FEDERAL COMMUNCIATIONS COMMISSION
PUBLIC SAFETY AND HOMELAND SECURITY BUREAU

MEMORANDUM

DATE: April 6, 2012

TO: Members of the Technical Advisory Board for First Responder Interoperability (Interoperability Board)

FROM: Public Safety and Homeland Security Bureau (PSHSB)

SUBJECT: FCC Staff Assessment of Public Safety Interoperability Requirements for the Public Safety Broadband Spectrum in the 700 MHz Band

---

Executive Summary

On March 28, 2012, the Interoperability Board asked PSHSB to provide a Federal Communications Commission (FCC or Commission) staff assessment "in support of issuing a potential ruling on public safety interoperability." Below, we provide you with this assessment, which constitutes a non-binding staff view of certain interoperability issues that were under consideration by the FCC prior to adoption of the Middle Class Tax Relief and Job Creation Act of 2012 (Spectrum Act). More specifically with respect to these issues, please note that FCC staff evaluated what baseline technical interoperability rules were necessary, in its view, to enable nationwide interoperability for the public safety broadband spectrum that was designated for this use prior to adoption of the Spectrum Act.

This memorandum addresses the following interoperability issues that were analyzed by staff in "issuing a potential ruling on public safety interoperability":

- the definition of "interoperability";
- technology platforms and system interfaces;
- prioritization and quality of service;
- performance;
- security;
- conformance testing; and
- additional issues.

Background

The public safety spectrum band that staff examined was the spectrum that was designated for public safety broadband use before the Spectrum Act (763-768 MHz/793-798 MHz) and licensed on a nationwide basis to the Public Safety Broadband Licensee (PSBL), the Public Safety Spectrum Trust (PSST).[1]

By way of background, in 2007, the Commission enacted rules for a mandatory partnership between the PSBL and a commercial licensee for the Upper 700 MHz D Block (758-763 MHz/788-793 MHz) for the construction and operation of a nationwide public safety broadband network using this spectrum.[2] At Auction, however, no bidder met the reserve price for the Upper 700 MHz D Block license.[3] The Commission then issued a *Second*[4] and *Third Further Notice of Proposed Rulemaking*[5] seeking comment on options to achieve an interoperable nationwide public safety network in light of this failure.

After issuance of the *Third Further Notice*, several 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.[6] In a May 2010 order, the Commission granted the requests of twenty-one public safety entities (Waiver Recipients) with conditions.[7] The *Waiver Order* required them to adopt the 3rd

---

[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 (2007) (*Second Report and Order*).

[2] *Id*. at 15428 ¶ 386.

[3] *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*).

[4] *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*).

[5] 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*).

[6] *See* Public Safety and Homeland Security Bureau Seeks Comment on Petitions for Waiver to Deploy 700 MHz Public Safety Broadband Networks, 24 FCC Rcd 10814 (PSHSB 2009) (*700 MHz Waiver Public Notice)*.

[7] 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 (2010) (*Waiver Order*)*; see also* Requests for Waiver of Various Petitioners to Allow the Establishment of 700

Generation Partnership Project (3GPP) Release 8 (LTE) broadband technology platform[8] and adhere to other technical requirements, which PSHSB then supplemented in an order it adopted in consultation with the Emergency Response Interoperability Center (ERIC).[9] The more detailed requirements of the *Interoperability Waiver Order* were designed to ensure that waiver deployments achieve interoperability from day one of operations and would be capable of integration into a nationwide system.[10] On January 9, 2012, the Bureau released an order requiring the Waiver Recipients to use a common PLMN ID in connection with anticipated deployments, and to retain the services of two entities, a numbering administrator and clearinghouse, to ensure the effective implementation of this PLMN ID within such deployments.[11]

The Commission began developing final service rules for the public safety broadband spectrum with the January 25, 2011 with the adoption of a *Third Report and Order* and *Fourth Further Notice of Proposed Rulemaking (Third Report and Order* and *Fourth Further Notice,* respectively*)*.[12] The *Third Report and Order* codifies for the nationwide network the requirement to use LTE technology and stays certain Part 90 rules that were designed to implement the mandatory public-private partnership. In the *Fourth Further Notice*, the Commission sought comment on technical matters relevant to ensuring nationwide operability and interoperability.

On May 24, 2011, the ERIC Public Safety Advisory Committee (PSAC) adopted an initial set of recommendations to assist the Commission and ERIC in developing rules to ensure nationwide interoperability. These recommendations are contained in four reports, which address: (1) Applications and User Requirements; (2) Security and Authentication; (3) Network Evolution; and (4) Interoperability.[13]

MHz Interoperable Public Safety Wireless Broadband Networks, PS Docket 06-229, *Order*, 26 FCC Rcd 6783 (PSHSB 2011) (Texas *Waiver Order*) (granting a twenty-second waiver, to the State of Texas).

[8] *See Waiver Order*, 25 FCC Rcd at 5157 ¶ 38.

[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,* 25 FCC Rcd 17156 (PSHSB 2010) (*Interoperability Waiver Order*).

[10] The *Waiver Order* requires Petitioners to submit "interoperability showings" detailing their plans for achieving interoperability with other segments of the network. *Waiver Order*, 25 FCC Rcd at 5164 ¶ 55. The State of Texas (Texas), the City of Charlotte, North Carolina (Charlotte) and the Adams County Communication Center (Adams County), have interoperability showings pending with the Bureau.

[11] *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 12-25 (PSHSB rel. Jan. 9, 2012) (*PLMN ID Order*).

[12] *See* Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket No. 06-229, *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, 26 FCC Rcd 733 (2011) (*Third Report and Order and Fourth Further Notice*).

[13] *See* Emergency Response Interoperability Center Public Safety Advisory Committee, Recommended Applications List and Guidelines for Developing Well-Behaved Applications (adopted May 24, 2011) (PSAC Applications and User Requirements Report); Emergency Response Interoperability Center Public Safety Advisory Committee, Considerations and Recommendations for Security and Authentication

Basis for Staff Consideration

In evaluating the record generated in response to the Fourth NPRM, staff recognized that the Commission has long regarded the deployment and operation of a nationwide public safety network using state-of-the-art commercial broadband technology as providing the best opportunity to achieve nationwide interoperability. Already waiver recipients were deploying the earliest phases of this nationwide network on a statewide or regional basis, but these pioneering jurisdictions have only the conditions required by their waivers and the limited requirements of the *Third Report and Order* to guide their efforts.[14] Staff believed that codifying baseline rules for the public safety broadband spectrum would establish with greater certainty the requirements that apply to the waiver recipients' build-outs and to future deployments. This in turn increases confidence that resources allocated for these deployments will be used effectively and providing increased market certainty for vendors.

The Commission received a number of comments opposing the adoption of further interoperability rules, although an underlying assumptions of some of these—that Congress would create a national governing body to manage the network—have now happened. Accordingly, we do not focus on this issue in this memo.

