Canadian Electricity Association | Association canadienne de l'électricité

Filed via My CRTC Account

Mr. Claude Doucet, Secretary General
Canadian Radio-television and Telecommunications Commission
Les Terrasses de la Chaudière
1 Promenade du Portage
Gatineau, Québec J8X 4B1

15 July 2020

RE: Final Submissions of the Canadian Electricity Association in *Review of mobile wireless services*, Telecom Notice of Consultation CRTC 2019-57, 28 February 2019 ("TNC 2019-57" or the "Notice"), as modified by Telecom Notices of Consultation 2019-57-1, -2, and -3

Dear Mr. Doucet,

1. Founded in 1891, the Canadian Electricity Association ("**CEA**") is the voice of more than 40 Canadian electrical utilities ("**CEUs"**) based in every Canadian province and territory. All of our member CEUs are electricity generators, transmitters, and/or distributors.

2. In the past, CEA members have built, operated and, in many cases, sold facilities-based telecom carrier arms acquired by third parties participating actively in the current proceeding. Today, our members' telecommunications carrier operations are integrated tightly into the business of getting power to Canadians, operating within regulatory frameworks that help ensure that CEUs focus on core activities.

3. These activities have, around the world, evolved to embrace advanced wireless, machine-to-machine applications to smart grids that can orchestrate disparate electricity generation and distribution activities in ways that are more resilient, more adaptable, and more efficient and environmentally friendly. In Canada this evolution is also underway, but in certain respects is stalled for reasons that fall under the CRTC's jurisdiction. To wit, wording in the *Canadian International Mobile Subscriber Identity (IMSI) Guideline* ("**Guideline**") prevents CIOs from accessing the Mobile Network Codes ("**MNCs**") that are the sole technical, standards-based way of assuming responsibility for routing this traffic.

4. These final submissions of the CEA, in the proceeding on wireless services initiated by Telecom Notice of Consultation CRTC 2019-57, are the culmination of what has been a long road before the CRTC in pursuing this topic. That road began with a Part 1 application filed, on 30 October 2018, whose submissions it was suggested would be better combined with the instant proceeding.

5. Throughout, the CEA's recommendations have been focussed and consistent with all critical infrastructure participants. We do not seek mandated wholesale. We are not advocating for any form of MVNO. We recommend only that the CRTC direct the Canadian Steering Committee on Numbering ("**CSCN**"), in which the CEA is now a participant, to correct the gaps in the Guideline and, thereby, unlock CIOs' ability to deploy service architectures the barriers to which, in our respectful view, the *Telecommunications Act* strongly militates in favour of removing.

275 Slater Street, Suite 1500 | 275, rue Slater, bureau 1500 | info@electricity.ca | info@electricite.ca | T 613 230 9263
Ottawa, Ontario K1P 5H9 | Ottawa (Ontario) K1P 5H9 | www.electricity.ca | www.electricite.ca | F 613 230 9326

A. The paragraph we seek is a low-risk, high-reward opportunity to fulfill Act objectives

6. In its appearance before the CRTC in this proceeding, the CEA excerpted the following four paragraphs, numbered 159-162, of Telecom Regulatory Policy CRTC 2015-177:[1]

