperability. The ability of public safety agencies to communicate with one another via radio communications systems – to exchange voice and/or data with one another on demand, in real time, when needed and when authorized.

Interoperability Testing. Testing to ensure interoperability between or among public safety broadband networks.

Public Safety Narrowband Operator. A Public Safety Narrowband Operator is a public safety entity that is authorized to operate and has deployed narrowband operations within the 763-769 MHz and 793-799 MHz bands.

Roamer. A mobile station receiving service from a station or system in the public safety broadband network other than one to which it is a subscriber.

Status or Information Homepage. A method by which the operator of a host network provides roamers access to and distribution of available applications, alerts, incident-specific information, system status information, and information that the operator deems important to share with roamers on its system.

Virtual Private Network Access. Access to a network, such as a roamer's home network, through use of a

Virtual Private Network connection.

* * * * *

* * * * *

3. Section 90.1407 is amended by revising paragraph (f) and adding paragraphs (g)-(j) to read as follows:

§90.1407 Spectrum Use in the Network

* * * * *

(f) Public Safety Broadband Network Operators must submit to the Chief of the Public Safety and Homeland Security Bureau the following certifications

(1) Prior to deployment of any Radio Access Network equipment, a certification that it will be in compliance with paragraph (e) of this Section as of the date its network achieves service availability.

(2) Prior to deployment of any Radio Access Network equipment, a certification that his has performed interoperability testing on the following 3GPP LTE interfaces: Uu – LTE air interface, S6a – Visited MME to Home HSS, S8 – Visited SGW to Home PGW and S9 – Visited PCRF to Home PCRF for dynamic policy arbitration

(3) Within thirty days of the date its network achieves service availability, a certification that its network can provide a minimum outdoor data rate of 256 Kbps uplink and 768 Kbps downlink for all types of devices, per single user at the cell edge.

(4) Six months following the release of a Public Notice announcing the availability of the PTCRB testing process for 3GPP LTE Band Class 14, a certification that the devices in use on its network have gone through and completed this process.

(g) *Out of Band Emissions:* Public Safety Broadband Network Operators must adhere to the following limitations on out of band emissions.

(1) On any frequency outside the 763-768 MHz band, the power of any emission shall be attenuated outside the band below the transmitter power (P) by at least 43 + 10 log (P) dB.

(2) On any frequency outside the 793-798 MHz band, the power of any emission shall be attenuated outside the band below the transmitter power (P) by at least 43 + 10 log (P) dB.

(h) Public Safety Broadband Network Operators must support the following applications: Internet access; Virtual Private Network access; a status or information "homepage;" access for users to the Incident Command System; and field-based server applications.

(i) Public Safety Broadband Network Operators must support LTE signaling layer security features over the Radio Resource Control (RRC) protocol layer (UE and eNodeB); EPC signaling layer security features over the Non Access Stratum (NAS) protocol layer (UE and MME); and user data/control layer security features over the Packet Data Convergence Sublayer (PDCP) protocol layer (UE and eNodeB).

(j) *Interference Mitigation.* Ninety days prior to the deployment of any Radio Access Network equipment, a Public Safety Broadband Network Operator must provide notice to all adjacent or bordering jurisdictions of its plans for deployment. Any notified jurisdiction may then request, in writing, the

opportunity to enter a written frequency coordination agreement with the operator.

(1) Any such agreement, or modification to such agreement, must be submitted to the Public Safety and Homeland Security Bureau within 30 days of its execution.

(2) If parties are unable to execute an agreement within ninety days of the date a request is made, the parties may submit the dispute to the Bureau for resolution.

* * * * *

4. New Section 90.1409 is added to read as follows:

§90.1409 Protection of Incumbent Narrowband Operations

(a) Ninety days prior to the deployment of any Radio Access Network equipment, a Public Safety Broadband Network Operator must provide notice to any incumbent Public Safety Narrowband Operator in within its proposed area of operation or in any adjacent or bordering jurisdictions of its plans for deployment. Such notice shall identify:

(1) the geographic borders within which the Public Safety Broadband Network Operator intends to operate;

(2) any geographic overlap; and

(3) the proposed method of interference mitigation or notice of their intent to relocate the incumbent Public Safety Narrowband Operator.

