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

In the Matter of	)	
	)	ET Docket No. 16-56
Amendment of Part 15 of the Commission's	)	
Rules for Unlicensed White Space Devices	)	RM-11745

COMMENTS OF GE HEALTHCARE

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

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

Counsel to GE Healthcare

May 6, 2016

TABLE OF CONTENTS

Page

I. INTRODUCTION AND SUMMARY. ..... - 3 -

II. THE FCC MUST ENSURE THE DEPENDABILITY OF THE SOFTWARE UPON WHICH WHITE SPACE DEVICES AND THE DATABASE ITSELF WILL RELY. ..... - 5 -

III. PRE-MARKET DESIGN CONTROL REQUIREMENTS AND PROCEDURES FOR NON-COMPLIANT DEVICES WOULD HELP ENSURE THAT WHITE SPACE DEVICE SOFTWARE OPERATES AS INTENDED. ..... - 9 -

IV. THE COMMISSION'S DEVICE CERTIFICATION PROCESS CAN HELP ENSURE THAT WHITE SPACE DEVICES OPERATE AS INTENDED. ..... - 10 -

V. THE ROBUST ENFORCEMENT OF THE FCC'S DEVICE SECURITY RULES WOULD HELP PROTECT THE INTEGRITY OF THE DATABASE SYSTEM. ..... - 11 -

VI. THE COMMISSION SHOULD ALSO BOLSTER WSAS FUNCTIONALITY TO ENSURE THAT LICENSED USERS CAN RELY ON ITS RELIABLE AND SECURE OPERATION. ..... - 12 -

VII. CONCLUSION. ..... - 14 -

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

In the Matter of	)	
	)	ET Docket No. 16-56
Amendment of Part 15 of the Commission's	)	
Rules for Unlicensed White Space Devices	)	RM-11745

COMMENTS OF GE HEALTHCARE

GE Healthcare ("GEHC")[1] hereby submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Notice of Proposed Rulemaking ("NPRM") and Order in the above-captioned proceeding.[2]

I. INTRODUCTION AND SUMMARY.

Although there would be some benefits to implementing the proposed changes to the Commission's Part 15 rules, none of these reforms address the most critical weaknesses that threaten to undermine the overall integrity of the white space geolocation/database system. To ensure that the geolocation/database scheme fully protects licensees and other authorized users, the Commission should also adopt safeguards to ensure that the software upon which this scheme depends – in particular that which will reside within TVWS devices – will consistently operate as intended.[3]

---

[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 White Space Devices*, Notice of Proposed Rulemaking and Order, 31 FCC Rcd 1657 (2016).

[3] *See* Petition for Reconsideration of GE Healthcare, ET Docket No. 14-165, GN Docket No. 12-268, at 39 (filed Dec. 23, 2015) ("GEHC Petition for Reconsideration") ("The Commission should ensure the

As explained below, the Commission should take a number of measures to help ensure the dependability of this critical software. First, the Commission should introduce an increased level of rigor with regard to software into its device certification process and robustly enforce its device security rules. Second, the Commission should adopt pre-market design control requirements and procedures for dealing with non-compliant white space devices. Third, the Commission should bolster the functionality of the geolocation/database system to ensure that licensed users can rely on its dependable and secure operation.

The Commission has moved in this direction in other contexts. For example, in 2014, it required U-NII device manufacturers to implement security features so that third parties are not able to reprogram a device to operate outside the parameters for which the device was certified.[4] The Commission also indicated that it intended to "enforce [these] security protocol requirement carefully and vigorously."[5] In the case of the geolocation/database scheme and the millions of devices that will eventually depend upon it,[6] the risk of harmful interference is great enough to go somewhat further by introducing a stricter certification process and setting specific security requirements.

---

scope of any NPRM related to the white space databases also encompasses other dependability concerns, including reliability.").