Several commenters raised a separate concern, that rules adopted at this early stage of deployment should not unduly constrain the growth and development of the network. The Association of Public-Safety Communications Officials (APCO) recommended that the Commission adopt only the rules "necessary now to ensure nationwide interoperability across the network."[15] Similarly, the San Francisco Bay Area (Bay Area) "recommend[ed] that the Commission set standards only to the extent absolutely necessary to allow regional operators to begin their build-outs with confidence that their networks will not be impaired or compromised by future interoperability rules."[16] Arguing that many of the rules proposed in the *Fourth Further Notice*, if adopted, "would need to be modified based on additional deployment and operational experience yet to come," the National Public Safety Telecommunications Council (NPSTC) cautioned against "codifying too many detailed rules at this early stage of broadband deployment."[17]

(adopted May 24, 2011) (PSAC Security and Authentication Report); Emergency Response Interoperability Center Public Safety Advisory Committee, Considerations and Recommendations for Evolution of the Public Safety Wireless Broadband Network (adopted May 24, 2011) (PSAC Network Evolution Report); Emergency Response Interoperability Center Public Safety Advisory Committee, Considerations and Recommendations for Public Safety Broadband Interoperability (adopted May 24, 2011) (PSAC Interoperability Report).

[14] *See* Adams County Quarterly Report, PS Docket 06-229 (July 15, 2011); State of Texas Quarterly Report, PS Docket 06-229 (July 18, 2011).

[15] APCO Comments at 2.

[16] Reply Comments of the City and County of San Francisco, City of Oakland and City of San Jose, Calif., at 8 (filed May 10, 2011) (Bay Area Cities Reply Comments).

[17] National Public Safety Telecommunications Council Comments at 1 (filed Apr. 11, 2011) (NPSTC Comments).

The baseline rules staff focused o were ones limited to the minimal essential requirements that must be established to ensure there is clear guidance for designing and constructing these networks and which must be present to form a solid foundation for any future network structure. These basic requirements were considered appropriate under any governance model or architectural framework that would be established for the nationwide network. Moreover, we regarded them as flexible enough to keep pace with rapid technological development. Staff believes that the baseline requirements promote a framework for nationwide interoperability on a competitive and cost-effective basis, with ample room for flexibility in the design, build-out, and operation of the nationwide interoperable public safety broadband network.

Areas of Analysis

Definition of Interoperability

The *Fourth Further Notice* proposed to amend the definition of "interoperability" in Part 90 of the Commission's rules to harmonize it with a definition used within the Department of Homeland Security (DHS) SAFECOM program.[18] Part 90 currently 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."[19] SAFECOM, however, defines interoperability as "the ability of emergency response 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."[20] The Commission observed that this latter definition better captures "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)" and tentatively concluded that it should adopt a definition of interoperability for Part 90 that is nearly identical to SAFECOM's.[21]

---

[18] SAFECOM is "an emergency communications program of the Department of Homeland Security's OEC [Office of Emergency Communications] and OIC [Office of Interoperability and Compatibility]" that "works to build partnerships among all levels of government, linking the strategic planning and implementation needs of the emergency response community with Federal, State, local, and tribal governments, to improve emergency response through more effective and efficient interoperable wireless communications." *See* SAFECOM, http://www.safecomprogram.gov/about/default.aspx (last visited Feb. 6, 2012).

[19] 47 C.F.R. § 90.7.

[20] *See* SAFECOM, http://www.safecomprogram.gov/about/default.aspx.

[21] *See Fourth Further Notice*, 26 FCC Rcd at 776 app. B. The proposed definition would have modified SAFECOM's by replacing the phrase "talk to" with the phrase "communicate with," a broader term that more clearly encompasses both voice and data communications. The proposed definition would also have referred to "public safety agencies" rather than "emergency response agencies."

The majority of commenters that addressed this issue supported amending the definition of "interoperability" in Part 90 of our rules as proposed in the *Fourth Further Notice*.[22] EF Johnson, for instance, states that "this more general statement better reflects the end goal of interoperability between Public Safety users for communications on demand and when needed and authorized."[23] The International Municipal Signal Association (IMSA) added that the proposed definition "aligns well with the needs of public safety and its current and future operations."[24] IPWireless, however, suggested that we modify the proposed definition to further clarify "on what and where users should be able to roam and obtain interoperability" when using public safety broadband networks.[25] The State of Minnesota (Minnesota) proposed an alternative definition, arguing that the proposal in the *Fourth Further Notice* "suggests that interoperability is a technology matter" and that this "does great disservice to the many people who work tirelessly to implement standardized operating procedures and incident communications plans that facilitate general interoperability."[26] The Commission's proposed definition, Minnesota argued, "limits the definition to public safety agencies and to radio communications systems" and should be replaced with a definition that recognizes "many technology types and government function."[27] Cassidian, meanwhile, proposed that we distinguish "tactical interoperability" among users and agencies from "technical interoperability" among devices and network nodes.[28]

Staff analysis is consistent with EF Johnson and other commenters who found that the Commission's proposed definition captures well the concept of interoperability and provides a sound basis for moving forward with the adoption of nationwide interoperability requirements for public safety communications networks. Accordingly, staff considered the definition of "interoperability" proposed in the *Fourth Further Notice*, "[t]he 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" and found it would be appropriate to implement.[29]

---

[22] Adams County Comments at 2; Seybold Comments at 6; EF Johnson Comments at 2 (filed Apr. 11, 2011); International Municipal Signal Association Comments at 4 (filed Apr. 11, 2011) (IMSA Comments); Los Angeles Regional Interoperable Communications System Comments at 2-3 (filed Apr. 11, 2011) (LA-RICS Comments); Layer 2 Connections Comments at 8 (filed Apr. 11, 2011) (Layer 2 Comments); NPSTC Comments at 5-6; NV Energy Comments at 2 (filed Apr. 11, 2011); State of Maryland Comments at 2 (filed Apr. 8, 2011) (Maryland Comments).

[23] EF Johnson Comments at 2.

[24] IMSA Comments at 4.

[25] IPWireless Comments at 4-5 (filed Apr. 11, 2011).

[26] State of Minnesota Comments at 1-2 (filed Apr. 11, 2011) (Minnesota Comments).

[27] *Id*. Minnesota proposes the following definition: "Interoperability is the ability to communicate, as needed, on demand, and as authorized at all levels of government and across all Public Safety disciplines." *Id*. at 2.

[28] Cassidian Communications Comments at 6-7 (Cassidian Comments) (filed Apr. 11, 2011).