(b) Any notified jurisdiction shall respond to a notification under subsection (a) within 60 days. Such response shall identify:

(1) the jurisdictions consent to any proposed interference mitigation or relocation proposal, and any counterproposals; and/or

(2) specific objections to any element of the notification.

(c) The Public Safety Broadband Network Operator and Public Safety Narrowband Operator shall memorialize such agreements in writing. These agreements, or modification to such agreement, must be submitted to the Public Safety and Homeland Security Bureau within 30 days of its execution.

(d) Any jurisdictions failing to resolve any disputes within 90 days following a response under subsection (b) may submit the dispute to the Bureau for resolution

APPENDIX C

Final Regulatory Flexibility Certification

Final Regulatory Flexibility Certification. The Regulatory Flexibility Act of 1980, as amended (RFA)[152] requires that a regulatory flexibility analysis be prepared for rulemaking proceedings, unless the agency certifies that "the rule will not have a significant economic impact on a substantial number of small entities."[153] The RFA generally defines "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[154] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[155] A small business concern is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[156]

In the *Third Further Notice* the Commission concluded that no Initial Regulatory Flexibility Analysis was required in light of the statutory exemption provided in Section 213 of the Consolidated Appropriations Act of 2000, which provides that the Regulatory Flexibility Act shall not apply to the rules and competitive bidding procedures governing certain frequencies in the 700 MHz band.[157] However, in this *Third Report and Order*, we proceed with rules for the public safety broadband spectrum, but not for those frequencies covered by Section 213. Accordingly, and as described below, we provide this certification.

In this *Third Report and Order*, the Commission requires that all public safety broadband networks that will be deployed in the 700 MHz spectrum allocated for public safety broadband services will deploy the LTE broadband standard, specifically at least 3GPP Standard E-UTRA Release 8 and associated EPC. This requirement reflects a strong consensus, both within the public safety community and within the commercial wireless sector, that LTE is the most suitable technology platform for 700 MHz public safety broadband deployments. The adoption of a requirement that public safety broadband networks deploy this particular broadband standard is necessary to provide a clear path for the deployment and evolution of public safety broadband networks and to ensure that these networks are interoperable and can support public safety roaming on a nationwide basis.

We do not anticipate that a "substantial number" of small entities will become operators of public safety broadband networks.[158] We note further that the requirement that public safety networks adopt the

---

[152] The RFA, *see* § 5 U.S.C. S 601 *et. seq.*, has been amended by the Contract With America Advancement Act of 1996, Pub. L. No. 104-121, 110 Stat. 847 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA).

[153] 5 U.S.C. § 605(b).

[154] 5 U.S.C. § 601(6).

[155] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in Small Business Act, 15 U.S.C. S § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[156] Small Business Act, § 15 U.S.C. S 632.

[157] *Third Further Notice* at 14450 ¶ 461.

[158] In this regard, we note that currently only a single entity holds the license for this spectrum on a nationwide basis. Moreover, we note that none of the jurisdictions granted conditional waivers for early public safety broadband network deployment, except one, would appear to qualify as "small governmental jurisdictions" for purposes of the RFA. *See* 5 U.S.C. § 601(5); *see also* (continued....)

LTE standard, as opposed to an alternative broadband standard, will not significantly increase the costs of network deployment. There is no reason to suppose that deployment of an LTE network would be significantly more expensive than deployment of a network using an alternative technology platform that also satisfies the minimum requirements of the *Second Report and Order*, namely that the chosen broadband platform "include current and evolving state-of-the-art technologies reasonably made available in the commercial marketplace with features beneficial to the public safety community."[159] In fact, we observe that major commercial wireless carriers have begun deploying commercial 700 MHz networks that use LTE technology; the adoption of LTE for public safety broadband networks will create opportunities to leverage these commercial deployments and achieve cost savings that would not be possible with any alternative technology. Therefore, we certify that the requirements of this *Third Report and Order* will not have a significant economic impact on a substantial number of small entities. The Commission will send a copy of the *Third Report and Order*, including a copy of this final certification, in a report to Congress and the Government Accountability Office pursuant to the Small Business Regulatory Enforcement Fairness Act of 1996.[160] In addition, the *Third Report and Order* and this certification will be sent to the Chief Counsel for Advocacy of the Small Business Administration, and will be published in the Federal Register.[161]

