



# PUBLIC NOTICE

Federal Communications Commission  
445 12<sup>th</sup> St., S.W.  
Washington, D.C. 20554

News Media Information 202 / 418-0  
Internet: <http://www.fcc.gov>  
TTY: 1-888-835-5

DA 10-884

Released: May 18, 2010

## 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 No. 06-229

Comment Date: June 17, 2010

On May 13, 2010, the Commission released an order (*Waiver Order*) granting conditional waivers to twenty one public safety entities (Petitioners) for early deployment of public safety broadband networks in the 700 MHz public safety broadband spectrum (PSBB Block).<sup>1</sup> The *Waiver Order* establishes technical, operational and governance conditions for early deployment and requires each Petitioner to submit to the Bureau, within a specified time window, a detailed plan for achieving interoperability with other public safety broadband networks. The release of this order is a major step towards development of a nationwide public safety broadband network. However, there remain open several key technical issues focused on network deployment. In this Public Notice, the Public Safety and Homeland Security Bureau (Bureau) seeks further comment on interoperability, out-of-band emissions, and equipment certification surrounding public safety broadband network interoperability which will serve the basis for final rules for the public safety broadband network.

### Interoperability

We seek comment on several specific aspects of the technical rules for interoperability as follows:

*Applications.* Are applications specified in National Public Safety Telecommunications Council's Broadband Task Force Report (*NPSTC BBTF Report*)<sup>2</sup> sufficient for the purpose of promoting nationwide interoperability? If so, should the Commission incorporate these as requirements in its rules for the nationwide public safety network? If not, what additional applications are needed? Are some unnecessary? Do we need to specify any performance measures for these applications within a given network and while roaming on other networks?

<sup>1</sup> 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*, FCC 10-XX (rel. May XX, 2010).

<sup>2</sup> See National Public Safety Telecommunications Council, 700 MHz Public Safety Broadband Task Force Report and Recommendations (2009), *available at* [http://www.npstc.org/documents/700\\_MHz\\_BBTF\\_Final\\_Report\\_0090904\\_v1\\_1.pdf](http://www.npstc.org/documents/700_MHz_BBTF_Final_Report_0090904_v1_1.pdf).

Some of these applications may rely on the further development of standards. We seek comment on the availability and timeliness of the standards development process and what standard conformance we should require to achieve interoperability. How can we ensure requirements are met through our rules, while still recognizing the need for technical evolution?

*Roaming.* The *Waiver Order* requires two types of roaming categories that would allow users of one public safety network to roam to another public safety network. We seek comment on any additional roaming requirements, such as handoff between public safety networks especially in case of regional emergencies. We seek comment on whether there would be any technical ramifications requiring rule changes for the operation of public safety networks should the Commission decide to allow roaming to and from commercial networks. Also, we seek comment on governance and technical parameters for roaming agreements between public safety regional networks. Should there be bilateral roaming agreements between regional networks, or should a single common roaming agreement be adopted by the Emergency Response Interoperability Center (ERIC) as a minimum requirement? What other technical and governance requirements must the Commission adopt to ensure roaming among public safety agencies? Noting that we will also seek comment separately in an upcoming Notice of Proposed Rulemaking (NPRM) on roaming between public safety and commercial networks, what similar or different considerations should we take into account for public safety/commercial roaming?

*Priority Access.* The *Waiver Order* does not address priority access among the state or local public safety broadband networks. We envision that priority access, as a technical matter, will be commonly standardized, supported and required among public safety networks. As a minimum, we envision that priority access will include both the access to the common air interface and prioritization of traffic. What other elements, if any, should be included in this definition of priority access? How should this capability be implemented for public safety networks? How should priority access apply across different regional networks, for example, while roaming? Is the technology and associated standards ready for deployment? Should priority access schemes in this context be the same or compatible with the one to be deployed over the commercial networks? What are the operational issues that need to be addressed for priority access? What technical requirements for priority access need to be incorporated among public safety broadband networks? How should governance of this scheme be handled?