[4] *See Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, First Report and Order, 29 FCC Rcd 4127 ¶¶ 47-57 (2014) ("*2014 U-NII Order*"); 47 C.F.R. § 15.407(i). The Commission had previously placed conditions on U-NII device certifications and initiated more than 40 enforcement actions when such devices were found to be causing harmful interference to the Terminal Doppler Weather Radar despite FCC rules that required the devices to incorporate dynamic frequency selection ("DFS") as an interference mitigation technique. *See 2014 U-NII Order* ¶¶ 11-14; FCC, *U-NII and TDWR Interference Enforcement*, https://www.fcc.gov/general/u-nii-and-tdwr-interference-enforcement (last visited May 5, 2016).

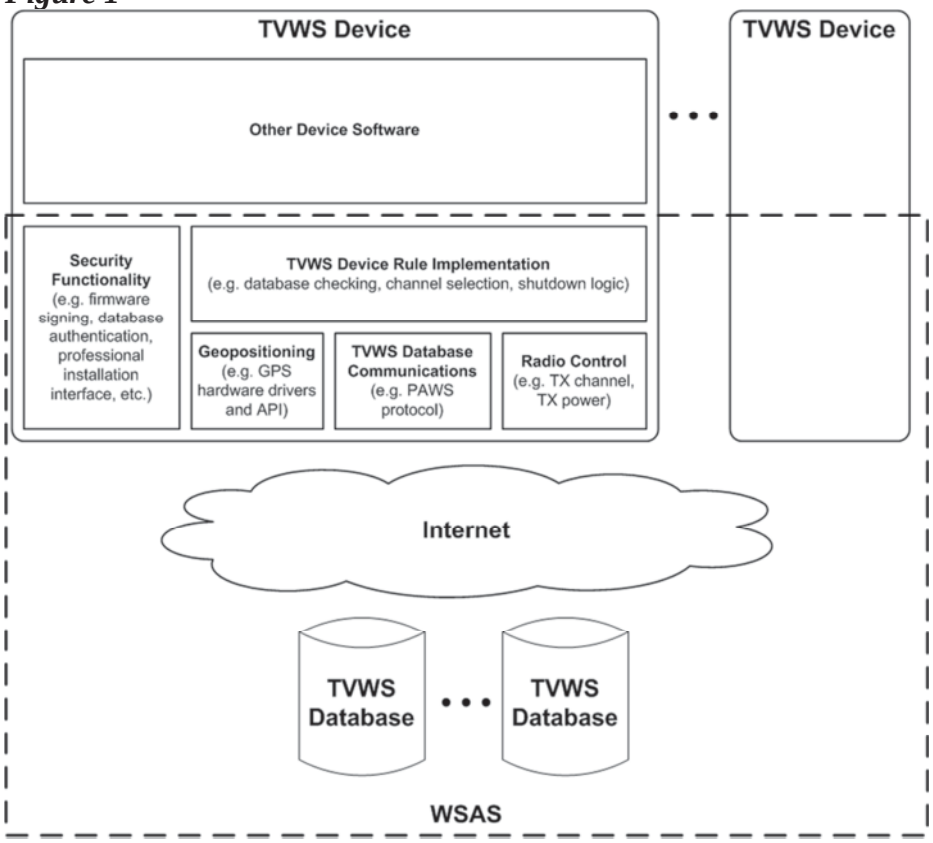
[5] *2014 U-NII Order* ¶ 57.

[6] *See, e.g.*, Opposition of Google, Inc., ET Docket No. 14-165, GN Docket No. 12-268, at 18 (filed Feb. 29, 2016)..

II. THE FCC MUST ENSURE THE DEPENDABILITY OF THE SOFTWARE UPON WHICH WHITE SPACE DEVICES AND THE DATABASE ITSELF WILL RELY.

As GEHC has previously explained,[7] the Commission's white space database regime entails a massive and complex, autonomous real-time distributed system (hereinafter referred to as the Whitespace Spectral Access System ("WSAS"))[8] as depicted below in Figure 1.

Figure 1



Yet the dependability[9] of the WSAS remains a key issue.[10] Of particular concern is the fact that much of the most critical WSAS functionality (*e.g.*, geopositioning, database interface,

---

[7] *See, e.g.*, GEHC Petition for Reconsideration at 36-39.

[8] The WSAS should not to be confused with the separate Spectrum Access System ("SAS") at issue in the 3.5 GHz proceeding.