(Continued from previous page)

Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks, PS Docket 06-229, *Order*, 25 FCC Rcd 5145, 5147 (2010) (*Waiver Order*).

[159] *See Second Report and Order*, 22 FCC Rcd at 15434 ¶ 405.

[160] *See* 5 U.S.C. § 801(a)(1)(A)

[161] *See* 5 U.S.C. § 605(b).

APPENDIX D

Initial Regulatory Flexibility Analysis

As required by the Regulatory Flexibility Act (RFA),[162] the Commission has prepared this present Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities by the policies and rules proposed in this *Fourth Further Notice of Proposed Rule Making* (*Fourth Further Notice*). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments provided in paragraph [xx] of this *Fourth Further Notice*. The Commission will send a copy of this *Fourth Further Notice*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[163] In addition, the *Fourth Further Notice* and IRFA (or summaries thereof) will be published in the Federal Register.[164]

A. Need for, and Objectives of, the Proposed Rules

The rules proposed in the *Fourth Further Notice* are necessary to ensure the interoperability of 700 MHz public safety broadband networks that are expected to be deployed in the near term. The proposed rules create technical requirements designed to ensure that public safety broadband networks are technically and operationally compatible, so that public safety personnel from various jurisdictions and departments are able to communicate effectively over these networks.

The *Fourth Further Notice* proposes changes to Part 90 of the rules. Specifically, it proposes to:

1) Develop a regulatory and operational framework for roaming from one public safety broadband network to another.

2) Require that public safety broadband networks meet certain technical requirements designed to ensure that networks are technically interoperable or compatible.

3) Require that public safety broadband networks meet additional requirements designed to ensure that networks achieve a baseline of operability necessary to support interoperable communications.

4) Require public safety broadband network operators to complete testing for equipment and user devices operated on their networks to ensure conformance with relevant technical standards and ensure interoperability between networks.

5) Make additional minor edits to Part 90.

B. Legal Basis

The proposed action is authorized under sections 1, 2, 4(i), 5(c), 7, 10, 201, 202, 208, 214, 301, 302, 303, 307, 308, 309, 310, 311, 314, 316, 319, 324, 332, 333, 336, 337, 614, 615, and 710 of the

[162] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. § 601 *et. seq.*, has been amended by the Contract With America Advancement Act of 1996, Pub. L. No. 104-121, 110 Stat. 847 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA).

[163] *See* 5 U.S.C. § 603(a).

[164] *See id.*

Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 155(c), 157, 160, 201, 202, 208, 214, 301, 302, 303, 307, 308, 309, 310, 311, 314, 316, 319, 324, 332, 333, 336, 337, 614, 615 and 710.

C. Description and Estimate of the Number of Small Entities To Which the Proposed Rules Will Apply

The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.[165] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[166] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[167] A small business concern is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[168]

The proposed requirements of the *Fourth Further Notice* would apply to public safety entities granted authority from the Commission to pursue deployment of public safety broadband networks within their jurisdictions.

The term "small governmental jurisdiction" is defined generally as "governments of cities, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[169] Census Bureau data for 2002 indicate that there were 87,525 local governmental jurisdictions in the United States.[170] We estimate that, of this total, 84,377 entities were "small governmental jurisdictions."[171] Thus, we estimate that most governmental jurisdictions are small.