[29] We did not believe that this definitional change would create any costs. The discussion below

Technology Platforms and System Interfaces

In the *Fourth Further Notice*, the Commission observed that LTE network elements can use one of two network addressing schemes, Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6), and asked whether "the use of both versions in various components of the nationwide network [would] create obstacles to achieving interoperability."[30] The Commission sought comment on the benefits and challenges of an all-IPv4 or all-IPv6 approach and on whether to establish a timetable for the public safety broadband network to complete migration to IPv6. The Commission asked specifically whether "any network element," including user devices, "should be required to support dual stack"—that is, to provide simultaneous support for both IPv4 and IPv6.[31]

As Motorola Solutions explained, "IPv6 is *not* backwards-compatible with IPv4. Users with IPv4 addresses will not be able to access IPv6 services or communicate with [an] IPv6 host, and vice versa."[32] Although the vast majority of today's networks and applications are IPv4-based,[33] there was widespread agreement among commenters that migration to IPv6 is inevitable for public safety broadband networks.[34] Underlying this view is the recognition that the IPv4 address pool is being exhausted. Nokia Siemens Networks (NSN) notes that the Internet Assigned Numbers Authority (IANA) "ran out of the free IPv4 address pool" in February 2011, and that Regional Internet Registries (RIRs) are expected to run out of IPv4 address reserves no later than 2012.[35] Staff thus agrees with Cassidian's observation that "due to the lack of IPv4 addresses … to achieve a uniform (nationwide) network, IPv6 will have to be supported."[36]

---

represents our consideration of the cost implications of the specific interoperability requirements that we had favored in evaluating the record of the *Fourth Further Notice*. We also note that neither this definition, nor the Commission's proceeding generally, considered the interoperability issues of consumer mobile equipment interoperability across commercial spectrum blocks in the 700 MHz Band. *See Public Notice*, Wireless Telecommunications Bureau Seeks Comment on Petition for Rulemaking Regarding 700 MHz Band Mobile Equipment Design and Procurement Practices, RM No. 11592, 25 FCC Rcd 1464 (2010).

[30] *Fourth Further Notice*, 26 FCC Rcd at 744 ¶ 30.

[31] *See id*.

[32] Motorola Solutions Comments at 6-7 (emphasis added).

[33] *Id*. at 7-8; *see also* NPSTC Comments at 11.

[34] *See, e.g.*, Motorola Solutions Comments at 7-8; *see also* Nokia Siemens Networks Comments at 8-9 (filed Apr. 12, 2011) (NSN Comments); Cassidian Comments at 10; Adams County Comments at 3; National Telecommunications and Information Administration Comments at 26 (filed June 10, 2011) (NTIA Comments); Alcatel-Lucent Comments at 12 (filed Apr. 11, 2011); Minnesota Comments at 3; IPWireless Comments at ¶ 30.

[35] NSN Comments at 8-9.

[36] Cassidian Comments at 10.

Some commenters advocated the exclusive use of IPv6-based network elements, including user devices, from the outset of network deployment. The Adams County Communication Center believed "it is in the best interest of the network's future" to require that all elements be IPv6-based "from the beginning," on the theory that "it will greatly reduce the costs and effort required to maintain future systems."[37] The National Telecommunications and Information Administration (NTIA) agreed, arguing that "future savings" would "far outweigh" the "minor incremental costs" of implementing an all IPv6 approach.[38]

NPSTC, on the other hand, observed that "[m]ost of the current applications deployed in public safety are based on IPv4."[39] The vast majority of public safety network elements today are also IPv4-based, including existing equipment that jurisdictions might leverage in constructing LTE networks and significant portions of the network backbone infrastructure that routes traffic. Given the current dominance of IPv4-based network elements in public safety systems, it was clear to us that support of IPv4 was a necessity at this nascent stage of deployment. In reaching this determination, we observed that commercial networks are also overwhelmingly IPv4-based and, as Motorola Solutions explained, "the transition from IPv4 to IPv6 end user traffic will likely take a significant amount of time."[40] We thus would expect IPv4-based network elements to remain in commercial networks in large quantities indefinitely. We believe that these networks transition from IPv4 to IPv6, "dual stack" commercial user devices would be needed to allow compatibility with both addressing schemes.

The same observation holds true for the public safety broadband network. Public safety user devices that support only IPv4 would need to be upgraded as networks migrate to IPv6. On the other hand, those devices that support only IPv6 would be unable to use many existing applications or interoperate with IPv4-based infrastructure. Either scenario would impair interoperability or generate costs in the future to retrofit existing user devices.[41] In contrast, the use of dual stack devices at the onset of network deployment would not create any incremental user device cost as the network migrates

---

[37] Adams County Comments at 3.

[38] NTIA Comments at 26.

[39] NPSTC Comments at 11; *see also* Motorola Solutions Comments at 7-8 ("Most government agencies deploying public safety LTE will have existing IPv4-based equipments and applications in narrowband system. . . . There will be an extended migration period where these agencies have to support the legacy IPv4 services.").

[40] Motorola Solutions Comments at 7.

[41] An all-IPv6 user device scenario would force operators either to employ translation mechanisms to convert IPv6 device traffic to IPv4 or replace all of their existing IPv4 equipment and applications at every network layer with state-of-the-art IPv6-only equipment and accept the prospect that devices may not be able to roam onto certain IPv4-based commercial networks. The former scenario would result in the high cost not only of designing the translation mechanisms, but also of the device testing that would then be necessary for each mechanism. The latter strategy presents the very costly proposition of massive, immediate upgrades to IPv6 for those that would otherwise be able to use a large amount of their existing infrastructure for the new broadband network—and even then, without the advantage of continued communication with IPv4 elements.

to IPv6 and would mesh the development of the public safety broadband ecosystem with the broader evolution of the wireless broadband market. As NSN observed, "[m]ost operating systems and IP stacks have been dual-stack capable for many years."[42]

We acknowledge that "there is always a cost of running two address families in one network."[43] However, our analysis supports that adopting this widespread industry practice to the public safety broadband sphere would create only minimal costs for jurisdictions, avoiding the incurrence of future costs and providing flexibility to individual operators to develop timetables for the necessary migration of their network infrastructure to IPv6. Moreover, we viewed this approach as one that would advance nationwide interoperability by enabling devices associated with networks in all phases of migration to IPv6 to access the full functionality of the network, including applications.

Accordingly, staff concluded that it would be appropriate to require that operators use on their networks only user devices designed and configured in dual-stack, *i.e*., capable of interoperating with both IPv4 and IPv6 networks and supporting applications based on either addressing scheme. With such a requirement, none of the devices operated on the network would lose their fundament interoperability due to a network infrastructure that contained IPv4-only and/or IPv6-only components.

[42] NSN Comments at 10.

[43] *Id.*

Prioritization and Quality of Service

In the *Fourth Further Notice*, the Commission sought comment on "how public safety broadband networks should support both prioritization and quality of service (QoS) among connections as well as applications over these connections."[44] The Commission stated that "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."[45] The Commission described the capabilities offered by the technology, namely "Allocation Retention Priority (ARP) … QoS Class Identifier (QCI) … and Access Class Barring [(ACB)],"[46] and sought comment on the adequacy of these capabilities to support traffic prioritization on the public safety broadband network. ARP assigns multiple levels of priority and flags to denote preemption capability and vulnerability for a connection; QCI assigns categories of connectivity performance for various application types; and ACB allows multiple levels of access classes to be barred from the network at times of congestion.