[9] *Dependability* includes both *Reliability* (the ability of a system to function correctly for a specified period of time under expected usage conditions) and *Security* (the ability to continue to function correctly under malicious attack).

radio control, and security functions) will reside not in sophisticated centralized database software (which may be carefully developed, rigorously validated, and, when necessary, disabled or patched) but rather will reside in disparate white space *device* software, including almost certainly many open-source and commercial off-the-shelf software components.[11] Failures in device-resident WSAS software could cause these devices to: (1) report incorrect information (*e.g*. location, height, transmit power, device ID, or software revision) to the whitespace database, which in turn could result in inappropriate authorization from the database and ultimately harmful interference; or (2) fail to respond or respond inappropriately to instructions from the database resulting in unauthorized operations and, again, harmful interference. As explained below, in the absence of rigorous software quality assurance measures, **such software failures are inevitable** due to exploited security vulnerabilities and, even in the absence of manipulation or attack, simply due to spontaneous malfunctions caused by latent software design defects ("bugs") that escape detection in device software development and equipment certification.

It is well established that 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

---

[10] *See, e.g*., Comments of GE Healthcare, ET Docket No. 14-165, GN Docket No. 12-268, at 28 (filed. Feb. 4, 2015); Reply Comments of GE Healthcare, ET Docket No. 14-165, GN Docket No. 12-268, at 2, 9-14, (filed Feb. 25, 2015), Letter from Ari Q. Fitzgerald, Counsel, GEHC, *et al*., to Marlene H. Dortch, Secretary, FCC, ET Docket No. 14-165, GN Docket No. 12-268 (filed July 31, 2015); GEHC Petition for Reconsideration at 36-43.

[11] *See* GEHC Reply Comments at 9-10.

too familiar to users of these devices are crashes, hangs, lost or corrupted data and incorrect output / behavior. And a seemingly endless stream of bug and security patches has become an unfortunate way of life for users of all major operating systems and applications.[12] Because most white space devices are likely to be low-cost, consumer-grade, and often based on open-source software, they can be expected to be susceptible to manipulation by unauthorized third parties or device owners. As evidenced by seemingly daily news stories, the risk that hackers will be able to tamper with these devices is high.[13] And among the most likely to perform such hacking are device owners themselves, who could be motivated to exploit devices' software vulnerabilities to enable them to operate in ways their manufacturers never intended and to circumvent the FCC's rules. For example, "jailbreaking" has become a ubiquitous practice by which individuals modify the security controls on certain smartphones to install their own modifications to the device software that are otherwise not allowed by the operating system.[14]

Although the FCC has recognized such concerns as they relate to software defined radios,[15] it has failed to adequately address them as they relate to white space devices and the

---

[12] *See, e.g.*, Bogdan Popa, Microsoft's Patch Tuesday Turns 10: A Decade of Botched Updates and Broken PCs, Softpedia (Oct. 4, 2013), http://bit.ly/1DP3eft; Ultimate Windows Security, *Patch Tuesday Observer Archive*, http://bit.ly/1D8fNNy (last visited May 6, 2016); Christian Florian, *Report: Most Vulnerable Operating Systems and Applications in 2013*, GFI (Feb. 3, 2014), http://bit.ly/1ErXur4 (last visited May 6, 2016); John Viega, *Open Source Security: Still a Myth*, ONLAMP.COM (Sep. 16, 2004), http://bit.ly/1LID0fW.

[13] *See, e.g.*, Paul Mah, *The WiFi Pineapple Makes It Easy to Hack Wireless Devices*, FIERCE CIO (Aug. 6, 2013), http://www.fiercecio.com/techwatch/story/wifi-pineapple-makes-it-easy-hack-wireless-devices/2013-08-06; Chris Price, *Mobile Revolution: Never Underestimate the Hackers*, THE TELEGRAPH (Jan. 6, 2015), http://www.telegraph.co.uk/sponsored/technology/4g-mobile/data-security/11325780/mobile-devices-hackers.html.