We anticipate, however, that the vast majority of small governmental jurisdictions will not be directly authorized to serve as operators of their own 700 MHz public safety broadband networks. Rather, we anticipate that such entities will operate primarily under authority granted to larger regional, tribal or national entities to serve as public safety broadband network operators.[172] Accordingly, we anticipate that the proposed requirements that apply directly to public safety network operators are unlikely to directly affect a substantial number of small entities.

---

[165] 5 U.S.C. § 603(b)(3).

[166] 5 U.S.C. § 601(6).

[167] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in 15 U.S.C. § 632). Pursuant to the RFA, the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register." 5 U.S.C. § 601(3).

[168] Small Business Act, 15 U.S.C. § 632 (1996).

[169] 5 U.S.C. § 601(5).

[170] U.S. Census Bureau, Statistical Abstract of the United States: 2006, Section 8, p. 272, Table 415.

[171] We assume that the villages, school districts, and special districts are small, and total 48,558. *See* U.S. Census Bureau, Statistical Abstract of the United States: 2006, section 8, p. 273, Table 417. For 2002, Census Bureau data indicate that the total number of county, municipal, and township governments nationwide was 38,967, of which 35,819 were small. *Id.*

[172] We note that none of the twenty-one jurisdictions that applied for and were granted conditional waivers for early public safety broadband network deployment, except one, would qualify as "small governmental jurisdictions." *See* 5 U.S.C. § 601(5); *see also* Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks, PS Docket 06-229, *Order*, 25 FCC Rcd 5145, 5147 (2010) (*Waiver Order*).

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements

The *Fourth Further Notice* proposes rule changes that will affect reporting, recordkeeping and other compliance requirements. Each of these changes is described below.

The *Fourth Further Notice* proposes to require public safety broadband networks to support roaming from users of other public safety broadband networks. This would require network operators to provide technical roaming capability within their networks and to support of minimum set of user applications.

The *Fourth Further Notice* proposes to require public safety broadband networks to support seamless handover within the network's coverage region. This would require network operators to implement the technical capability to support this feature within their networks.

The *Fourth Further Notice* proposes to require public safety broadband networks to adhere to a specified out-of-band-emissions requirement. This would require to public safety network operators to incorporate the proposed out-of-band-emissions requirement into the planning and design of their networks.

The *Fourth Further Notice* proposes to require public safety broadband networks to support a minimum set of applications, namely (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; and (5) field-based server applications. This would require public safety network operators to implement the technical capability to support these applications on their networks.

The *Fourth Further Notice* proposes to require public safety broadband network to meet performance requirements, namely that they provide outdoor coverage at minimum data rates 768 kbps downlink and 256 kbps uplink, for all types of devices, for a single user at the cell edge. Public safety network operators would need to incorporate these requirements into the planning and design of their networks. Public safety network operators would also be required to certify to the Public Safety and Homeland Security Bureau their compliance with these performance requirements. These certifications would need to be based on a representation of the actual "as-built" network and be accompanied by uplink and downlink data rate plots that map specific performance levels.

The *Fourth Further Notice* proposes to require public safety broadband networks to support specified security features, namely (1) the LTE signaling layer security features over the Radio Resource Control (RRC) protocol layer (UE and eNodeB); (2) EPC signaling layer security features over the Non Access Stratum (NAS) protocol layer (UE and MME); (3) and user data/control layer security features over the Packet Data Convergence Sublayer (PDCP) protocol layer (UE and eNodeB).

The *Fourth Further Notice* proposes to require public safety broadband networks to meet coverage and coverage reliability requirements. Specifically, it proposes to require public safety broadband networks to provide outdoor coverage reliability at a probability of coverage of 95 percent for all services and applications throughout the network. Public safety network operators would need to incorporate this requirement into the planning and design of their networks.

The *Fourth Further Notice* proposes to require each public safety broadband network operator to notify adjacent or bordering jurisdictions prior to deployment, and to allow adjacent or bordering jurisdictions the opportunity to negotiate a formal coordination agreement with the deploying jurisdiction. Any formal written agreements would be required to be submitted to the Bureau.