> **Regulatory measures with respect to wholesale MVNO access**
>
> **Acquisition of mobile network codes by full MVNOs**
>
> 159. Mobile network codes (MNCs)[33] in Canada are assigned by the Canadian Numbering Administrator pursuant to the Canadian International Mobile Subscriber Identity (IMSI) Guideline (the Guideline). The Guideline was developed by the Canadian Steering Committee on Numbering (CSCN)[34] and approved by the Commission.[35] The Guideline requires that an applicant for an MNC hold a spectrum licence from Industry Canada. Thus, MVNOs cannot acquire MNCs.
>
> 160. CNOC, Cogeco, Lycamobile, and Orange submitted that full MVNOs should be permitted to acquire their own MNCs, which would enable them to provision their own IMSI numbers. Cogeco submitted that allowing full MVNOs to acquire their own MNCs is critical to ensuring that a full MVNO can operate in the retail market independently of its host wireless carrier.
>
> **Commission's analysis and determinations**
>
> 161. The Commission considers that allowing full MVNOs to acquire MNCs would provide MVNOs with a greater level of independence, because they would not have to rely on the host wireless carriers' MNCs and subscriber identification module (SIM) cards. Having its own unique MNC enables a full MVNO to more easily switch its host wireless carrier, make arrangements with multiple wireless carriers, and negotiate its own wholesale roaming arrangements (e.g. with international wireless carriers). The Commission therefore considers that it is appropriate to amend the Guideline to allow for the assignment of MNCs to full MVNOs.
>
> 162. The Commission hereby **directs** the CSCN to (i) amend the Guideline to allow full MVNOs to acquire MNCs, and (ii) submit the amended Guideline for Commission approval by **6 July 2015**.

7. The outcome that CIOs seek in this proceeding, which we have suggested that section 7 of the *Telecommunications Act* guides the Commission towards implementing, is similar to that which the Commission undertook in 2015 in respect of giving MVNOs the ability to enter into commercial, non-mandated negotiations. We suggested, in our appearance, that it could for instance take the following form, blacklined to paragraphs 161 and 162 of TRP 2015-177:

> **Proposed Commission's analysis and determinations**
>
> #. The Commission considers that allowing ~~full MVNOs~~Critical Infrastructure Network

[1] *Regulatory framework for wholesale mobile services,* Telecom Regulatory Policy CRTC 2015-177, 5 May 2015.

> Operators to acquire MNCs would provide ~~MVNOs~~critical infrastructure operators with ~~a greater level of independence~~the opportunity to continue to innovate and invest in always-on, resilient networks, including in rural and remote areas, because they would not have to rely on the host wireless carriers' MNCs and subscriber identification module (SIM) cards. Having its own unique MNC enables a ~~full MVNO~~Critical Infrastructure Network Operator to more easily switch its host wireless carrier, make arrangements with multiple wireless carriers, and negotiate its own wholesale roaming arrangements (e.g. with international wireless carriers). The Commission therefore considers that it is appropriate to amend the Guideline to allow for the assignment of MNCs to ~~full MVNOs~~Critical Infrastructure Network Operators.
>
> #. The Commission hereby **directs** the CSCN to (i) amend the Guideline to define Critical Infrastructure Network Operators (CINOs) and allow CINOs to acquire MNCs, and (ii) submit the amended Guideline for Commission approval by ~~6 July 2015~~**● 2020**.

8. This approach would, we submit, combine low risk with high reward, as follows.

Low risk

9. The approach proposed is low-risk because there is a wide consensus around it, there is an expert stakeholder committee in place to properly implement it, no one appears to oppose it, and it disadvantages no one.

10. With respect to wide consensus and implementation by the related stakeholder committee, we note that not only do Canada's counterparts provide for similar measures, as set out in the CEA's prior submissions, but the Canadian Steering Committee on Numbering similarly recognizes what is in fact a far broader use than the approach suggested above. CSCN Task Identification Form (TIF) 104, to which the CEA averted in its oral presentation, sets out an approach to requesting further Mobile Network Code inventory from the ITU-T Telecommunication Service Bureau, on the grounds that

> [t]here is a potential for a rapid increase in demand by various entities such as prospective Full MVNOs and private LTE radio network operators. The purpose of this TIF is to recommend appropriate steps before the industry runs out of suitable Mobile Network Codes (MNCs) available for assignment…[2]

11. Of course, the CEA recognizes that non-CIO operators of the large-scale private LTE networks identified in the above-cited TIF will likely have an interest in MNC access going forward in order to pursue innovative and future-oriented wireless machine-to-machine applications. But the approach we have set out is more modest. It would merely extend potential MNC access, always subject to the discretion of the CSCN having regard for scarcity and for alternative uses, to a new category of Critical Infrastructure Network Operators to be defined alongside the existing Full MVNOs, within which the CRTC could embed any gating criteria—such as network size, whatever the basis on which it were measured—recommended by the CSCN.