The record contained broad support for the use of QoS and prioritization capabilities in the public safety broadband network, including broad support for ARP, QCI, and ACB in particular.[47] NTIA favored these "standards-based solutions,"[48] while IPWireless observed that "the LTE standards provide a powerful set of capabilities for both user and application prioritization."[49] NSN further contended that "the capability defined in 3GPP Release 8, *i.e*., [ARP, QCI and ACB] are sufficient for supporting priority access within the public safety network."[50] Alcatel-Lucent meanwhile "recommends that governance rules should be defined across all public safety jurisdictions for use of [ARP and QCI] to facilitate priority access services for public safety networks."[51] Aeroflex explained that "[a]n emergency situation may require clearing the network to save capacity only for responders to the emergency . . . . [S]pecial features for quality of

[44] *Fourth Further Notic*e, 26 FCC Rcd at 746 ¶ 43. 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 categories of connectivity performance to different applications based on certain performance attributes and objectives and maintain the network performance for the application within the acceptable range.

[45] *Id.* at 747 ¶ 45.

[46] *Id.* at ¶ 46.

[47] *See, e.g.*, Alcatel-Lucent Comments at 3; Ericsson Comments at 11-12 (filed Apr. 11, 2011); IPWireless Comments at 13-14; NSN Comments at 12; Telcordia Comments at 13 (filed Apr. 11, 2011); Telecommunications Industry Association Comments at 3 (filed Apr. 11, 2011) (TIA Comments); Motorola Solutions Comments at 13-14.

[48] Letter from Lawrence Strickling, Administrator, National Telecommunications and Information Administration, to Julius Genachowski, Chairman, Federal Communications Commission at 1 (dated Sept. 23, 2011) (NTIA Letter).

[49] IPWireless Comments at 13.

[50] NSN Comments at 12; *see also* Ericsson Comments at 12 ("Ericsson believes the current Release 8 QoS scheme is sufficient to support the required functionality.").

[51] Alcatel-Lucent Comments at 13.

service, pre-emption and other things … have to be used in a way that is standard across all vendors and networks so that this works as needed for public safety."[52]

Staff agreed with the majority of the commenters that supported the implementation of QoS and priority access capabilities in the public safety broadband network. We regarded prioritization as an "essential element" of the network and QoS as a "fundamental requirement of any network carrying multimedia services."[53] We believed that these capabilities would allow public safety agencies to prioritize users and applications within their jurisdictions as well as between jurisdictions. Public safety agencies rely on these capabilities to manage access to the network during emergencies and to support the proper functioning of mission-critical applications. We concluded that the implementation of a common set of prioritization and QoS capabilities in the public safety broadband network would increase the ability of public safety users from various jurisdictions and departments "to exchange voice and/or data with one another" when converging on the scene of a disaster or emergency.

The record demonstrated widespread support for the capabilities defined in the LTE standard, the technology platform already adopted for the public safety broadband network. Accordingly, staff concluded that operators should be required in the public safety broadband spectrum to use only network equipment and devices that fully support LTE prioritization and QoS capabilities in accordance with the relevant LTE Release 8 specifications documents should be used. Staff further concluded that QCI will enable the regulation of applications have priority access to bandwidth over other applications, while ARP and ACB would allow operators to manage connections to the network and to prioritize them accordingly. We regarded these features as particularly crucial during the worst emergencies, when network capacity tends to be significantly constrained and resources must be carefully allocated.

ARP, ACB, and QCI are native to the LTE standard and can be incorporated into the public safety network without the purchase of additional hardware. Staff believes that delaying the introduction of these standard features could impede the management of network access and QoS during emergencies, which could jeopardize emergency response and ultimately threaten nationwide interoperability. Furthermore, we concluded that these features could be most cost-effectively implemented into deployments before service commences, rather than after devices and equipment have already been procured and deployed in the field.

Some commenters proposed that the Commission proceed one step further by adopting operational requirements for managing prioritization and QoS assignments on the public safety broadband network.[54] Telcordia, for instance, "encourages the FCC to develop

---

[52] Aeroflex Comments at 8 (filed Apr. 8, 2011)

[53] State of Minnesota Comments at 5-6.

[54] Alcatel-Lucent provided an example of a priority scheme and "recommends that governance rules should be defined across all public safety jurisdictions for use of LTE's Allocation and Retention Priority ('ARP') and QoS Class Identifier ('QCI') to facilitate priority access services for public safety networks." Alcatel-Lucent Comments at 13. Motorola Solutions supported the establishment of a nationwide

detailed guidelines on QoS and priority access treatment in the network and when roaming to other public safety and commercial networks."[55] Although we found it premature to address the operational aspects of user prioritization and QoS management at this early stage of network deployment, we recognized that nationwide interoperability would require consistency in the implementation of prioritization and QoS functionalities across the nationwide network. As NTIA observed, the "application of proprietary mechanisms to features critical to interoperability such as prioritization and QoS raise particular concerns."[56] Thus, while NTIA favored the "standards-based solutions" identified above, it recommended that the Commission prohibit jurisdictions "from employing prioritization and QoS features that are not embodied in the LTE standard."[57] We agreed with NTIA's recommendation because such a requirement would ensure that users of the public safety broadband network make use of a common set of prioritization and QoS mechanisms.

---

framework for priority access and QoS and stated that "there must be a nationwide QoS prioritization framework from which prioritization of public safety users is enabled across the nationwide system." Motorola Solutions Comments at 13. For the sake of roaming, NSN supported establishing "a nationally applicable prioritization scheme for all regional public safety broadband networks." Similarly, it supported defining "a minimum QoS level to be provided for each application that is nationally applicable." NSN Comments at 25-26. TIA supported the "standardization of the ARP value [that] insures appropriate priority for public safety and insures LTE resources are available especially for life threatening situations." TIA Comments at 11.

[55] Telcordia Comments at 13.

[56] NTIA Letter at 2.

[57] *Id*.

Performance

Observing the importance of network performance to achieving nationwide interoperability, the Bureau in the *Interoperability Waiver Order* established baseline performance requirements for the networks deployed by waiver recipients.[58] In the *Fourth Further Notice*, the Commission proposed to codify these performance requirements as final rules for the nationwide network.[59] In particular, the Commission tentatively concluded that it should require the public safety broadband network to provide outdoor coverage at minimum physical layer data rates of 256 kilobits per second (kbps) uplink (UL) and 768 kbps downlink (DL) for all types of services and devices, for a single user at the cell edge.[60] As part of its initial design, the network built out by each jurisdiction would be required to provide the minimum data rates based on a sector loading of seventy percent throughout the entire network.[61] The Commission also tentatively concluded that it should require each jurisdiction to certify, within thirty days of its date of service availability, that the network is capable of achieving these data rates.[62] This certification would 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.[63] The Commission also sought comment on whether to require periodic reports and updates on coverage maps and data on actual usage and traffic.[64] Finally, the Commission tentatively concluded in the *Fourth Further Notice* that it should require jurisdictions to meet the performance requirements proposed in the *Fourth Further Notice* prior to the date that service was available on the network.[65]

Many commenters acknowledged the necessity of establishing performance parameters for the public safety broadband network to facilitate interoperability.[66] Northrop Grumman supported the Commission's proposed minimum data rates and sector loading requirement, maintaining that "[t]hese are practical limits allowing the system to linearly support increasing user demand from normal to incidence operations without dropping active public safety user traffic."[67] Cassidian also "agrees with the

---

[58] *See Interoperability Waiver Order,* 25 FCC Rcd at 17162 ¶ 22.