The *Fourth Further Notice* proposes to require public safety broadband network operators to

complete conformance testing for the devices used on their network after a testing process for LTE devices operating in the public safety broadband spectrum becomes available. Public safety network operators would also be required to certify to the Commission their completion of conformance testing.

The *Fourth Further Notice* proposes to require public safety broadband network operators to submit plans for completing interoperability testing with other public safety broadband networks. The scope of the testing called for in a network operator's plan would be required to be sufficiently broad to address all LTE capabilities and functions required for public safety broadband waiver recipients. Public safety network operators would also be required to certify their performance of such testing in accordance with their approved plans.

The *Fourth Further Notice* proposes to require that public safety LTE devices support, at minimum, a five megahertz channel bandwidth. This requirement would need to be taken into account when designing or purchasing devices for use on public safety broadband networks.

E. Steps Taken to Minimize Significant Economic Impact on Small Entities, and Significant Alternatives Considered

The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.[173]

The proposed requirements of the *Fourth Further Notice* are designed to ensure that public safety broadband networks achieve a baseline of operability and nationwide interoperability. In developing these proposed requirements, the Commission has made significant efforts to ensure that the requirements imposed are the minimum necessary to ensure that public safety broadband networks are truly interoperable. As an alternative to its proposed approach, the Commission could have proposed more detailed and burdensome conditions on the design and implementation of these networks. The proposed rules seek to balance the need for flexibility in network design, cost, and implementation with the demands of nationwide interoperability.

The establishment of differing compliance or reporting requirements for small entities would frustrate the goal of achieving nationwide interoperability. Given the importance of ensuring that public safety broadband networks are technically and operationally compatible, it is important that each network is subject to a comparable set of rules and requirements.

F. Federal Rules that May Duplicate, Overlap, or Conflict With the Proposed Rule

None.

[173] *See* 5 U.S.C. § 603(c).

STATEMENT OF CHAIRMAN JULIUS GENACHOWSKI

Re: *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, *Third Report and Order* and *Fourth Further Notice of Proposed Rulemaking*.

It has been almost ten years since the horrific acts of September 11, 2001. Almost seven years since members of the bipartisan 9/11 Commission urged action to ensure that first responders have the ability to communicate with each other over interoperable networks.

But nationwide interoperability for our first responders has remained elusive.

As we noted in the National Broadband Plan, we now have a real opportunity to ensure nationwide interoperability -- using spectrum cleared by the digital television transition and state of the art mobile broadband technologies.

An interoperable mobile broadband public safety network would not only allow first responders to communicate effectively with each other. It would provide first responders with real-time information on emergency incidents through photographs, video and other data.

First responders would be able to send critical information back to hospitals, including on-site scans and diagnostic information, improving success rates by taking advantage of every second.

And all these communications would be interoperable. They could be shared by first responders across agencies and jurisdictions, a critical communications element not possible today.

In addition to interoperability, a mobile broadband public safety network will also advance our Next Generation 911 goals. It will allow emergency responders to receive pictures, video or information that is sent via text to NG911 systems.

There are many challenges to making this vision a reality, including the funding and deployment of nationwide mobile broadband public safety network. One vital piece of the puzzle is a nationwide framework for interoperability. Without it, we won't achieve our goals.

That's why we created the Emergency Response Interoperability Center (ERIC), which is charged with the development of a technical and operational framework that will support and foster nationwide operability and interoperability in wireless broadband communications for America's first responders.

It's also why today we adopt a common air interface for a mobile broadband public safety network. While selecting a common technology platform is the exception and not the rule at the FCC, in order to ensure nationwide interoperability for public safety communications there's widespread agreement that a common air interface is desirable and necessary to enable nationwide interoperability

I thank the public safety community for working with us as we developed this proposal and for providing us with input in response to the Notice we are adopting today. And I look forward to continuing to work with the public safety community and our federal partners to create a framework that will enable the deployment of a nationwide interoperable broadband network for first responders.

I thank the staff for their tireless work on this and other critical public safety issues, and I'm looking forward to real progress.