12. The CEA and its members are experienced network builders and operators and radiocommunication licensees. We are long-standing, active members of the Radio Advisory Board of Canada. While a preceding remark that critical infrastructure operators are "seeking mandated access for enterprise

---

[2] *TIF 104: Update Canadian IMSI Assignment Guideline* (CNTF104x), Canadian Steering Committee on Numbering (CISC CSCN).

and public entities"[3] is, with respect, plainly incorrect—neither the CEA nor, the record demonstrates and we have confirmed, the RAC seeks mandated access of any type—we concur with the remarks of Rogers Communications to the extent they recognize that CIO access to MNCs is a necessary "part of the commercial arrangement"[4] that will allow our members to do business with MNOs like Rogers in assembling redundant multi-provider connectivity portfolios for sensitive functions. More broadly, we note that no party has opposed the proposal of the two critical infrastructure sectors with an interest in this proceeding, notwithstanding certain, frankly, confusing suggestions as to disharmony addressed below.

13. Finally, we note that the approach proposed disadvantages no one. No party is being asked to unbundle their own network or provide network resources on any basis other than commercial negotiation. No party is being asked to give over limited resources to critical infrastructure operators when these are needed operationally. Indeed, the ability of CEUs as non-PSTN providers to make use of three-digit Mobile Network Codes, in contrast to the very large two-digit blocks, or multiples thereof, allocated even to non-operational MVNOs or for experimental purposes, may help entrench more efficient forms of MNC stewardship within Canada.

High reward

14. If the downside to the CEA's and, more broadly, the critical infrastructure sectors' proposal is small, the potential rewards are great.

15. First, paragraph 7(a) the *Telecommunications Act* requires that the Commission exercise its powers and perform its duties with a view to facilitating the orderly development, throughout Canada, of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions. The efficient, ecological, and resilient operations that smart grids portend, and the simple act of enabling MNC access will let CEUs pursue them, will do so. These functions will enrich the social and economic fabric of Canada's regions everywhere that it is important to keep the lights on and the machines humming.

16. Second, however, they will also unlock potential CEU technology investment that, under the Private Virtual Network Operator ("**PVNO**") architecture, would create significant new connectivity revenue streams for established and competitive MNOs in Canada's regions—and potential co-build opportunities that lower deployment costs where CEUs pursue a Shared RAN architecture. This outcome corresponds not only to the objectives of paragraph 7(a) of the Act, but also those of paragraph 7(b), requiring the Commission to act with a view to rendering reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada.

17. If the CRTC wishes to aggressively pursue rural broadband opportunities that do not require subsidy, in other words, acceding to the critical infrastructure sectors' requests early in a focussed, one-off decision is such an opportunity.

---

3 Transcript, 26 February 2020, paragraph 9918 (CRTC—Chairperson).

4 Transcript, 26 February 2020, paragraph 9923 (Rogers Communications Canada Inc.—H. Slawner, Vice-President, Regulatory Telecom). We note a subsequent discussion with respect to network slicing (which is not directly relevant to the topic at hand) and eSIMs (confirming that these do not permit the multi-homing which all full participants in the Canadian telecommunications system require in order to manage their own resiliency and connectivity).

18. Third, the *Telecommunications Act* requires that the Commission exercise its powers and perform its duties with a view to enhancing the efficiency and competitiveness of Canadian telecommunications, at paragraph 7(c); and to fostering increased reliance on market forces and ensuring that regulation is efficient and effective, at paragraph 7(f). The CEA's submissions have identified minor but, to Canada's utilities and those who rely on them, critical instances of over-regulation that prevents major telecommunications operators in Canada from accessing the resources needed to negotiate and pursue market-based solutions for resilient infrastructure. This is an opportunity for the Commission to correct this in a way that fulfils its obligation to fulfil these policy objectives.

