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

In the Matter of	)	
	)	
Amendment of Part 15 of the Commission's Rules for Unlicensed Operations in the Television Bands, Repurposed 600 MHz Band, 600 MHz Guard Bands and Duplex Gap, and Channel 37, and	)	ET Docket No. 14-165
	)	
Amendment of Part 74 of the Commission's Rules for Low Power Auxiliary Stations in the Repurposed 600 MHz Band and 600 MHz Duplex Gap	)	
	)	
Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions	)	GN Docket No. 12-268

REPLY COMMENTS OF GE HEALTHCARE

Neal Seidl
Matthew Pekarske
GE Healthcare
8200 W. Tower Avenue
Milwaukee, WI 53223

Ari Q. Fitzgerald
Tom Peters*
Tony Lin
Wesley B. Platt
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004

Counsel for GE Healthcare

February 25, 2015

* Not an attorney

Table of Contents

I. INTRODUCTION AND SUMMARY 1

II. THE GOAL OF PROMOTING THE MARKET FOR UNLICENSED DEVICES DOES NOT OUTWEIGH THE GOAL OF PROTECTING CRITICAL SAFETY-OF-LIFE WMTS OPERATIONS. 3

III. NO COMMENTERS PROVIDE VALID TECHNICAL SUPPORT FOR THE ADOPTION OF THE COMMISSION'S PROPOSED SEPARATION DISTANCES BETWEEN UNLICENSED TVWS DEVICES AND WMTS OPERATIONS. 4

A. There is no technical basis for establishing shorter separation distances between TVWS devices operating on Channel 37 and WMTS operations. 6

B. Broadcom's application of the WINNER+ Urban Micro model is flawed and fails to represent a realistic worst-case scenario, which is appropriate for calculating separation distances for a safety-of-life service. 7

IV. GEOLOCATION DATABASE SCHEMES ARE UNPROVEN AND CANNOT SERVE AS THE BASIS FOR CONCLUDING THAT WMTS OPERATIONS WILL BE PROTECTED FROM HARMFUL INTERFERENCE FROM PERSONAL-PORTABLE DEVICES OPERATING ON CHANNEL 37. 9

V. THE COMMENTS SUPPORT THE CONCLUSION THAT A MORE NUANCED INTERFERENCE MITIGATION APPROACH CAN HELP PREVENT HARMFUL INTERFERENCE TO WMTS OPERATIONS. 15

VI. IF THE COMMISSION ADOPTS A MODELED INTERFERENCE APPROACH FOR CALCULATING SEPARATION DISTANCES, IT SHOULD BASE SUCH DISTANCES ON THE MOST CONSERVATIVE PROPAGATION ASSUMPTIONS AND PROHIBIT UNLICENSED DEVICE USE ON CHANNEL 37 IN RURAL AREAS. 16

VII. CONCLUSION. 17

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

In the Matter of	)	
	)	
Amendment of Part 15 of the Commission's Rules for Unlicensed Operations in the Television Bands, Repurposed 600 MHz Band, 600 MHz Guard Bands and Duplex Gap, and Channel 37, and	)	ET Docket No. 14-165
	)	
Amendment of Part 74 of the Commission's Rules for Low Power Auxiliary Stations in the Repurposed 600 MHz Band and 600 MHz Duplex Gap	)	
	)	
Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions	)	GN Docket No. 12-268

REPLY COMMENTS OF GE HEALTHCARE

GE Healthcare ("GEHC")[1] hereby submits these reply comments in response to the comments submitted in the above-captioned proceeding.[2]

I. INTRODUCTION AND SUMMARY.

In its comments, GEHC emphasized the importance of the safety-of-life Wireless Medical Telemetry Service ("WMTS") and urged the Commission to protect such operations on Channel 37 from harmful interference in the event it allows co-channel, unlicensed television

[1] GEHC is a unit of General Electric Company and provides a broad range of products and services that enable healthcare providers to better diagnose and treat diseases and medical conditions, including products and services that incorporate wireless technology.