*System Characteristics, Interfaces and Testing.* We seek comments on the requirements set in the *Waiver Order* for use as a basis for the final FCC rules. Is the self-certification sufficient to ensure the Interoperability Testing (IOT) requirement on a long term basis? If not, what other mechanisms should be implemented? Similarly, if standards conformance testing as specified in the *Waiver Order* is not fully available in a timely manner, what other mechanisms should be implemented?

Regarding the selection and use of network identification numbers, the *NPSTC BBTF Report* notes that there are two alternatives for assigning network identification numbers to the regional networks: (1) use a single Public Land Mobile Network (PLMN) identifier for all of public safety, and use a secondary identifier (sub ID) for each individual regional network, or (2) use a different PLMN identifier for each regional network. Which alternative for network identifiers should be adopted? The report also notes that, because of the limited availability of network numbers, the number of network identification numbers must be kept below one hundred. Would this cause any problem for the second approach? How, if at all, could this problem be

remedied?

As noted in the *Waiver Order*, ERIC will consider the use of a common/single third-party clearinghouse as recommended by the *NPSTC BBTF Report* for the purpose of Inter-network authentication and connectivity. How should this clearinghouse be selected, and what criteria should be considered for selection?

*Security.* The *Waiver Order* requires the technical support for all the optional security features by the equipment and devices that are deployed for the public safety network. However, the selection of the security features, as a matter of operational capability, needs to be specified by ERIC. What features for Key Management, Encryption, Authentication, Authorization, and Identification need to be selected in order to optimize network security?

*Performance, Reliability, Capacity and Coverage.* The *Waiver Order* does not address the performance, reliability, capacity or coverage of public safety wireless broadband networks. How, if at all, do such operability parameters affect interoperability? Does a “network of networks” with different operability criteria at various parts hinder nationwide interoperability? Is service ubiquity important for public safety across all networks? For example, would it be important if performance and reliability of public safety service allowed 256 Kbps at the cell edge in one network, but only 128 Kbps in another network? Or similarly, would it be important if variances in capacity and coverage across regional networks created disparities of service throughout the nation? On the other hand, would the benefits of local control over these matters outweigh the benefits of service ubiquity and transparency? What requirements for performance, reliability, capability and coverage, if any, should the Commission adopt for the public safety broadband network or devices utilized on the network?

*Nationwide Core.* The *Waiver Order* requires the use of LTE and the associated “Evolved Packet Core” (EPC) for each public safety regional network. However, the order does not address a whether there should be a nationwide core to which all the individual networks would be connected and assumes connection to Internet as a minimum for the purpose of interconnectivity and roaming. We seek comment on whether there should be a nationwide core created for the purpose of achieving a nationwide interoperable broadband network for public safety. How would this nationwide core achieve the essential goal of nationwide interoperability and what functions should this core have? For example, would such a core network facilitate interoperability and connectivity amongst regions and provide security, performance and reliability that otherwise Internet could not provide? Does the benefit outweigh the cost of such network and what are other alternative means that can be implemented to achieve this goal? What model should be adopted for deployment and operation of such core network? Should the FCC establish such a model and the corresponding requirements for this nationwide core? Is there another approach that is appropriate? If a nationwide core is not the right approach, what other alternatives are available?

*Network Operations, Administration and Maintenance (OA&M).* 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 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 and nationwide basis? 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?

*Governance.* An important part of achieving interoperability is governance. The *Waiver Order* does not provide an approach for governance of the nationwide public safety broadband network. Accordingly, we seek comment on how we should ensure a governance structure that promotes interoperability. Should we require the waiver jurisdictions to submit reports to the FCC that detail the steps they are taking to align their investments to governance standards relating to interoperable emergency communications, including alignment of investments to relevant Statewide Communications Interoperability Plans (SCIP), coordination of expenditures with the grantees' Statewide Interoperability Coordinators (SWIC), and any review required by the relevant Statewide Interoperability Governing Bodies (SIGB) and network? Are there other mechanisms we can leverage to ensure interoperability? How can we ensure that the governance procedures contained in the Plans submitted to the Commission align to national governance requirements? What other actions are required?