19. Fourth, the *Telecommunications Act* requires that the Commission act with a view to stimulating telecommunications research and development and innovative service provision. The solutions that the CEA calls on the CRTC to enable CEUs to pursue, which are in use in a growing number of jurisdictions throughout the world, are ones that in the Canadian context have been developed and elaborated in CEU-administered research facilities,[5] and would provide for major machine-to-machine deployments over wireless broadband in ways that align completely with the Act's obligations.

20. Fifth, and as discussed in greater detail below, CEUs are obligated to adhere to specific and strict cybersecurity standards in ways that will contribute to the protection of the privacy of persons and their data in Canada, advancing objective (i) of the Canadian Telecommunications Policy. Indeed, that obligation on CEUs is what drives the requirement that CEUs continue to manage their own networks and be directly answerable for their own security needs—but also what will help ratchet up the telecommunications sector's cybersecurity stance by introducing these obligations into it.

B. Canadian Electrical Utilities are infrastructure operators with strong cybersecurity obligations

21. The CEA was surprised to note, in certain submissions made in this proceeding, the proposition that cybersecurity obligations will be best-served by ensuring that the operation of mobile network cores in Canada is restricted to Mobile Network Operators who operate primarily consumer-facing businesses.

22. We understand that such submissions were, in many cases, directed towards MVNOs, presumably on the basis that although the cybersecurity standards that the Commission has put in place in respect of MNOs and MVNOs do not differ, MVNOs are likelier to be smaller, newer operators who are less proficient at operating the secure telecommunications equipment that MNOs and MVNOs alike source from third parties.

23. However, we respectfully underline a key distinction between telecommunications carriers regulated only by the CRTC, and critical infrastructure operators whose networks are regulated both by the CRTC and by sector-specific regulators that have not been shy to impose specific, direct, and mandatory cybersecurity obligations.

24. The Ontario Energy Board in Ontario, for instance and to cite only one example, adopted in 2018 an *Ontario Cyber Security Framework*, following a two-year process initiated by a February 2016 letter on a *Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario* initiative. This framework includes both a policy and specific reporting requirements, and is

---

5 See, *e.g.*, B.L. Agba, S. Riendeau, M. Shirazipour, S. Jrishnan, A. Aranibar, and D. Monette, "LTE for smart grid communication: the Canadian outlook", *IEEE Canadian Review,* Spring 2014.

tracked to CCS, COBIT 5, ISA 62443, ISO 27001, and NIST specifications.[6] That framework has now been in place for years. It complements other cybersecurity specifications for which electrical utilities are similarly answerable, including notably the North American Reliability Corporation ("**NERC**") Critical Infrastructure Plan.

25. One could no doubt re-litigate and re-engineer the technical decisions by which electrical utilities assure their always-on resilience and their compliance at all times with these and other obligations. Indeed, inviting CIOs to radically revise their operating models by suggesting that, for the first time, they become customers of MNOs in respect of these critical functions would constitute one such redesign. However, we respectfully submit that such a redesign is not only unrealistic, but unhelpful and inappropriate. As the CEA noted in its prior submissions, the pervasive operation of telecom networks highly enmeshed in utility operations is a core functionality for electricity telecom networks. Inserting an intermediary between CEUs and this functionality would threaten CIOs' ability to meet and demonstrate their constant readiness to meet their rigorous operating standards.

26. It would no doubt be possible to re-imagine the businesses of Bell, TELUS, or Rogers if they had to outsource all of their core network operations. But, we respectfully submit, fidelity to the Canadian Telecommunications Policy and an attempt to favour market forces and commercial negotiations militates against this complex re-litigation, re-engineering, and re-imagining. The more straightforward, more effective and, it is submitted, more Act-compliant approach is simply to remove the regulatory barrier preventing CIOs from operating broadband wireless networks.