[2] *Amendment of Part 15 of the Commission's Rules for Unlicensed Operations in the Television Bands, Repurposed 600 MHz Band, 600 MHz Guard Bands and Duplex Gap, and Channel 37; Amendment of Part 74 of the Commission's Rules for Low Power Auxiliary Stations in the Repurposed 600 MHz Band and 600 MHz Duplex Gap; Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, Notice of Proposed Rulemaking, 29 FCC Rcd 12248 (2014) ("*Part 15 NPRM*").

whitespace ("TVWS") device operations.[3] GEHC demonstrated that the Commission's proposed technical rules for unlicensed Channel 37 operations, if adopted, would fail to do so. There are a number of material errors and other flaws in the Commission's reasoning underlying its proposed technical rules, including basic mathematical mistakes and inappropriate models and methodologies – all of which result in an understatement of the separation distances required to protect WMTS operations from harmful interference. GEHC also emphasized that, if the Commission permits unlicensed devices to operate on Channel 37 (after developing technical standards that do adequately protect WMTS), the Commission should limit such unlicensed use to fixed devices. It also pointed out that the Commission's proposed geolocation database scheme is completely unproven, and there are serious concerns about how to assure its dependability (including reliability and security), especially given its safety-critical nature. Unlike other radiocommunications services, where harmful interference could result, for example, in merely a temporary loss of television reception or a disconnected telephone call, here the consequences of harmful interference can be orders of magnitude more grave.

While a number of commenters support unlicensed use on Channel 37, none provide credible technical analyses demonstrating that unlicensed device operations, as proposed by the Commission, would protect WMTS operations, and none address the technical mistakes and problems in the Commission's *Part 15 NPRM* analysis identified by GEHC. Most of the commenters simply rely on the Commission's flawed technical analyses or the assumption that a geolocation database scheme, which GEHC has shown would be problematic for reliability and security reasons, would be sufficient to protect WMTS operations.

---

[3] *See* Comments of GE Healthcare (Feb. 4, 2015) ("GEHC Comments").

For these reasons, GEHC urges the Commission not to allow unlicensed operations in Channel 37 unless and until it develops both technical standards and the regulatory certification and enforcement regime necessary to fully protect WMTS operations from harmful interference and to prohibit, under any circumstances, the use of Channel 37 by unlicensed, personal-portable devices. GEHC also supports the comments submitted by the WMTS Coalition in this proceeding, including the WMTS Coalition's request that the Commission ensure that WMTS operators are reimbursed for all direct or indirect expenses reasonably incurred as a result of the resolution or mitigation of interference from the sharing of Channel 37 with unlicensed devices, and asks the Commission to take action consistent with that filing.[4]

II. THE GOAL OF PROMOTING THE MARKET FOR UNLICENSED DEVICES DOES NOT OUTWEIGH THE GOAL OF PROTECTING CRITICAL SAFETY-OF-LIFE WMTS OPERATIONS.

Nearly all commenters addressing Channel 37 in this proceeding acknowledge that WMTS operations provide important public service benefits and should be protected from harmful interference.[5] Indeed, as GEHC and the WMTS Coalition explain in their respective comments, wireless medical telemetry equipment is routinely used in hospitals and other healthcare facilities to monitor real-time patient data (such as electrocardiography, heart rate, and

---

[4] *See generally* Initial Comments of the WMTS Coalition (Feb. 4, 2015) ("WMTS Coalition Comments").

[5] *See, e.g.*, Comments of Broadcom Corporation at 3 (Feb. 4, 2015) ("Broadcom Comments") ("Broadcom commends the Commission for its decision to introduce broadband operations in portions of channel 37, <u>while preventing harmful interference to incumbents</u>.") (emphasis added); Comments of Dynamic Spectrum Alliance at 10 (Feb. 4, 2015) ("DSA Comments") ("The existing users — wireless telemetry and radio astronomy — both provide important services to the public."); Comments of Google Inc. at 19 (Feb. 4, 2015) ("Google Comments") ("Google therefore agrees with the Commission's goal of enabling unlicensed operations in channel 37 <u>as long as white space databases and devices protect incumbents from harmful interference</u>.") (emphasis added).

oxygen saturation data) and detect life-threatening events (*e.g.*, cardiac arrhythmias and apneas).[6] Thus, as a critical safety-of-life service, WMTS should not be subjected to even small or episodic incidents of interference. Accordingly, any technical standards adopted by the Commission for unlicensed Channel 37 operations should be conservative enough to cover all realistic worst-case scenarios, and not simply "typical" or "average" cases.[7]

Although some commenters assert that the market for unlicensed devices may benefit from liberal re-use of Channel 37, that goal should be secondary and factor into the Commission's analysis only if such use will not harm hospitals and their patients.[8] Protecting safety-of-life WMTS operations from harmful interference should be the Commission's top priority as it considers whether to allow unlicensed operations in Channel 37.

III. NO COMMENTERS PROVIDE VALID TECHNICAL SUPPORT FOR THE ADOPTION OF THE COMMISSION'S PROPOSED SEPARATION DISTANCES BETWEEN UNLICENSED TVWS DEVICES AND WMTS OPERATIONS.