[59] *See Fourth Further Notice*, 26 FCC Rcd at 751 ¶ 61.

[60] *Id*. In the *Fourth Further Notice*, the Commission clarified that "[t]he 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." *See Fourth Further Notice*, 26 FCC Rcd at 751 ¶ 72.

[61] *Id*.

[62] *Id*.

[63] *Id*.

[64] *Id*. at 751-52 ¶ 62.

[65] *Id*. at 751 ¶ 61.

[66] Cassidian Comments at 19; *see also* NV Energy Comments at 5 (supporting the proposed minimum data rates but proposing a fifty percent sector loading requirement).

[67] Northrop Grumman Comments at 20 (filed Apr. 8, 2011).

recommended performance requirements of 256 kb/s uplink and 768 kb/s downlink."[68] NSN examined in particular the costs and benefits of establishing a 256 kbps UL requirement, ultimately finding this requirement "reasonable for the expected performance of a 5x5 MHz FDD LTE system."[69] NYPD also supported the proposed performance requirements but cautioned that these should be "minimum required standards, particularly in the early stages of network deployment, allowing regional network operators to exceed the standards as the network matures and technology evolves."[70] NV Energy supported the proposed minimum data rates but recommended a fifty percent sector loading requirement, arguing that "[i]n rural areas [it] is unlikely that a more stringent requirement will be needed."[71] Motorola Solutions, on the other hand, argued that "[a]ny RF performance requirements defined with fixed data rates must allow for variance" in loading assumptions, among other factors.[72] Motorola Solutions also urged that the minimum data rates be measured not at the physical layer but "closer to the application layer, such as the UDP payload data rates," contending that "data rates specified at this layer are representative of rates that users would experience" and "can be easily measured with off-the-shelf tools and monitors."[73]

Some commenters opposed the adoption of performance requirements, asserting that each jurisdiction should have the discretion to set performance parameters for the network in its area.[74] Harris stated that "not all jurisdictions should be subject to the same coverage and performance requirements," noting that jurisdictions "may have varying coverage needs."[75] Ericsson contended that the system performance requirements proposed in the *Fourth Further Notice* "should not be inflexibly mandated through a rule or Commission policy."[76] Alcatel-Lucent argued that "interoperability is not synonymous with service availability" and that "[t]wo distinct contiguous radio systems built around different service edge criteria, with one network denser than the other, can still allow for interoperability."[77] The PSST argued that "there is no need for the FCC to regulate 'baseline operability'" of the public safety broadband network, observing that "the Commission does not do this for narrowband, commercial, and most

---

[68] Cassidian Comments at 19.

[69] NSN Comments at 17.

[70] NYPD Reply Comments at 20 (filed May 10, 2011).

[71] NVEnergy Comments at 5.

[72] Motorola Solutions Comments at 20.

[73] *Id*.

[74] *See* Alcatel-Lucent Comments at 18; Seybold Comments at 8; APCO Comments at 8; Harris Comments at 23-24 (filed Apr. 11, 2011); Ericsson Comments at 13-14; IPWireless Comments at 19; Mesa Comments at 6; NPSTC Comments at 15-18; PSST Comments at 17-18; Minnesota Comments at 8; PSST-OAC Comments at 3, 6.

[75] Harris Comments at 25.

[76] Ericsson Comments at 13.

[77] Alcatel-Lucent Comments at 18.

other networks."[78]

We recognized that radio network planning is a crucial factor in ensuring nationwide interoperability, and that the design of the public safety broadband network must accommodate users from various jurisdictions and departments and support the disparate broadband applications used in day-to-day operations. We regarded the adoption of minimum performance requirements as a way to help ensure that public safety broadband users share a baseline of operability for their mission-critical applications, even when responding to emergencies in other jurisdictions or in geographically remote areas. This appeared to us to be an essential capability for public safety users, as it is impossible to determine in advance where an emergency may strike or the scope of the response. As NSN acknowledged, the failure to establish a baseline performance standard for the public safety broadband network would result in a "higher probability of users falling into areas where the minimum performance is below [their] expectations" or, "in the worst case, even [a] risk of service unavailability."[79] We concluded that that the adoption of baseline performance requirements would thus promote interoperability, defined as the ability of users "to exchange voice and/or data with one another on demand, in real time, when needed and when authorized."[80]

Moreover, we took note of the Commission's observation in the *Fourth Further Notice* that "[s]pectrum is a valuable public resource and the Commission is committed to ensuring that this resource is used efficiently."[81] Similarly, we recognized that the propagation characteristics and other features of the public safety broadband spectrum make it particularly desirable for a wireless broadband network. Staff believes it is appropriate to that the spectrum allocated for a public safety broadband network will achieve a degree of spectral efficiency, operability, and interoperability consistent with that allocation and with the fundamental goals of the proceeding.[82] Staff also was committed to ensuring that the public safety broadband network would realize the full benefits of LTE technology, which is designed for implementation using a cellular network architecture with sites deployed more densely than is typical for a public safety narrowband voice network.[83] Staff reasoned that the use of a cellular network architecture would align deployment of the public safety broadband network with commercial LTE deployments, enhancing opportunities to leverage commercial assets and economies of scale.

Staff determined that the minimum data rates proposed in the *Fourth Further Notice* set a reasonable and practical baseline standard for the performance of a public safety

---

[78] PSST Comments at 17.

[79] NSN Comments at 17.

[80] *See supra* Section III.B.1.

[81] *Fourth Further Notice,* 26 FCC Rcd at 750 ¶ 59.