C. Critical Infrastructure Operators are completely aligned

27. The CEA was similarly surprised to review submissions that the CEA and RAC, or the members of the CEA and members of the RAC, or the members of either association with respect to one another, might not be completely aligned on the issues set out in the two associations' submissions.[7]

28. We note that no evidence has been filed to corroborate this assertion and, to the contrary, underline the well-publicized joint resolutions adopted at the 26 March 2019 multi-sectorial workshop hosted by the CEA and RAC, which included representation from ISED and Transport Canada.[8] To the same end, we confirm that upon further verification, we are not aware of any contrary position taken by CEA or RAC member with respect to the matters set out in the CEA's and RAC's filings in this proceeding.

29. The CEA's board of directors is made up of executives from virtually of Canada's electricity utilities. Attached, as Appendix A, is a CEA letter to the same effect that is executed by the chair of the CEA's board and by the CEA's chief executive officer. As the letter notes,

---

6 *Ontario Cyber Security Framework*, Ontario Energy Board, 6 December 2017, pages 35-59 (Appendix E, "Security Controls & Risk Profiles Requirements"), adopted in *Amendments to the Transmission System Code and the Distribution System Code to Address Cyber Security for Electricity Transmitters and Distributors*, Ontario Energy Board EB-2016-0032, 15 March 2018.

7 See, *e.g.*, transcript, 19 February 2020, paragraph 2538 (Bell Canada—M. Graham, Assistant General Counsel, Regulatory Policies and Competition).

8 See, *e.g.*, Denis Carmel, "Wireless Review: Railways, Utilities, want spectrum access, too", *Cartt.ca*, 20 May 2019.

> While each CEA member operates in jurisdictions with unique geographies, customer bases, and operating models, for which they develop, build, own, and operate advanced telecommunications networks accordingly, the lack of MNC access represents a common barrier. Investing in the continued modernization of advanced networks is essential and, in the regulated environment in which CEA members function, lack of MNC access is a bottleneck for all members.

30. We trust that this will put to rest any suggestion to the contrary.

D. Critical infrastructure and public safety are distinct sectors

31. We earlier noted a further misapprehension, suggesting that critical infrastructure sectors seek mandated wholesale access. This misapprehension likely, in our view, stems from a related misapprehension as to the relationship between the public safety and critical infrastructure sectors, which are distinct and separate from one another. In fact, these categories are clearly delineated and strictly policed within public safety broadband. For instance:

> Public safety services (services involving the preservation of life and protection of property) will continue, if possible, to have access to exclusive channels and any eventual sharing of channels by public safety services will be with other public safety services. The Department recognizes the following hierarchy of public safety agencies:
>
> Category 1 — police, fire and emergency medical services
>
> Category 2 — forestry, public works, public transit, hazardous material clean-up border protection and other agencies contributing to public safety
>
> Category 3 — other government agencies and certain non-government agencies or entities
>
> Category 1 system operators are eligible for trunked or conventional systems. Category 2 system operators are eligible to share trunked systems with Category 1 users provided that the latter remain the major users of the system. Major users are agencies which have priority over other types of users on the system. Category 2 system users would not be eligible to operate their own systems within the bands 821-824 MHz and 866-869 MHz unless the local spectrum management office is satisfied that their operation would not preclude the future introduction of a Category 1 system. Category 3 system operators and selected supervisory personnel of non-government agencies (e.g. hydro and gas utilities) may be permitted access to public safety systems during emergency situations where their access will be controlled by the major users operating those systems.[9]

32. The same distinction exists with respect to broadband spectrum. Public safety organisations, which do not raise funds directly from rate-payers in the way that critical infrastructure organisations do, benefit from a public grant of 700 MHz spectrum, known as Band 14, towards a Public Safety Broadband Network ("**PSBN**"), with an associated MNC assignment, in order to facilitate their own expansion from narrowband into broadband wireless applications. There will be an opportunity, not only for MNOs, but also for other third parties like CIOs to become involved as partners with the PSBN. To that effect, the Temporary National Coordinating Office currently responsible for the

---

9 *Technical Requirements for Land Mobile and Fixed Radio Services Operating in the Bands 806-821/851-866 MHz and 821-824/866-869 MHz*, ISED SRSP-502 (Issue 5), December 2017 (emphasis added).