As GEHC explained in its comments, the Commission appears to have used a combination of the TM 91-1 model and the F(50,50) FM and TV propagation curves as a basis for calculating proposed separation distances between TVWS devices and WMTS operations.[9] As GEHC explained in its comments, the use of either of these models is inappropriate for calculating separation distances in this instance.[10] For example, the TM 91-1 model is not valid for the assessment of coverage for transmitter heights in excess of 300 feet (or ~91 meters), but

---

[6] *See, e.g.*, GEHC Comments at 3; WMTS Coalition Comments at 7-9.

[7] *See, e.g.*, Broadcom Comments at 24 (proposing the use of average expected path loss).

[8] *See, e.g.*, Broadcom Comments at 21, 24-25; DSA Comments at 12; Google Comments at 18; Comments of Microsoft Corporation at 19 (Feb. 4, 2015) ("Microsoft Comments").

[9] *See* GEHC Comments at 5-24.

[10] *See* GEHC Comments at 14-17.

the Commission makes eight such calculations in the WMTS interference tables.[11] Similarly, the F(50,50) propagation curves, as well as the height above average terrain (or HAAT) measure, were developed for assessment of TV and radio coverage areas – high-site and high-power applications that are very different from unlicensed, low-power transmissions in virtually every respect.[12] None of the comments by supporters of unlicensed device use on Channel 37 addresses, much less rebuts, GEHC's analyses of the Commission's material errors and flaws in reasoning.

Moreover, a number of parties, including ones that support liberal use of unlicensed devices on Channel 37, agree that other propagations models, including the Longley-Rice methodology, would be more accurate and appropriate for calculating separation distances between TVWS devices and WMTS operations.[13] If the Commission were to adopt a modeled interference approach, GEHC agrees that for greater accuracy and to reduce the potential for harmful interference to WMTS operations, a free space loss or Longley-Rice model should be used to calculate separation distances.[14]

---

[11] *See* GEHC Comments at 15.

[12] *See* GEHC Comments at 17.

[13] *See, e.g.*, Comments of Adaptrum, Inc. at 9 (Feb. 4, 2015) ("Adaptrum Comments") ("There is no reason to prohibit the use of Longley-Rice by those data base providers who are willing to invest the resources to implement it."); DSA Comments at 4 ("The Commission should require TVWS geo-location databases to use terrain-based modeling, such as the Longley-Rice propagation methodology, to calculate required protection contours for broadcast operations."); Google Comments at 19 ("Rather than relying purely on assumptions and modeling, the Commission should alight its separation distances with real-world conditions."); Microsoft Comments at 19-20 ("Microsoft therefore proposes that the FCC make good on its offer to work with WMTS stakeholders to collect better data, and revisit the proposed zones for protection of WMTS and adjust them based on real-world interference protection needs."); Comments of Wi-Fi Alliance at pp. 30-31 (Feb. 4, 2015) ("Wi-Fi Alliance Comments") ("[T]he FCC should not rely on the TM 91-1 model.").

[14] *See* GEHC Comments at 18.

A. There is no technical basis for establishing shorter separation distances between TVWS devices operating on Channel 37 and WMTS operations.

For the same reasons as those stated above, the Commission should reject the arguments by a few of the commenters suggesting that the Commission's proposed separation distances are too conservative and overprotect WMTS operations.[15] Moreover, as GEHC explains in its comments, the TM 91-1 model, as well as the F(50,50) propagation curves, as a theoretical matter, generally yield the most path loss when compared to other commonly used models.[16] The chart below, which was provided in the GEHC Comments, shows that for most transmitter heights, the TM 91-1 model and the F(50,50) propagation curves predict more path loss than any of the other models, which means they are <u>the least conservative</u> in establishing separation distances.[17]

	Path Loss						
	Theoretical	Empirical Models giving MEDIAN path loss			10% Time Var	50% Time Var	
Tower height (m)	FSPL (2.0)	Hata (Suburban)	TM 91-1	Winner+ LOS	Longley Rice (ITM)	F(50,50)	
3	100.2	131.9	138.2	125.5	114.2	N/A	*Out of range for Hata*
10	100.2	122.6	127.8	116.5	103.9	N/A	*Out of range for Hata*
30	100.2	114.1	118.2	108.2	100.1	119.1	
50	100.2	110.2	113.8	104.4	100.2	114.6	
75	100.2	107.1	110.3	104.5	100.2	111.3	
100	100.2	104.9	107.8	104.5	100.2	108.9	*Out of range for TM91-1*
150	100.2	101.7	104.2	104.5	100.2	106.3	*Out of range for TM91-1*
200	100.2	99.5	101.7	104.5	100.2	104.7	*Out of range for TM91-1*
250	100.2	97.8	99.8	104.5	100.2	103.7	*Out of range for TM91-1, LR & Hata*

FSPL or Less

Additionally, GEHC's field tests confirm that in real-world conditions the TM 91-1 model consistently predicts path loss that is greater than measured path loss and, thus, yields

[15] Google Comments at 20-21; Microsoft Comments at 20; Comments of Motorola Solutions, Inc. at 10-11 (Feb. 4, 2015); Wi-Fi Alliance Comments at 30.