[14] *See, e.g.*, Thorin Klosowski, *How to Jailbreak your iPhone: The Always Up-to-Date Guide [iOS 9]*, LIFEHACKER.COM (Oct. 14, 2015), http://lifehacker.com/5771943/how-to-jailbreak-your-iphone-the-always-up-to-date-guide-ios-61.

[15] *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

related databases. Instead, the FCC has vaguely required that white space devices "incorporate adequate security measures" and that the white space database "employ protocols and procedures to ensure that all communications . . . are accurate and secure."[16] The FCC also recently observed in a footnote[17] that it believes that these rules are "adequate to ensure security of the white space access systems" without addressing any of the specific concerns that GEHC raised last year or acknowledging that its certification procedures had already failed to prevent devices that violate these rules[18] from reaching the market and corrupting the integrity of registration information in the databases, as further discussed in section IV below.

Additionally, the Commission must remain mindful that the WSAS has itself become a safety-critical system under its recently-adopted rules because the continued interference-free operation of thousands of safety-of-life WMTS systems will depend on its reliable and secure operation. Specifically the Commission is relying upon the WSAS not only to prevent interference but also to be an essential tool for remediation of any interference events that do occur. Therefore, in order to dependably prevent unauthorized white space device operations, the Commission should take steps to assure the ***end-to-end* reliability and security of the *entire* WSAS** (including not only the centralized databases but also the WSAS

---

approved with a software defined radio can be loaded into the radio); *see also* 47 C.F.R. § 2.944; GEHC Reply Comments at 10.

[16] *See* 47 C.F.R. §§ 15.709(f), 15.711(j), 15.713(a), 15.713(l).

[17] *See 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*, Report and Order, ET Docket No. 14-165, GN Docket No. 12-268, 30 FCC Rcd 9551 ¶ 195 n.490; *see also id*. ¶ 196 n.495.

[18] These FCC-certified devices failed to secure professional installation features, thus violating Section 15.709(f) of the FCC's rules, which requires white space devices to "incorporate adequate security measures . . . to ensure that unauthorized parties cannot modify the device ***or configure control features*** to operate in a manner inconsistent with the rules and protection criteria set forth in this subpart." 47 C.F.R. § 15.709(f) (emphasis added). Previously, this requirement was set forth in Section 15.709(a)(6) of the FCC's rules.

functionality residing within TVWS devices), which the Commission is depending upon to implement and enforce its mandated separation distances and other operational rules.

III. PRE-MARKET DESIGN CONTROL REQUIREMENTS AND PROCEDURES FOR NON-COMPLIANT DEVICES WOULD HELP ENSURE THAT WHITE SPACE DEVICE SOFTWARE OPERATES AS INTENDED.

The Commission should take a number of measures to help ensure that white space device software operates as intended. For example, the Commission should establish pre-market design control requirements, including software quality assurance and life cycle processes,[19] for white space device manufacturers and procedures (*e.g.*, audits) to ensure that manufacturers comply with design control requirements.[20] It is widely recognized that the intrinsic quality and dependability of software is established during the development phase of if its life cycle and cannot be sufficiently assured through black-box certification testing alone.[21] In addition, the Commission should establish procedures to identify, locate, recall, correct, or disable white space devices that are found to be non-compliant after they have been certified and placed on the market including measures for dealing with devices that, due bugs or vulnerabilities in device-resident WSAS software, cannot be disabled remotely via the centralized databases.[22]

---

[19] The Commission could simply recognize or adopt the IEC 61508 series of standards including, in particular, IEC 61508-3, which establishes requirements for lifecycle phases and activities to be applied during the design and development of safety-related software.

[20] If the Commission recognizes or adopts IEC 61508 it could then simply recognize certifications to that standard provided to white space device manufacturers by accredited third parties.