That's why I'm pleased to announce today that we are moving forward with the ERIC Public Safety Advisory Committee (PSAC). The ERIC PSAC will be charged with providing recommendations to assist the Commission in the development of a technical framework and requirements for interoperability. The ERIC PSAC will be a key part of our effort to ensure that the public safety wireless broadband network is interoperable on a nationwide basis.

I am particularly pleased to announce that this important advisory Committee will be chaired by Chief Jeff Johnson, Past President of the International Association of Fire Chiefs and CEO of the Western Fire Chiefs Association and Deputy Chief Eddie Reyes of the City of Alexandria Police Department. These are two highly respected members of the public safety community, and I'm grateful that they have agreed to take on these roles. Thank you to Chief Johnson, Deputy Chief Reyes, and all of the members of the Committee for volunteering their time for this critical advisory role.

STATEMENT OF COMMISSIONER MICHAEL J. COPPS

Re: *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, *Third Report and Order* and *Fourth Further Notice of Proposed Rulemaking*.

The Commission has a long list of challenges it needs to tackle, but the safety of the American people must always be at the top of that list. We are fast approaching the ten-year anniversary of 9/11. *The 9/11Commission Report*—which I encourage everyone to read and read again—lays out in chilling detail a lack of communications readiness that seriously hampered our country's ability to respond on that terrible day. More should have been done immediately after 9/11 to address the needs of public safety. I called for it then, but little action was taken. Quite frankly, it is inexcusable that we still do not have a nationwide interoperable public safety network.

Every public safety organization should have access to a reliable system that they can use *anywhere*, to talk to *any* other first responder, in *any* emergency. Today's action gets us closer to that goal. We provide a clear framework to guide the development and deployment of a nationwide public safety broadband network in the 700 MHz public safety spectrum. When we granted waivers last year to allow a number of jurisdictions to move forward with deployment of public safety networks, we imposed an initial set of technical requirements aimed at ensuring that any network deployed could be integrated into and be interoperable with a nationwide network. We must avoid the balkanization of new public safety broadband networks, and ensure that all public safety organizations—those in jurisdictions with the money to start deployment today and those that cannot yet make such an investment—will be able to communicate with themselves and each other.

By adopting today a common technology platform, Long Term Evolution (LTE), we are hopeful that public safety organizations will be able to reap the benefits of the economies of scale and the continuing innovation in standards development resulting from ongoing private sector investment in the 700 MHz band. Better promoting the safety and protection of the American people today means, in large measure, realizing the potential of new and evolving technologies. We also propose further technical rules to support interoperability, public safety-to-public safety roaming, and use of the 700 MHz band by Federal government public safety entities.

Title I of our enabling statute gives us clear responsibility to ensure the safety of the American people through communications networks. Today we take just such an action—moving us closer to creating a much needed, nationally connected, interoperable broadband network for public safety. I commend Admiral Barnett and the amazing team in the Public Safety and Homeland Security Bureau for the hard work they did on this item and for the work they do each day to ensure first responders have access to the communications tools they need to protect American lives and property.

STATEMENT OF COMMISSIONER ROBERT M. McDOWELL

RE: *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; Third Report and Order* and *Fourth Further Notice of Proposed Rulemaking.*

I am voting to approve today's order and notice of proposed rulemaking, which discusses discrete matters pertaining to broadband interoperability within 10 megahertz of the full 24 megahertz of spectrum reserved for public safety use by Congress in 1997. It is important that the Commission continue to take any and all actions to provide the certainty necessary for the 20 jurisdictions that are building this spectrum pursuant to waiver, not to mention the numerous additional jurisdictions seeking to do so.

While I support our decision to require use of the Long Term Evolution (LTE) standard given the presence of a unique set of circumstances, I appreciate that we are seeking further comment on how future technology platforms would fit into this paradigm. In addition, I am pleased that the Commission remains committed to relocating those narrowband voice incumbents presently operating in the broadband public safety allocation. Down the road, I hope that we will examine and analyze ideas for ensuring that the full 24 megahertz block may be used more flexibly to support a complement of broadband uses and accommodate the ongoing rapid innovation in the mobile broadband sector. After all, the Commission undertook the design of this spectrum band more than a decade ago. Much has changed since then. I hope, therefore, that interested parties will continue to educate us on this important "big picture" issue.