[16] Microsoft's claim that GEHC has in this proceeding incorrectly "assumed a 10 dB penalty to account for aggregation gain when multiple WMTS antennas receive interference from the same signal" should be disregarded. Microsoft Comments at 21. As explained in its comments, GEHC reduced the effect of DAS aggregation of a single interferer from 10 dB to 3 dB and has included the effect of this aggregation in its recommended field strength values. *See* GEHC Comments at 25 n. 67.

[17] *See* GEHC Comments at 19-20.

shorter separation distances than are necessary to protect WMTS operations from harmful interference from unlicensed, co-channel TVWS devices.[18] Accordingly, the interference analyses and related technical claims by commenters seeking shorter separation distances should be rejected.[19]

B. Broadcom's application of the WINNER+ Urban Micro model is flawed and fails to represent a realistic worst-case scenario, which is appropriate for calculating separation distances for a safety-of-life service.

Broadcom urges the Commission to adopt the WINNER+ Urban Micro Model for purposes of calculating separation distances between TVWS devices and WMTS operations.[20] Under that model, Broadcom asserts that "even under highly pessimistic assumptions, a separation distance of 65 meters would be adequate for TVWS devices operating in [C]hannel 37."[21] As GEHC has previously explained in this proceeding, Broadcom's modeling assumptions that hospitals are low-rise buildings located in a flat, cluttered urban environment are unrealistic and inappropriate for interference analyses designed to protect a safety-of-life service.[22] As the WMTS Coalition notes, hospitals are often among the tallest buildings in a local community, especially where the hospitals are located in rural areas, and are often

---

[18] *See* GEHC Comments at 25-27 and Appendix A.

[19] The primary justification by commenters for shorter separation distances is the failure of the TM 91-1 model to account adequately for a building penetration loss. *See* Broadcom Comments 23; *see also infra* Section III.B (rebutting the assumption that building penetration loss should be 20 dB).

[20] *See* Broadcom Comments at 22-25. Microsoft relies on the Broadcom conclusions but does not purport to independently verify or confirm Broadcom's analyses. *See* Microsoft Comments at 20-22.

[21] *See* Broadcom Comments at 21-22.

[22] *See* Letter from Ari Q. Fitzgerald, Counsel to GE Healthcare, to Marlene H. Dortch, Secretary, Federal Communications Commission (Mar. 7, 2014) ("GEHC Ex Parte Letter"). GEHC incorporates by reference its prior submission.

centralized facilities serving large dispersed populations.[23] Moreover, Broadcom continues to use in its analysis the WINNER+ mean path loss prediction and omit the fading variation that is a part of the WINNER+ model, resulting in an overstatement of path loss.[24]

There is also no reason to conclude, as Broadcom asserts, that TVWS signals in Channel 37 would be consistently subject to a building penetration loss of 20 dB and that non line-of-sight conditions could be relied upon.[25] Indeed, GEHC's field tests show that building penetration and clutter loss can vary widely at any specific site (ranging from 10 to 20 dB at the Inova Mount Vernon Hospital),[26] especially if WMTS receive antennas are located in patient rooms with windows or a hospital's exterior has significant elements of glass, which is often the case for more modern buildings.[27] Google's tests also show that a building penetration loss of 20 dB is unrealistic in many cases,[28] and the WINNER+ model endorsed by Broadcom suggests typical building loss of only 7 dB at 600 MHz.[29]

---

[23] *See* WMTS Coalition Comments at 15.

[24] *See* Broadcom Comments at 21-25; *see also* GEHC Ex Parte Letter at 4.

[25] *See, e.g.*, Broadcom Comments at 23.

[26] *See* GEHC Comments, Appendix A at 10.

[27] *See* WMTS Coalition Comments at 15 ("Newer hospitals typically have significant elements of glass in their exteriors, with WMTS antennas in most patient rooms in immediate sight of the glass windows.").