[21] *See* GEHC Reply Comments at 12-14

[22] The Commission and its bureaus have suggested on a number of occasions that the FCC has the ability to order a product recall. *See, e.g.*, *Proposals for New or Revised Classes of Interstate and Foreign Message Toll Telephone Service (MTS) and Wide Area Telephone Service (WATS)*, Memorandum Opinion and Order, 57 FCC 2d 1216 ¶ 10 (1976) (listing recall as one of the "corrective actions" available to the FCC); *Pace Micro Technology PLC Petition for Special and Interim Relief*, Order, 19 FCC Rcd 1945 ¶ 8 (MB 2004) (declining to recall certain set-top boxes due to the burden it would impose on the manufacturer and consumers); *Spectrum Bridge, Inc. and Meld Technologies, Inc. Request for Waiver of Sections 15.711(b)(2) and 15.711(b)(3)(ii) of the Rules*, Order, 28 FCC Rcd 13159 ¶ 18 (OET 2013) (declining a request to recall certain white space devices no because it lacked the authority, but because it

IV. THE COMMISSION'S DEVICE CERTIFICATION PROCESS CAN HELP ENSURE THAT WHITE SPACE DEVICES OPERATE AS INTENDED.

An increased level of rigor with respect to software during the certification process is warranted to assure that white space devices consistently meet critical WSAS functional requirements in the Commission's rules. In particular, Commission should update its white space device certification procedures to require applicants to provide attestations as to the following:

- The geopositioning technology employed by the device, including its reliability, security, and accuracy;
- The method used to secure all embedded software involved in WSAS functionality against unauthorized modification and to maintain and update all software security and authentication methods in response to any changes in the FCC's certification, security, or authentication standards and other industry standards;
- The method used to secure all memory-resident device parameters (whether intended to be dynamic, configurable or static) upon which proper WSAS functionality depends (*e.g*., geolocation coordinates, transmit power, database polling intervals, device ID, software revision, etc.) against unauthorized modification; and
- A description of the software quality assurance and life cycle processes employed by the device manufacturer in the development, validation and maintenance of all embedded software involved in WSAS functionality, as further described in Section III).

The Commission should also require testing during the FCC certification process that sufficiently exercises the operational domain of WSAS software control functionality. For example, such testing should include that which: (1) uses various combinations of channels authorized to ensure the transition from one combination to another occurs correctly; (2) ensures that when the database does not renew the authorization automatic shutdown occurs reliably within the expected timeframe (including fast polling times as described below); and (3)

---

found that a recall was not necessary because the devices in question had already been brought into compliance with the FCC's rules).

confirms that the device responds correctly to any shutdown commands that may be "pushed" from the database. To provide meaningful assurance, all such tests must exercise a significant (using statistical, combinatorial, or other objective metrics) set of distinct inputs and operating conditions. In lieu of performing all such testing itself or at TCBs, the Commission could consider objective evidence (*i.e.*, detailed test procedures and results) of such rigorous verification activities submitted by a proposed white space device vendor as part of its own quality management system established pursuant to pre-market design controls as described in Section III.

V. THE ROBUST ENFORCEMENT OF THE FCC'S DEVICE SECURITY RULES WOULD HELP PROTECT THE INTEGRITY OF THE DATABASE SYSTEM.

As NAB and GEHC have both indicated, the FCC should institute more thorough and robust enforcement of its Part 15 rules, including those set forth in Sections 15.709(f) and 15.711(j), to incorporate real and effective accountability.[23] Its 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 white space device software.[24] Moreover, even if the FCC introduces an increased level of rigor into the certification process as suggested above, it must still swiftly investigate and sanction those who fail to comply with its operational rules.

[23] *See* 47 C.F.R. §§ 15.709(f), 15.711(j).

[24] *See* GEHC Reply Comments at 10; see also, e.g., Opposition and Reply of CTIA to Petitions for Reconsideration, GN Dockets No. 12-268, 14-166, at 10 (filed Feb. 29, 2016) ("stress[ing] that for this regime to be effective, white space databases must contain accurate information regarding the technical parameters and location of white space devices").

Illustrating this, NAB recently found rampant false device registrations – including, most alarmingly, inaccurate device location information upon which the effectiveness of the geolocation/database scheme depends entirely.[25] Although this problem may be alleviated slightly by eliminating the "professional installer option," these inaccurate registrations clearly demonstrate that: (1) many existing devices are inherently insecure and thus fail to comply with the Commission's rules; and (2) the FCC's current certification process is manifestly ineffective in preventing non-compliant white space device operation. For example, at least one manufacturer makes its "professional installer manual" freely available on its website, so that any user can modify critical information (such as geolocation information upon which WSAS functionality depends) without authorization or authentication.[26] These unsecure devices pose a security vulnerability to the entire WSAS and its dependability.

