GE Healthcare
8200 W. Tower Avenue
Milwaukee, WI 53223
T +1 414-362-2715
www.gehealthcare.com

February 6, 2018

**VIA ELECTRONIC DELIVERY**

Director General, Engineering
Planning and Standards Branch
Innovation, Science and Economic Development Canada
235 Queen Street
Ottawa, Ontario K1A 0H5

Re: **Consultation on the Technical and Policy Framework for White Space Devices, SMSE-018-17, November 2017**

Dear Director General:

GE Healthcare ("GEHC") hereby submits these comments in response to Innovation, Science, and Economic Development Canada's ("ISED") Consultation on the Technical and Policy Framework for White Space Devices.[1] The Consultation seeks comment on a technical and policy framework for the use of white space devices. In **Question 4**, ISED proposes to continue to preclude the use of television channel 37 ("Channel 37") by white space devices. As explained below, GEHC supports ISED's proposal to continue to prohibit white space devices from operating in Channel 37 in light of the risk of harmful interference they would pose to safety-of-life wireless medical telemetry systems ("WMTS").

## 1. WMTS Operations in Channel 37 Must Remain Protected.

Hospitals and other healthcare facilities routinely use WMTS to monitor patient data in real time (*e.g.*, heart rate, oxygen saturation, and electrocardiography data). This information is, in turn, used to detect life-threatening events such as cardiac arrhythmias and apneas. By empowering healthcare providers to remotely monitor their patients' physiological data, WMTS equipment has played a transformative role in the healthcare industry, "provid[ing] significant benefits to patients in terms of mobility and comfort" and emerging as a "significant tool in reducing healthcare costs."[2]

[1] *See* Consultation on the Technical and Policy Framework for White Space Devices, SMSE-018-17, published in the Canada Gazette, Part 1, on November 25, 2017 ("Consultation").

[2] *See Amendment of Parts 2 and 95 of the Commission's Rules to Create a Wireless Medical Telemetry Service*, Order, 16 FCC Rcd 4543 ¶ 2 (2001).

WMTS thus plays a pivotal – and increasingly important – role in Canadian healthcare. Indeed, WMTS are currently deployed in thousands of unique locations in Canada and the United States, and the number of healthcare facilities that rely on WMTS is expected to increase significantly as hospitals and other healthcare providers adapt to aging patient populations and increased patient acuities.

### 2. Considerable Separation Distances Would be Required to Protect WMTS Operations from Harmful Co-Channel Interference.

As a safety-of-life service, WMTS cannot tolerate even small or episodic incidents of interference. For example, a single source of interference can cripple an entire WMTS and be extremely difficult to identify, all the while endangering patients and diverting the attention of hospital staff. Accordingly, it would be critical that ISED ensure separation distances that would adequately protect WMTS from co-channel, unlicensed operations if it were to allow white space devices to operate in channel 37.

Tests performed in 2015 by GEHC and the WMTS Coalition (through its technical consultant, Comsearch) confirm the sensitivity of WMTS to co-channel interference and the fact that the separation distances required to adequately protect WMTS operations from harmful interference would be considerable.[3] These tests assessed interference effects on two hospitals' existing WMTS from a simulated white space device and separately measured path loss between the simulated white space device and third party receive antennas that had been placed near actual WMTS receive antenna.[4]

Among other things, the tests demonstrated that significant harmful interference can be caused to WMTS from even a single white space device operating at the power levels, separation distances, and height that the Federal Communications Commission ("FCC") had proposed to allow, which include separation distances ranging from 8 to 0.03 kilometers.[5] The tests also confirmed that the TM 91-1 propagation model, which the FCC had used to calculate separation distances, frequently overestimates path loss over short distances and line-of-sight conditions. At both hospitals, GEHC and the WMTS Coalition found that free space or near free space path loss could be expected from white space devices located outdoors at near ground level to the perimeter of the hospital.[6]

[3] *See* Letter from Lawrence J. Movshin, Counsel, WMTS Coalition, et al., to Marlene H. Dortch, Secretary, FCC, ET Docket No. 14-165, GN Docket No. 12-168 (filed July 20, 2015) ("Field Test Results").

[4] *See id*.