[28] *See* Google Comments at 4-5 (observing 13 dB building penetration loss in commercial office buildings with concrete walls and standard windows). Google claims that its findings support shorter separation distances. *See id*. However, Google incorrectly assumes that "the Commission's analysis did not account for any building penetration loss." *Id.* at 4. In fact, building penetration loss had already been factored into GEHC's proposed field strength limit, which the FCC's *Part 15 NPRM* analysis used. *See Part 15 NPRM* at ¶ 110; Petition for Reconsideration of GE Healthcare, GN Docket No. 12-268, at 10-11 (filed Sept. 15, 2014) ("GEHC Petition for Reconsideration").

[29] *See* Celtic Telecommunications Solutions, *D5.3: WINNER+ Final Channel Models* at 61 (2010), *available at* http://bit.ly/1DbyUq3 ("Building penetration values are suggested in [Rudd-03]. *Mean values of the perpendicular loss are 9.2 dB at 1.3 GHz***,** 11.2 dB at 2.4 GHz, and 12.7

IV. GEOLOCATION DATABASE SCHEMES ARE UNPROVEN AND CANNOT SERVE AS THE BASIS FOR CONCLUDING THAT WMTS OPERATIONS WILL BE PROTECTED FROM HARMFUL INTERFERENCE FROM PERSONAL-PORTABLE DEVICES OPERATING ON CHANNEL 37.

Aside from, but equally important as, determining separation distances sufficient to protect WMTS operations are the serious questions regarding the *dependability* (including *reliability* and *security*)[30] of the Commission's proposed geolocation database scheme. No separation distance – no matter how large – will be effective unless dependably enforced. Some commenters simply take it for granted that this yet-to-be-designed technology will work flawlessly.[31] However, as GEHC has explained, this is unlikely to be the case.

The Commission has limited experience with the use of geolocation database technology for unlicensed fixed devices and *no experience whatsoever* with respect to using such technology for personal-portable devices. The envisioned geolocation database scheme entails a massive and complex, autonomous real-time distributed *system* (hereinafter referred to as the Whitespace Spectral Access System ("WSAS")). Furthermore, because under the Commission's proposed rules the continued interference-free operation of thousands of safety-of-life WMTS systems

---

dB at 5.7 GHz. From this we can deduce that the penetration loss increases 1.8 dB per octave between 1.3 and 5.7 GHz. *We assume that this can be extrapolated down to 450 MHz*.") (emphasis added).

[30] "Dependability" refers to system properties like reliability and security that allow a system to be relied on to function as required. *See, e.g.*, Bev Littlewood and Lorenzo Strigini, *Software Reliability and Dependability: a Roadmap*, In Proceedings of the Conference on the Future of Software Engineering (2000), *available at* http://bit.ly/1MPOoYP; "Reliability" is the probability of failure-free software operation for a specified period of time in a specified environment, and software is "secure" if it continues to function correctly under malicious attack. *See, e.g.*, Aasia Quyoum et al., *Improving Software Reliability Using Software Engineering Approach – A Review*, INT. J. OF COMP. APPLICATIONS, NOV. 2010, *available at* http://bit.ly/1wmqW0z; Gary McGraw, Software Security, IEEE SECURITY & PRIVACY (2004), *available at* http://bit.ly/1LBeknx/.

[31] *See, e.g.*, Adaptrum Comments at 5-6; Broadcom Comments at 21, 25; DSA Comments at 10-12; Google Comments at 31-32.

would depend on the reliable and secure operation of the WSAS, that system would itself become a safety-critical system. However, as envisioned, the WSAS would be comprised of potentially millions of disparate constituent devices, most of which would be of low-cost, consumer-grade design and construction, the antithesis of dependability.

Of particular concern to GEHC is the fact that the critical WSAS functionality (*e.g.*, geo-positioning, database interface, radio control and security functions) residing in these devices would be software-based, undoubtedly including many open-source and commercial off-the-shelf software components. The FCC's existing device certification regime, which is essentially limited to black-box type testing and manufacturer attestation regarding the technical specifications of the device, is inadequate to ensure the reliable and secure operation of critical WSAS functionality embodied in the whitespace device software.[32] Indeed, the Commission has acknowledged the security challenges presented by the use of software defined radios.[33] But, it has relied mainly on voluntary industry efforts to protect the security of such devices and implemented only limited security requirements,[34] which would not be sufficiently robust for devices that impact safety-of-life WMTS operations. And, apart from this cursory treatment of

---

[32] This is in sharp contrast to equipment authorizations not involving software defined radios, where compliance with spectrum rules are simply and reliably implemented by fixed-frequency hardware filters.

[33] *See, e.g., Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies; Authorization and Use of Software Defined Radios,* Notice of Proposed Rule Making and Order, 18 FCC Rcd 26859 ¶ 84 (2003) ("[W]e are concerned about the potential for parties to make unauthorized changes to software programmable radios after they are manufactured and first sold which could result in harmful interference to authorized services").