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

[83] *See* 3GPP TR 36.942, Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) system scenarios.

broadband LTE network.[84] While we recognized that data rates, particularly the UL data rate, are key drivers of the cost of a network, we concluded that baseline rates were necessary to realize the benefits of spectral efficiency and enhanced network functionality that LTE technology promises. The benefit of adopting 256 kbps UL and 768 kbps DL as minimum baseline data rates for operation of the broadband network would be the assurance that, at a minimum, public safety users could receive a baseline level of service needed to support broadband applications.[85] Although we recognized that the proper definition of "broadband" service may vary from one context to another, we found that the rates proposed in the *Fourth Further Notice* set a baseline for the support of bandwidth-intensive applications, including image transfers and video uploads, that public safety commenters widely envision for this network[86] and that should deliver concrete public safety benefits. For instance, first responders in the San Diego area use a broadband application that employs facial recognition technology to identify individuals with documented gang affiliations,[87] and doctors at George Washington University use broadband technology to monitor patient vital signs transmitted wirelessly from the scene of an emergency.[88] APCO has remarked that "[d]ata (including video) is expected to take on greater importance in emergency situations and will quickly assume a mission critical status."[89] We regarded the nationwide deployment of a broadband network dedicated for public safety use as the key to ensure that such services and applications would be available on an interoperable basis, with the degree of reliability and security that public safety users require.

---

[84] *See* NSN Comments at 17; Northrop Grumman Comments at 20.

[85] In a network designed to achieve the minimum data rates proposed in the *Fourth Further Notice*, the minimum cell edge uplink rate—256 kbps—will determine the link budget and, ultimately, the maximum size of the cell radii. The number of cells is the key driver of network infrastructure costs. A network properly designed to support 256 kbps UL at the cell edge throughout the coverage area would also support 768 kbps or higher DL. Accordingly, we focused our analysis on the costs and benefits of imposing the 256 kbps UL requirement.

[86] *See, e.g.,* PSST Comments on National Broadband Plan Public Notice #8, GN Docket 09-51 at 4-5 (filed Nov. 12, 2009) (identifying "Mobile Video and Complex, High-Quality Image Transmission Applications" among "current and anticipated public safety applications"); see also APCO Comments on National Broadband Plan Notice of Inquiry, GN Docket 09-51 at 3 (filed June 8, 2009) (predicting that "public safety is likely to have a substantial need for all types of video applications" and clarifying that "[v]ideo will need to be real-time, with mobile (and probably airborne) capability over wide areas").

[87] *See* Automated Regional Justice Information System Presentation at National Broadband Plan Mobile Applications and Spectrum Field Hearing, Oct. 8, 2009, GN Docket 09-51 (filed Nov. 24, 2009).

[88] *See* Presentation of Dr. Richard Katz, Professor of Medicine, George Washington University, at National Broadband Plan Field Hearing on Improving Public Safety Communications and Emergency Response (Nov. 12, 2009) (video transcript available at http://reboot.fcc.gov/video-archives and slide presentation available at http://www.broadband.gov/fieldevents/fh_public_safety/katz.ppt).

[89] APCO Comments on National Broadband Plan Public Notice #8, GN Docket 09-51 at 9 (filed Nov. 12, 2009); *see also* Public Safety Joint Comments in Response to T-Mobile Ex Parte Filing, GN Docket 09-51 at 5-6 (filed Jan. 13, 2010) (identifying "critical broadband applications" for the network, including "[s]treaming video and graphical display", "[m]obile Geospatial information systems" and "[f]loor plans, drawings and 3D graphical displays").

256 kbps as a minimum baseline UL data rate for this network is also consistent with NPSTC's 2007 Statement of Requirements.[90] Additionally, the Department of Homeland Security's 2008 "Public Safety Statement of Requirements for Communications & Interoperability" identified 256 kbps as the minimum rate for "tactical and live surveillance video" operations under specified parameters.[91] Our analysis concluded that the establishment of 256 kbps as the required minimum cell edge UL rate would advance nationwide interoperability by ensuring the nationwide availability of certain minimum applications and services, such as those discussed above. Thus, in our view, allowing operators to build to a lower performance standard, on the other hand, would fail to ensure that the network consistently achieved a level of service sufficient to meet public safety user needs and requirements as reflected in the record.

Staff acknowledged that data rates of 256 kbps UL and 768 kbps DL may not support every application or service envisioned for the nationwide network under every circumstance. Andrew Seybold, for instance, has remarked that "video data rates of 256 Kbps do not provide the level of resolution that will be needed for various kinds of incidents."[92] We observed, however, that a network supporting 256 kbps at the cell edge would deliver higher rates throughout the cell site coverage area, particularly for users closest to the base station. And we recognized that the Commission recently observed, in its proceeding to establish the Connect America Fund, that "[s]ignal coverage satisfying [200 kbps UL and 768 kbps DL at the cell edge] will produce substantially faster speeds under conditions closer to the base station, very often exceeding the 4 Mbps downstream and 1Mbps upstream that have been proposed as minimum speeds for fixed broadband."[93] As the Commission explained in its *Sixth Annual Broadband Progress Report*, actual rates of 4 Mbps DL/1 Mbps UL represent the minimum "required to stream a high-quality—even if not high-definition—video while leaving sufficient bandwidth for basic web browsing and e-mail."[94] Staff found that the

---

[90] *See* National Public Safety Telecommunications Council, Statement of Requirements (2007) (filed as attachment to NPSTC Comments on *Second Further Notice*, PS Docket 06-229 (filed June 20, 2008)).

[91] *See* DEP'T OF HOMELAND SECURITY, SAFECOM PROGRAM, PUBLIC SAFETY STATEMENT OF REQUIREMENTS FOR COMMUNICATIONS & INTEROPERABILITY, VOLUME II 31-32 (2008).

[92] *See* Andrew Seybold Filing, PS Docket 06-229 at 9 (filed June 23, 2011) (commenting on FED. COMMC'N COMM'N, THE PUBLIC SAFETY NATIONWIDE INTEROPERABLE BROADBAND NETWORK: A NEW MODEL FOR CAPACITY, PERFORMANCE AND COST (2010)).

[93] *See* Connect America Fund, WC Docket 10-90, *Report and Order and Further Notice of Proposed Rulemaking*, FCC 11-161 at 129 ¶ 362 (rel. Nov. 18, 2011).

[94] *See* Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, Amended by the Broadband Data Improvement Act, GN Docket Nos. 09-137, 09-51*, Report,* 25 FCC Rcd 9556, 9559 ¶ 5 (2010) (*Sixth Broadband Progress Report*) (establishing the 4 Mbps/1 Mbps broadband speed threshold for the first time). The report noted, however, that "[t]his definition [of "broadband"] is not a standard that the Commission is bound to employ in other reports or proceedings." *Id. See also* Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act, GN Docket No. 10-159, *Seventh Broadband*

baseline cell edge rates discussed herein, would ensure that the public safety broadband network would provide broadband service that meets this benchmark—4 Mbps DL and 1 Mbps UL—throughout significant portions of the coverage area. We determined that failure to build to these cell edge specifications, on the other hand, would reduce public safety users' access to high-data-rate broadband applications and services such as "high-quality [streaming] video," greatly detracting from the "broadband" character of the emerging network.