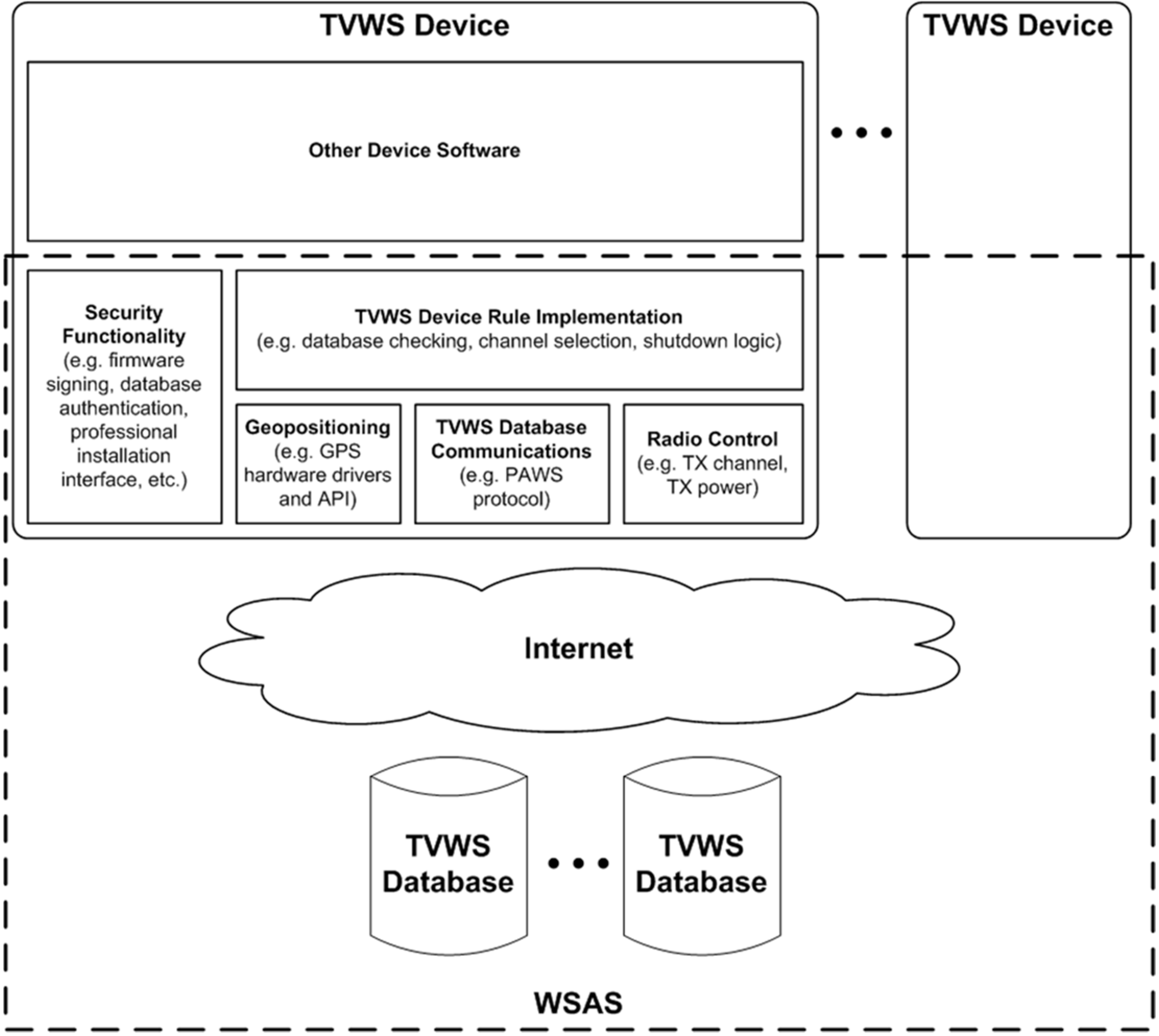
[5] *See id*.; *Amendment of Part 15 of the Commission's Rules for Unlicensed Operations in the Television Bands et al*., Notice of Proposed Rulemaking, 29 FCC Rcd 12248, ¶¶ 42, 112 (2014).

[6] *See* Field Test Results.

### 3. Serious Concerns Exist Concerning the Dependability of the Software Upon Which White Space Devices and the Geolocation Database Will Rely.

The envisioned geolocation database scheme[7] required for white space device operation entails a massive and complex, autonomous real-time distributed system (hereinafter referred to as the Whitespace Spectral Access System ("WSAS"), as depicted below in Figure 1.