[34] *Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies; Authorization and Use of Software Defined Radios,* Report and Order, 20 FCC Rcd 5486 ¶¶ 54-61 (2005) (requiring manufacturers to take steps to ensure that only software that has been approved with a software defined radio can be loaded into the radio); *see also* 47 C.F.R. § 2.944.

security, the FCC has never explicitly considered the separate but equally critical aspect of dependability – reliability – despite GEHC having raised it on numerous occasions.[35]

As explained below, software cannot be assumed to be dependable in the absence of rigorous quality assurance measures. To the contrary, everyday experience with consumer software applications and operating systems tells a different story. As computers and embedded microprocessors become more powerful, pervasive, and inter-connected, the software they run becomes more complex and capable. At the same time, that software inevitably becomes less dependable due to additional vulnerabilities and opportunities for failure. Among the failures all too familiar to users of these devices are crashes, hangs, lost or corrupted data and incorrect output / behavior. And a seemingly endless stream of security patches has become an unfortunate way of life for users of all major operating systems and applications.[36] For example, a search of the Department of Homeland Security's United States Computer Emergency Readiness Team ("US-CERT") National Vulnerability Database regarding Google Android returns 338 distinct vulnerabilities discovered between 2009 and 2014.[37] Similarly, a search regarding Apple's iPhone Operating System ("iOS") returns 429 vulnerabilities discovered

---

[35] *See, e.g.*, Letter from Ari Q. Fitzgerald, Counsel, GE Healthcare, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 12-268, at 1-3 (filed Ap. 21, 2014); GEHC Petition for Reconsideration at 9-10.

[36] *See, e.g.*, Microsoft's Patch Tuesday Turns 10: A Decade of Botched Updates and Broken PCs, http://bit.ly/1DP3eft (last visited Feb. 24, 2015); Ultimate Windows Security, Patch Tuesday Observer Archive, http://bit.ly/1D8fNNy (last visited Feb. 24, 2015); GFI Blog, Report: Most Vulnerable Operating Systems and Applications in 2013, http://bit.ly/1ErXur4 (last visited Feb. 24, 215); John Viega, *Open Source Security: Still a Myth*, ONLAMP.COM (Sep. 16, 2004), http://bit.ly/1LID0fW.

[37] *See* National Institute of Standards and Technology, National Vulnerability Database, https://web.nvd.nist.gov/view/vuln/statistics (last visited Feb. 24, 2015).

between 2009 and 2014.[38] In fact, even the BlackPhone, which had been billed as "the world's first Smartphone which places privacy and control directly in the hands of its users," was found to suffer from a critical vulnerability that let hackers compromise it in less than five minutes.[39] And these are just the software defects that happened to manifest as security vulnerabilities. Similar statistics are not readily available regarding software defects that impact reliability rather than security, but there is no reason to believe that such defects are any less prevalent. Although users of consumer devices and applications generally tolerate these inconveniences because they are typically outweighed by the benefits provided and because they have no better alternative, such instability and poor dependability is completely unacceptable for safety-critical systems.

Assuring the quality and dependability (including both security and reliability) of safety-critical and other "high consequence" devices and systems – especially those involving software – is extremely challenging and requires application of rigorous quality controls throughout the product lifecycle (including in design, supply chain, manufacturing, installation, service, post-market surveillance and field corrections). For example, when adopting a more comprehensive Quality System Regulation (including preproduction Design Controls) in 1996, the Food and Drug Administration ("FDA") recognized that its original regulations "provided less than an adequate level of assurance that devices would be safe and effective" because "[t]he intrinsic quality of devices, including their safety and effectiveness, is established during the design

[38] *See id*.

[39] *See* Wang Wei, *NSA-Proof "Blackphone" Gets Rooted Within 5 Minutes*, THE HACKER NEWS (Aug. 11, 215), http://bit.ly/1pmZREx; Eduard Kovacs, *Researchers Uncover Security Vulnerabilities in Ultra-Private Blackphone*, SECURITY WEEK (Aug. 11, 2014), http://bit.ly/1MPNnQv.

phase."[40] Although dated, the FDA's original regulations still greatly surpass the quality assurance standards in the Commission's current equipment authorization rules.[41] This tenet is nearly universally recognized by medical device regulators worldwide through the adoption of similar regulations and harmonized standards.[42] Similar regulations and standards also exist for safety-critical devices in other industries, including transportation, aviation, and energy.[43]

In practice, software cannot be proven correct through testing. Practical (non-exhaustive) testing can only hope to show the presence of defects, but the absence of test failures cannot prove the absence of defects. It is generally not possible to assure sufficient dependability of high consequence systems or software through testing alone – even with test protocols that are orders of magnitude more extensive than the limited functional and security checks currently imposed under the FCC's equipment certification tests.[44] Because software quality control is recognized as a significant challenge, the FDA and other regulators expect device manufacturers

---

[40] Food and Drug Administration, *Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule; Quality System Regulation*, 61 Fed. Reg. 52602, 52615-16 (1996).