In a perfect world, we would have already finalized an order setting forth auction and service rules for the D Block spectrum. Perhaps we would have already concluded an auction of this spectrum, and public safety entities would be in a position to elect to partner with these auction winners. I am eager to move to this step, which I urge that we undertake sooner rather than later.

Thank you to the Public Safety and Homeland Security Bureau for your ongoing work.

STATEMENT OF COMMISSIONER MIGNON L. CLYBURN

Re: *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.

Communications difficulties, during September 11th and Hurricane Katrina, made it clear that we should do everything in our power to develop an advanced communications system that meets our Nation's public safety needs. While Congress is actively reconsidering how best to address spectrum in the D Block, I am glad that our Commission is moving forward and taking important steps to develop the framework for the first, nationwide, interoperable broadband network for public safety.

The Further Notice takes a comprehensive approach, to identify issues that should be addressed, in order to develop a nationwide public safety broadband network that will not only be truly interoperable, but also reliable, secure, and advanced. I am especially pleased to see, that the Further Notice focuses on issues, which if not properly addressed, could result in interoperability gaps in the nationwide network. Those issues include ensuring interconnection with narrowband operations in legacy networks, and promoting greater coverage, performance, and quality of service requirements. I understand that staff carefully considered the input of public safety in our discussion of the coverage requirements. I am confident that the public safety jurisdictions, proudly represented here today, will continue to stay engaged, throughout these proceedings.

I am also glad that the Further Notice seeks comment on how best to interconnect with Next Generation 9-1-1 networks. These 21st Century 9-1-1 networks will permit the transmission of emergency messages, through various media types such as text, photos, and video, to 9-1-1 centers. If we want to develop the most advanced public safety system, then we should ensure that it can leverage the vast technological benefits the new NG-9-1-1 networks will offer.

I strongly support this Order and Further Notice, and applaud Admiral Barnett for his leadership and Jennifer Manner for her resiliency. I also wish to thank the other members of the Public Safety and Homeland Security Bureau, who worked on the Further Notice, for presenting such a thorough item.

STATEMENT OF COMMISSIONER MEREDITH ATTWELL BAKER

Re: *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; and *Amendment of Part 90 of the Commission's Rules*, WP Docket No. 07-100.

I am pleased today to support an Order and Notice of Proposed Rulemaking that takes us closer to our goal of establishing a nationwide, interoperable, wireless public safety broadband network. By requiring a common air interface—LTE—and specifying elements of the LTE standard for inclusion in each network deployment, this Order provides much needed guidance to members of the public safety community deploying or planning to deploy broadband networks. Our action today will help public safety officials select with certainty technology options that not only address their needs but also provide and support interoperability across the country. As such, it is truly an important step forward.

The accompanying Notice asks significant additional questions about further technical and operational considerations for public safety broadband networks. The Bureau's thoughtful and comprehensive analysis of the next set of critical deployment issues to be addressed reflects the complexity of the task before us, and before public safety.

State-of-the-art wireless broadband networks, which include a significant backhaul component, are complex undertakings. We should never forget their ability to interoperate is fundamentally a technological rather than a political question. Due deference must be paid to technical experts, and to the guidelines they establish.

I would like to thank everyone in the Bureau for all their hard, unfaltering dedication to what has often been difficult work. I am glad for the comments and participation of so many interested parties. In addition to the experts from industry and the public safety community, I would also like to acknowledge the work of the Departments of Justice and Homeland Security and NTIA. Interoperability is critical but we cannot get there without interagency cooperation. I would also like to recognize the input from my friends at the Public Safety Communications Research program in Boulder, Colorado at the Department of Commerce Labs. I am glad we are able to leverage all of your considerable expertise. It is hard to overestimate how important this is.