***Figure 1***


TVWS Device
Other Device Software
Security Functionality (e.g. firmware signing, database authentication, professional installation interface, etc.)
TVWS Device Rule Implementation (e.g. database checking, channel selection, shutdown logic)
Geopositioning (e.g. GPS hardware drivers and API)
TVWS Database Communications (e.g. PAWS protocol)
Radio Control (e.g. TX channel, TX power)
TVWS Device
Internet
TVWS Database
TVWS Database
WSAS

Yet the dependability of the WSAS is a key issue.[8] Of particular concern is that the critical WSAS functionality (*e.g.*, geopositioning, database interface, radio control, and security

[7] *See* Consultation at 2-3.

functions) in white space devices will be software-based and almost certainly include many open-source and commercial off-the-shelf software components. Malfunctions or programming errors could cause these devices to transmit incorrect information to the white space database or mistakenly assume that they have permission to operate on a particular channel when, in fact, they do not.

Meanwhile, most white space devices are likely to be low-cost, consumer-grade devices that are vulnerable to manipulation by unauthorized third parties or device owners. As evidenced by seemingly daily news stories, the risk that hackers will be able to access these devices is high.[9] Meanwhile, device owners themselves will likely be able to easily modify the devices to operate in ways their manufacturers never intended. 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.[10]

Additionally, the WSAS itself would become a safety-critical system if white space devices were allowed to operate in Channel 37 because the continued interference-free operation of thousands of safety-of-life WMTS would end up depending on its reliable and secure operation. Specifically, ISED would be relying upon the WSAS not only to prevent interference to WMTS, but also to be an essential tool for the remediation of any unexpected interference events. Therefore, no matter what distance- or location-based separation rules were adopted to protect Channel 37 WMTS operations from harmful interference, in order to dependably prevent unauthorized operations at locations near WMTS ISED would have to take steps to ensure the *end-to-end* reliability and security of the entire WSAS that implements and enforces those separation rules, including not only the databases but also the WSAS functionality (*e.g.*, geopositioning, database interface, radio control and security functions) that resides within consumer devices.

Indeed, basic security vulnerabilities in white space devices currently on the market, including publicly-disclosed default passwords for professional installation settings (including geographic coordinates), may have already compromised the integrity of the information in white space databases used in the United States. The National Association of Broadcasters, for

[8] "Dependability" refers to system properties like reliability and security that allow a system to be relied on to function as required. "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.

[9] *See, e.g.*, Douglas Busvine and Stephen Nellis, *Security Flaws Put Virtually All Phones, Computers at Risk*, Reuters (Jan. 3, 2018), https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO; 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.

[10] *See, e.g.*, Patrick Lucas Austin, *How to Jailbreak your iPhone: The Always Up-to-Date Guide [iOS 10]*, Lifehacker.com (July 26, 2017), https://lifehacker.com/how-to-jailbreak-your-iphone-the-always-up-to-date-gui-1797058645.

example, has reported a number of location errors in the white space databases authorized by the FCC.[11] Moreover, these errors were not immediately corrected. In the case of a white space device improperly registered to a site in the middle of Lake Michigan, for instance, the device's operating location was not changed until nearly three months after the error was reported.[12]

**4. Conclusion.**

Given the safety-of-life nature of WMTS and its susceptibility to interference, ISED should continue to prohibit white space devices from operating in Channel 37. The separation distances required to adequately protect WMTS operations would be considerable, as evidenced by the GEHC and WMTS Coalition field tests. Moreover, even if ISED was able to craft separation distances that adequately protected WMTS, serious questions would remain regarding the dependability (including reliability and security) of the proposed geolocation database scheme. No separation distance – no matter how large – will be effective unless dependably enforced.

Respectfully,

/s/ Neal Seidl
Neal Seidl
Principal Engineer – Systems Interoperability
GE Healthcare
Neal.Seidl@med.ge.com
T+1 414-362-2880

/s/ Matthew Pekarske
Matthew Pekarske
Principal Engineer – Wireless
GE Healthcare
Matthew.Pekarske@ge.com
T +1 414-362-2715

[11] *See, e.g.*, Reply Comments of the National Association of Broadcasters, ET Docket No. 16-56, at 4-6 (filed June 3, 2016).

[12] *See id*. at 5.