We estimated that doubling the minimum required uplink data rate from 256 kbps to 512 kbps would increase the radio access network costs by 36 percent, and further doubling it to 1.2 Mbps would increase the network costs by an additional 35 percent.[95] Given that billions of dollars in capital costs have been projected for a nationwide build-out,[96] each doubling of the minimum required uplink rate would require at least hundreds of millions of additional dollars of investment to build out this network. Accordingly, while higher minimum rates would bring with them significant improvements in network performance and the potential for use of more intensive data applications, we concluded that a more modest baseline rate would be appropriate at this early stage of deployment. We did not regard the evidence in the record as sufficient to conclude that the additional benefits of imposing higher minimum rates would exceed the costs. We stress that this cost-benefit assessment was predicated on the fact that the required baseline rates were to be measured at cell edge and that much higher rates would be provided throughout the coverage area. Moreover, as NYPD recommended, implementation of "minimum required standards" for network performance would preserve flexibility "to exceed the standards as the network matures and technology evolves."[97]

We saw baseline requirements for network performance as an effective way to provide certainty for public safety broadband users as to the minimum performance that can be expected anywhere in the nationwide network, thereby advancing nationwide interoperability. We concurred with Motorola Solutions' view, however, that the adoption of a fixed sector loading requirement would unduly constrain network design and deployment flexibility. We also concluded that without a numerical sector loading requirement, the costs of compliance with the minimum data rates discussed herein would also be lower, because a network built with reduced sector loading will be capable of achieving the required data rates using marginally fewer sites.[98] Accordingly,

---

Progress Report and Order on Reconsideration, 26 FCC Rcd 8008 (2011).

[95] This estimate was based on an internal staff analysis. IPWireless provided a comparable estimate in its comments. *See* IPWireless Comments at 19. It estimated a 30 percent increase in network costs from increasing the minimum uplink rate from 256 kbps to 512 kbps and over a 54 percent additional increase from increasing it from 512 kbps to 1.2 Mbps. *Id*.

[96] *See, e.g.*, FED. COMMC'N COMM'N, OMNIBUS BROADBAND INITIATIVE , CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 318 (2010) (National Broadband Plan).

[97] NYPD Reply Comments at 20.

[98] Holding data rates constant, an LTE network's cell radii must reduce in size to accommodate an increase in sector loading.

we did not support the implementation of a sector loading requirement.

Security

In the *Fourth Further Notice*, the Commission identified "five security feature groups" defined in LTE specifications documents: (I) network access security; (II) network domain security; (III) user domain security; (IV) application domain security; and (V) visibility and configurability of security.[99] The Commission tentatively concluded that it should require the public safety broadband network to fully support three Network Access Security group features specified in 3GPP TS 33.401: 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).[100] These are features designed to secure the most vulnerable component of the network, the air interface between users and eNodeBs.

The majority of commenters addressing this issue supported the adoption of these security features,[101] with some noting that these requirements are consistent with the recommendations set forth in the NPSTC's 2007 Broadband Task Force (BBTF) report.[102] Others recommended that the Commission adopt additional features of TS 33.401,[103] features of 33.210,[104] and a variety of other measures, such as end-to-end Virtual Private Network (VPN) functionality.[105] Telcordia and Northrop Grumman suggested establishing a full suite of protocols for end-to-end protection,[106] while Motorola Solutions and NSN suggested the adoption of network domain security

---

[99] *Fourth Further Notice*, 26 FCC Rcd at 752-53 ¶ 65.

[100] *Id*. at 753 ¶ 66. These confidentiality and integrity security features are specified in Sections 5.1.3 and 5.1.4 of 3GPP TS 33.401. *See* 3GPP TS 33.401, V8.6.0 (2009-12), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture; (Release 8)," December, 2009.

[101] *See, e.g.*, Bay Area Comments at 13; Cassidian Communications Comments at 20-21; Harris Comments at 21; Motorola Solutions Comments at 22-23; Telcordia Comments at 15; NSN Comments at 20; NTIA Comments at 30.

[102] *See* NAT'L PUB. SAFETY TELECOMM. COUNCIL, 700 MHZ PUBLIC SAFETY BROADBAND TASK FORCE REPORT AND RECOMMENDATIONS AT 21 § 6.3.3, 65-66 (NPSTC BBTF REPORT); *see also* Northrop Grumman Comments at 5-6.

[103] *See, e.g.*, Motorola Solutions Comments at 21-22; NSN Comments at 20.

[104] *See, e.g.*, Telcordia Comments at 15 ("Telcordia suggests that the FCC establish requirements for a minimum set of network domain security features as well as features for visibility and configurability of security."); Motorola Solutions Comments at 22.

[105] *See, e.g.,* Northrop Grumman Comments at 13.

[106] *See* Telcordia Comments at 15; Northrop Grumman Comments at 13.

standards.[107] The PSAC recommended the adoption of additional security features from the network domain security, user domain security and application domain security feature groups.[108]

The security features proposed by the Commission in the *Fourth Further Notice* are part of the LTE standard and are available for deployment in commercial networks. The FCC acknowledged that the cost of their implementation in public safety build-outs would depend on the extent to which these features were being deployed commercially. However, as the record demonstrated, the failure to implement adequate security features for the nationwide broadband network would render it vulnerable to intrusions and attacks that could pose incalculable risks to life, health, and property, given the specialized purpose the network would serve. Accordingly, staff believes that the benefits of adopting at least basic security requirements would clearly exceed the costs associated with their implementation and is prudent. In short, we viewed the failure to establish a baseline level of security support as a threat that would undermine the very purpose of this network. Furthermore, we observed that early implementation of these essential security features – before service commences – would be much more cost-effective than attempting to graft these feature onto the network after devices and equipment have already been procured and deployed in the field.

We regarded the security requirements proposed for adoption in the *Fourth Further Notice* crucial to maintaining reliable communications and to protecting public safety user traffic from intentional and unintentional intrusions or attacks. Similarly, we believed that it would be critical to require the implementation of security requirements from the outset of deployment to facilitate an efficient roll-out of the network and to preserve interoperability. Thus, we agreed with the Commission's proposed requirement that the public safety broadband network support, as a common security baseline, the three features for network access security specified in 3GPP TS 33.401 as a common security baseline.

We recognized that individual jurisdictions may opt to implement LTE security features that exceed this baseline, and that such enhancements could threaten interoperability by creating disparities among networks. Users traveling to a network with a different security profile may find their user devices unable to connect to the host network, crippling their ability to respond. While we acknowledged that this could be a serious danger, we believed that jurisdictions could minimize this potential by configuring their networks and devices to accommodate users with varying security profiles. Accordingly, we supported the requirement that the deployments of operators in the public safety broadband spectrum be capable of supporting any user device in which the required Network Access Security features are operable. We also supported the requirement that all user devices operated in the public safety broadband spectrum be capable of operating on any network that supports these security features. We found that these requirements would provide flexibility to jurisdictions in securing their

[107] *See* Motorola Solutions Comments at 21-22; NSN Comments at 20.

[108] *See* PSAC Security and Authentication Report.

networks, and that implementation of baseline security features would neither impair interoperability throughout the network nor compromise the security of network deployments that have implemented non-proprietary enhanced security features.