[41] *See id*.

[42] *See, e.g.*, International Organization for Standardization, ISO 13485, Medical devices — Quality management systems — Requirements for regulatory purposes (2003), *available at* http://bit.ly/1FqLynu (setting out an international standard designed to facilitate harmonized medical device regulatory requirements for quality management systems).

[43] *See, e.g.*, International Organization for Standardization, ISO 03.220.20, Road Transport, *available at* http://bit.ly/1FVV5Xx (setting out international standards for road transportation systems such as road traffic safety management systems and traffic impediment warning systems).

[44] *See supra* nn. 32-33 and accompanying text; *see also, e.g*. David L. Parnas, A. John van Schouwen, and Shu Po Kwan, *Evaluation of Safety-Critical Software*, 33 Communications of the ACM, 636-658 (1990), *available at* http://bit.ly/1Es3Ab4; Bev Littlewood and Lorenzo Strigini, *Software Reliability and Dependability: a Roadmap*, In Proceedings of the Conference on the Future of Software Engineering, 175-188 (2000), *available at* http://bit.ly/1Es3EHI; Lynnette I. Millet, Martyn Thomas, and Daniel Jackson, eds., Software for Dependable Systems: Sufficient Evidence?, National Academies Press (2007).

to apply even more rigorous practices throughout the software lifecycle by conforming to prescriptive, risk-based process standards, such as IEC 62304, an internationally accepted standard for life cycle processes with activities and tasks necessary for the safe design and maintenance of medical device software.[45] Similar regulations and standards also exist for safety-critical software in other industries, including aviation[46] and energy.[47]

Despite the benefit of all of the quality assurance mechanisms prescribed by the FDA, defects still do go undetected until after commercialization. Software defects, in particular, are a leading cause of medical device recalls.[48] As a result, regulatory requirements for device traceability and mandatory device recalls are also critical components to protecting the public. However, these key quality system elements are notably absent from the Commission's proposed scheme for regulating ubiquitously deployed, unlicensed consumer devices.

Accordingly, if the FCC were to use an autonomous WSAS to control unlicensed devices sharing spectrum with WMTS, it would need to adopt a rigorous quality assurance regulatory

---

[45] *See* International Electrotechnical Commission, IEC 62304, *Medical Device Software — Software Life Cycle Processes* (2006) (summarizing the standard), *available at* http://bit.ly/1Es3Er8. *See also* Food and Drug Administration, *Modernizations to the List of Recognized Standards*, 77 Fed. Reg. 50118 (2012).

[46] *See, e.g.* Radio Technical Commission for Aeronautics, DO-178C, Software Considerations in Airborne Systems and Equipment Certification (2012). Recent Federal Aviation Administration ("FAA") releases recognize DO-178C. *See, e.g.*, FAA, Order 8110.49, *Software Approval Guidelines* (last rev. 2011), *available at* http://1.usa.gov/1zJfbwY; FAA, Advisory Circular 20-115C, *Airborne Software Assurance* (2013), *available at* http://1.usa.gov/1LFfBdb.

[47] *See, e.g.*, Institute of Electrical Engineers, IEEE Std 7-4.3.2-2003, Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (2003); U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152, *Criteria for use of Computers in Safety Systems of Nuclear Power Plants*, at 2 (2011) (recognizing IEEE Std 7-4.3.2-2003), *available at* http://1.usa.gov/1al46MB.

[48] *See, e.g.*, FDA, Medical Device Recall Report FY2003 to FY2012, *available at* http://1.usa.gov/1j69ymm (last visited Feb. 25, 2015).

system, similar to those adopted for medical devices and other safety-critical systems, spanning the entire lifecycle of the TVWS devices.

V. THE COMMENTS SUPPORT THE CONCLUSION THAT A MORE NUANCED INTERFERENCE MITIGATION APPROACH CAN HELP PREVENT HARMFUL INTERFERENCE TO WMTS OPERATIONS.