VI. THE COMMISSION SHOULD ALSO BOLSTER WSAS FUNCTIONALITY TO ENSURE THAT LICENSED USERS CAN RELY ON ITS RELIABLE AND SECURE OPERATION.

The required WSAS functionality can be bolstered by modifying the Commission's Part 15 rules in at least the following three respects. First, the FCC should require white spaces devices to use reliable, secure, and accurate geopositioning technology, such as properly implemented GPS. Although the FCC appropriately proposes to eliminate the "professional installer option" for fixed devices,[27] its rules otherwise provide only that white space devices

[25] *See* Letter from Scott Goodwin, Associate General Counsel, National Association of Broadcasters, to Marlene H. Dortch, Secretary, FCC, RM-11745, ET Docket No. 14-165, Attach. at 3 (filed June 11, 2015).

[26] *See* Adaptrum, ACRS 2.0 Professional Installer Manual, *available at*: http://www.adaptrum.com/acrs2launch/content/acrs20_professional_installer_02062014.pdf (last visited May 5, 2016).

[27] *See* NPRM ¶ 2.

incorporate "geolocation capability" to determine their locations.[28] The Commission should go a step further by identifying either: (a) which geopositioning technologies are appropriate for use by white space devices; or (b) a set of criteria – including, but not limited to, accuracy – that can be used to determine whether a geopositioning technology is appropriate for use by white space devices.[29]

Second, the FCC should decrease the interval at which devices must renew their authorization with the white space database to – at most – ten minutes for fixed white space devices and one minute for personal/portable white space devices.[30] White space devices' current ability to operate for up to two days while disconnected from the database undermines the effectiveness of the geolocation/database scheme, as GEHC and others have explained in numerous filings.[31] A fast-polling approach, for example, could be a better alternative if it includes Channel 37 as one of the fast-polling channels.[32]

Third, as part of the device authentication process, the FCC should require databases to validate the revision and integrity of embedded software with respect to what is currently certified.[33] Fourth, the Commission should require registration of personal/portable white space

---

[28] *See* 47 C.F.R. § 15.711.

[29] The white space database should take into account the worst case inaccuracy for a device when determining whether it may operate at a particular location so that the same required protection distances are maintained at all times.

[30] The Commission's current rules allow white space devices to operate for up to two days while disconnected from the white space database, which would cripple any "push" technology. *See* 47 C.F.R. §§ 15.711(c), (d).

[31] *See, e.g.*, Consolidated Reply of GE Healthcare, ET Docket No. 14-165, GN Docket No. 12-268, at 9-10 (filed Mar 10, 2016).

[32] *See id*.

[33] "Firmware signing" technology is mature, robust, simple and inexpensive. It is used, for example, in gaming consoles to ensure that only software approved and licensed by the console manufacturer may run on the device. When security vulnerabilities or other bugs impacting WSAS functionality are inevitably identified after a device is certified and placed on the market the WSAS must be capable of suspending

device information in the database to support interference investigation and remediation of these devices which (due to ubiquity and mobility) will be most likely to cause interference and most difficult to identify and locate.[34]

VII. CONCLUSION

If adopted, the NPRM's proposals would likely improve somewhat the accuracy of fixed white space device data, but the Commission should also address key weaknesses in current WSAS technical requirements and in the Commission's rules governing device-resident WSAS software development, certification and enforcement in order to ensure that its geolocation/database scheme fully protects licensees and other licensed users.

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
Wesley B. Platt
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004
Phone: (202) 637-5663

May 6, 2016

Counsel to GE Healthcare

---

authorization for any devices containing the defective software and ensuring that necessary updates have been installed before authorizing the device to access spectrum.

[34] Under the Commission's current rules, only fixed white space devices are required to register in the database. *See* 47 C.F.R. § 15.711.