Conformance Testing

In the *Fourth Further Notice*, the Commission tentatively concluded that it should require that all user devices operated in the public safety broadband spectrum complete conformance testing.[109] The Commission observed that a conformance testing and certification process had not yet been developed for user devices operating in LTE Band Class 14 but that the PTCRB[110] was expected to complete development of such a process within the near term. The Commission proposed to require that, within six months of the Commission's release of a public notice announcing the availability of a PTCRB testing process for Band Class 14, each jurisdiction operating in the public safety broadband spectrum must certify to the Commission that it had completed this testing process for the user devices operating on its network.[111] The Commission further proposed to require that, in its certification to the Commission, each jurisdiction commit to any future testing called for by the certification process.

The record strongly supported conformance testing for public safety user devices.[112] Motorola Solutions, for instance, stated that "all user devices should be subject to conformance testing to ensure basic device-network interoperability."[113] Northrop Grumman "concurred with the Commission on the need to have all public safety LTE User Equipment (UEs) pass the certification tests based on the 3GPP Release 8 standards for conformance (3GPP 36.141, etc.)."[114] Telcordia also supported the Commission's requiring "conformance testing on every user device to ensure compliance to 3GPP LTE Release 8 and higher standards."[115] Aeroflex similarly contemplated that PTCRB conformance testing would be conducted on public safety

---

[109] *See Fourth Further Notice*, 26 FCC Rcd at 762 ¶ 106.

[110] 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/.

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

[112] *See* Aeroflex Comments at 1; Minnesota Comments at 12; 7Layers Comments at 4-5 (filed Apr. 11, 2011); Alcatel-Lucent Comments at 21; Bay Area Comments at 20-21; Cassidian Comments at 28; Idaho National Laboratory Comments at 1 (INL Comments); IPWireless Comments at 29; Motorola Solutions Comments at 8; NSN Comments at 27; Northrop Grumman Comments at 17; Telcordia Comments at 17; NYPD Reply Comments at 24-25.

[113] Motorola Solutions Comments at 30.

[114] Northrop Grumman Comments at 17.

[115] Telcordia Comments at 17.

user devices,[116] while 7Layers "confirms the Commission's proposal" to require such testing.[117] Cassidian expressed support for conformance testing as well and "recommends the Commission to refer to the applicable 3GPP TS documents for Radio and Protocol Conformance."[118] NTIA also supported the Commission's adoption of a conformance testing mandate, for both user devices and infrastructure equipment.[119]

Adams County, however, stated that "without established and understood testing processes it is too early to require and mandate [conformance testing] requirements."[120] NPSTC also found the proposed mandate premature and recommends deferring the adoption of conformance testing requirements until "decisions are made on the larger issues of architecture and governance."[121] Adams County and NV Energy also cautioned that conformance testing requirements could create significant costs for network operators,[122] while NPSTC contended that the adoption of its proposed network architecture "may allow this testing to be done in ways that reduce cost and duplication."[123]

The record showed that conformance testing was the best available means of verifying the conformance of public safety user devices to the LTE standard, an essential building block of nationwide interoperability. Conformance testing is already well established as a key driver of device interoperability in the commercial sector. As 7Layers explained, conformance testing "is considered by almost all global wireless operators as the minimum standard by which a user device may be considered as acceptable for network introduction."[124] We note that conformance testing of public safety LTE devices would closely approximate the testing already performed on a vast ecosystem of commercial wireless devices, which should create opportunities to leverage existing resources to reduce costs.[125] As 7Layers observed, the added cost of conformance testing for public safety broadband devices is modest and reflective of industry

---

[116] Aeroflex Comments at 3 (stating that "[a]ll mobile devices which connect to the public safety network will also be required to follow the same rigorous process as commercial devices").

[117] 7 Layers Comments at 5.

[118] Cassidian Comments at 28.

[119] NTIA Comments at 20; *see also* NYPD Comments at 24-25.

[120] Adams County Comments at 6.

[121] NPSTC Comments at 23.

[122] Adams County Comments at 6; NV Energy Comments at 6-7.

[123] NPSTC Comments at 23.

[124] *Id*. at 4; *see also* NSN Comments at 27 (stating that "device interoperability is based on industry wide principles and standards").

[125] *See, e.g*., IPWireless Comments at 29 ("As a supplier [Band Class 14] user equipment for public safety, IPWireless intends to have devices certified by the appropriate certification body, be it GCF or PTCRB, noting that both of these organizations approve [user devices] against the same test scenarios developed by 3GPP."); *see also* NSN Comments at 27 (stating that "device interoperability is based on industry wide principles and standards").

standards.[126]

As explained above, conformance testing ensures compliance with 3GPP open standards and is a widely accepted and cost effective commercial industry practice. While requiring conformance testing for public safety network equipment may impose a nominal cost, but we recognized that it ultimately would prevent non-conforming devices from entering the network and degrading network performance, which would diminish the value of the network. Specifically, we believed that requiring conformance testing would ensure a competitive market for devices that can be utilized on the nationwide interoperable public safety broadband network, which would result in substantially reduced costs to public safety and greater innovation than would occur in a less competitive marketplace.

Some commenters proposed that the Commission require conformance testing and certification for network elements other than user devices. For instance, Telcordia stated that "to support the goal of an interoperable public safety network every component of the network must be subject to a conformance certification process," and it was "imperative that the FCC create a certification requirement for LTE infrastructure equipment."[127] NTIA also supported a testing requirement for network infrastructure and noted that the "Multi-Service Forum is investigating the development of a framework" for infrastructure conformance testing.[128] IPWireless observed, on the other hand, that "there is no formal industry process equivalent to [user device] conformance testing for network infrastructure" and that requiring such testing at this time "would impose a huge cost burden on the industry, which would be borne by public safety."[129]

Although we recognized that conformance testing of LTE infrastructure equipment could serve as an important safeguard of network interoperability, we determined that a mandate for such testing would be premature. In the absence of an established commercial testing regime, we believe it is appropriate to take a cautious approach toward developing testing requirements for public safety LTE infrastructure equipment.

---

[126] *See* 7Layers Ex Parte Filing, PS Docket 06-229 (filed Dec. 20, 2011). 7Layers estimates that it will cost approximately $75,000 per device type to complete PTCRB LTE Band Class 14 conformance testing. *See id*. at 3. This represents a minimal cost per expected user of the public safety broadband network.

[127] Telcordia Comments at 18.

[128] NTIA Comments at 20; *see also* NYPD Comments.

[129] IPWireless Comments at 29.

Additional Issues

At the time of the FCC staff's assessment of the issues, there was an insufficient record on a number of other important areas, including how to enable open standards, additional security requirements as recommended in the PSAC Reports, and the use of a single PLMN ID for the network. These are issues that the FCC staff believe are critical to resolve in order to craft minimum technical requirements for interoperability for the nationwide public safety broadband network.