### **Out-of-Band Emissions (OOBE)**

We recognize that 3GPP Release 8 Long Term Evolution (LTE) has requirements to enable co-existence in the same geographical area and co-location between operators on adjacent channels, and that it includes other co-existence and interworking specifications.<sup>3</sup>In the *Waiver Order*, the Commission specified  $43 + 10\log P$  dB as the OOBE limit for operations in the PSBB Block. We seek comment on the benefits of this specification, or of any proposed alternative specification, for the public safety broadband network in protecting and promoting the use of both the PSBB Block and the D Block and minimizing interference. If we impose an OOBE limit on the PSBB Block that is different from the limit currently imposed on the Petitioners, what should that limit be and what benefits will be derived from applying them? If more stringent OOBE limits were applied to the PSBB Block, would it be possible to attenuate signals outside the band without a guard band between D Block and the PSBB Block? Would this require stringent filtering that would be costly or otherwise impractical to implement?

### **Equipment Certification**

In the *Waiver Order*, the Commission waived the equipment certification requirements under Section 90.203 of the rules and required the manufacturers to comply with the various technical requirements of 3GPP Release 8 LTE specifications pending finalization of the rules. What impact will any changes in the Commission rules have on the equipment that may be deployed for operations in the PSBB Block prior to the adoption of final rules?<sup>4</sup> What alternative approach would vendors and authorized network operators propose to minimize the

---

<sup>3</sup> This requirement can be found in specification 3GPP TR 36.913 V8.0.1 (2009-03).

<sup>4</sup> The Commission's equipment authorization rules restrict the changes to certificated equipment. See 47 C.F.R. § 2.1043.

impact in the field deployed equipment, for continued interoperability, prior to the adoption of final rules?<sup>5</sup>

How do the licensees and manufacturers plan to address the continued evolution of the 3GPP standard from Release 8 LTE to future 3GPP releases? How should the Commission address this (*i.e.*, the continued evolution of the 3GPP standard from Release 8 to future 3GPP releases) in establishing the future interoperability requirements, such that there is minimal impact on the deployed equipment while continuing to provide necessary functionality?

It is common practice within the wireless industry for a network operator to qualify user devices and other equipment that will be used on its network to ensure compatibility with industry standards as specifically applied within its network. Some network operators support 3<sup>rd</sup> party service providers and equipment manufacturers with technical programs to adapt their devices to the operator's network.

Should the Commission require that public safety network operators avail themselves of these processes to ensure mobile devices selected for public safety use will operate not only on public safety networks but be able to roam onto specific commercial carrier networks as well? If so, what criteria should be used to select which commercial networks equipment should be qualified for use on?

## FILING PROCEDURES

Comments may be submitted using (1) the Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies.<sup>6</sup> Comments can be filed through the Commission's ECFS filing interface located at the following Internet address: <http://www.fcc.gov/cgb/ecfs/>. Comments can also be filed via the Federal eRulemaking Portal: <http://www.regulations.gov>.<sup>7</sup> In completing the transmittal screen, commenters should include their full name, U.S. Postal Service mailing address, and the applicable docket or rulemaking number. Parties who choose to file by paper must file an original and four copies of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- 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 12<sup>th</sup> St., SW, Room

---

<sup>5</sup> *Id.*

<sup>6</sup> *See* Electronic Filing of Documents in Rulemaking Proceedings, 63 Fed. Reg. 24121 (1998).

<sup>7</sup> Filers should follow the instructions provided on the Federal eRulemaking Portal website for submitting comments.

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.

- 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.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12<sup>th</sup> Street, SW, Washington DC 20554.

People with Disabilities: 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](mailto:fcc504@fcc.gov) or call the Consumer and Governmental Affairs Bureau at (202) 418-0530, (202) 418-0432 (TTY).

For further information about this Public Notice, please contact Jennifer Manner at (202) 418-3619.