A number of commenters, including GEHC, suggest that the Commission consider a more nuanced approach to interference mitigation, which would take into account surrounding terrain and other factors specific to each WMTS site.[49] GEHC would support an interference mitigation approach that considers site-specific propagation conditions (including terrain and building features), provided it is based on whitespace device locations and WMTS deployments in three dimensions and uses realistic site-specific interference calculations.[50] As GEHC and others have noted, the Commission has taken similar approaches on other occasions.[51]

A more nuanced interference mitigation approach should apply only where an entity can demonstrate that the actual characteristics of the WMTS facility make it possible to deviate from the default separation distance. That default separation distance should be conservatively based

---

[49] *See* GEHC Comments at 27-28; Google Comments at 19 ("Rather than relying purely on assumptions and modeling, the Commission should alight its separation distances with real-world conditions."); Microsoft Comments at 19-20 ("Microsoft therefore proposes that the FCC make good on its offer to work with WMTS stakeholders to collect better data, and revisit the proposed zones for protection of WMTS and adjust them based on real-world interference protection needs.").

[50] Because propagation conditions will depend on the vertical position of unlicensed devices, as well as the horizontal position, the protection contour with respect to a WMTS site must be modeled as a two-dimensional surface in three dimensions. Additionally, as GEHC explained, WMTS facilities cannot be simply be assumed to be 10 meters above-ground-level. *See* GEHC Comments at 21.

[51] *See, e.g., Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, Second Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 13071 ¶¶ 39, 41, 50 (2014); *In the Matter of Amendment of the Commission's Rules to Provide Spectrum for the Operation of Medical Body Area Networks*, Order on Reconsideration and Second Report and Order, 29 FCC Rcd 10662 ¶ 41 (2014).

on free-space calculations to ensure that safety-of-life WMTS operations do not experience harmful interference. Moreover, as discussed by the WMTS Coalition, any expenses incurred as part of this process by WMTS operators or a WMTS coordinator should be reimbursable.[52]

VI. IF THE COMMISSION ADOPTS A MODELED INTERFERENCE APPROACH FOR CALCULATING SEPARATION DISTANCES, IT SHOULD BASE SUCH DISTANCES ON THE MOST CONSERVATIVE PROPAGATION ASSUMPTIONS AND PROHIBIT UNLICENSED DEVICE USE ON CHANNEL 37 IN RURAL AREAS.

GEHC agrees with the National Academy Sciences' Committee on Radio Frequencies ("CORF") that there is no need for unlicensed devices to operate on Channel 37 in rural areas, where TVWS spectrum is likely to be abundant.[53] Use of unlicensed devices on Channel 37 in rural and suburban areas is also more problematic because there is a greater chance of a line-of-sight transmission to a WMTS receive antenna. For example, test site 4 in GEHC's field study, which was a partially obstructed transmitter site, caused interference to WMTS receivers even when transmitting at 9 dB below FCC-proposed TVWS transmission levels.[54]

Accordingly, if the Commission adopts a modeled interference approach for calculating separation distances, GEHC supports CORF's proposal to prohibit TVWS use on Channel 37 in rural areas, defined as any area where more than 10% of the TV channels are unused for broadcast services and available for use by TVWS devices.[55] Moreover, GEHC urges the Commission to adopt such a prohibition in any area (rural, suburban or otherwise), where the

---

[52] *See* WMTS Coalition Comments at 23-25.

[53] *See* Comments of the National Academy of Sciences' Committee on Radio Frequencies at 6-7 (Feb. 4, 2015).

[54] *See* GEHC Comments, Appendix B at 68 and Appendix A at 12.

[55] *Id*. at 6.

same channel availability condition is met in light of the safety-of-life nature of WMTS operations.

VII. CONCLUSION.

The technical standards proposed in the NPRM, if adopted, would fail to protect WMTS operations on Channel 37. There are numerous material errors and flaws in the Commission's derivation of those proposed standards, including basic mathematical mistakes and inappropriate models and methodologies. GEHC's recent field tests confirm these conclusions. If the Commission permits unlicensed devices to operate on Channel 37 (after developing technical standards and quality assurance regulations that do adequately protect WMTS), it should limit such operations to fixed devices. Given the potentially ubiquitous nature of unlicensed, personal-portable devices and the serious concerns regarding the dependability of a geolocation database scheme (upon which the protection of WMTS operations is premised), the risk of life-threatening harmful interference in hospitals is simply too great to justify allowing the operation of unlicensed, personal portable devices.

Respectfully submitted,

By: */s/ Ari Q. Fitzgerald*

Neal Seidl
Matthew Pekarske
GE Healthcare
8200 W. Tower Avenue
Milwaukee, WI 53223

Ari Q. Fitzgerald
Tom Peters*
Tony Lin
Wesley B. Platt
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004
Phone: (202) 637-5663

Counsel to GE Healthcare

February 25, 2015

* Not an attorney