PSBN noted recently ISED's 2017 decision paper's statement that "commercial use of unused capacity will be allowed provided that public safety users, will have priority and pre-emption rights over any form of commercial usage", and went on to note that

> [c]ommercial utilities and other infrastructure operators have also identified synergies with a PSBN and have expressed interest in leveraging Band 14 spectrum to support their mission critical communication requirements. These potential partners in a PSBN could bring valuable communications infrastructure thereby speeding deployment and increasing the coverage footprint of the PSBN.[10]

33. The opportunity to explore synergies with PSBN implementation is of significant interest to CIOs, as it is to MNOs and other parties. However, it is important to underline that at the logical layer, the PSBN will operate as a coherent network with responsibility for its own routing and its own traffic, which will maintain priority over that of external users such as MNOs and CIOs. The ability to explore the above-noted synergies with the PSBN by bringing valuable communications infrastructure, thereby speeding deployment, depends on CIOs' ability to similarly operate a distinct logical layer alongside the PSBN through shared-RAN and PVNO architectures. That, in turn, requires that CIOs have access to MNCs, such as could be effected through the regulatory approach recommended in paragraph 7 of these final submissions.

E. <u>The CSCN is best-placed to address any resource scarcity questions</u>

34. It is common ground that Mobile Network Codes are a limited resource to be stewarded carefully by the Canadian Numbering Administrator ("**CNA**"). Appropriately, therefore, the appearing portion of the instant proceeding put questions to both the CEA and RAC with respect to their commitment to using this resource minimally and efficiently. In particular, there appeared to be a concern as to the opening of potential floodgates.

35. With respect to floodgates, we note that, alongside the public safety, only two critical infrastructure sectors had an interest in the instant proceeding, both of which are long-standing and active telecommunications-sector participants and investors. Further, upon review of the various constituencies represented at the Radio Advisory Bureau of Canada, the telecommunications and broadcasting, public safety, transport, and energy sectors appear to account for virtually all participants. The outlier, home appliance and electronics manufacturing, would to that end appear well-suited to reliance on telecommunications service providers, whether existing players or machine-to-machine connectivity specialists, whose MNC access is already covered off under MNO/MVNOs.

36. There would therefore appear to be little evidence to support a floodgates argument from long-standing telecommunications-reliant sectors. More importantly, however, we have also noted that

- the CSCN is engaged, in its TIF 104, in procuring an additional MNC allocation in anticipation of a far broader, generalized private-LTE use; and

- the CSCN is constituted for the purpose of stewarding these limited resources wisely and

---

10 *Progress Report on a National Public Safety Broadband*, Temporary National Coordination Office, 2019, citing *Decisions on Policy, Technical and Licensing Framework for Use of the Public Safety Broadband Spectrum in the Bands 758-763 MHz and 788-793 MHz (D Block) and 763-768 MHz and 793-798 MHz (PSBB Block)*, ISED SMSE-014-17, June 2017.

efficiently, and has the means to do so.

37. We respectfully submit that, rather than second-guess the work of the CSCN, simple instructions such as those proposed in paragraph 7 would allow the CSCN to carry forward the framework in which it will continue to apply its expertise to this end. Indeed, insofar as the work of TIF 104 also includes "add[ing] monitoring and jeopardy condition procedures to the Canadian IMSI Assignment Guideline", such an approach is surely attuned to the direction in which the CSCN is already headed.

38. The CEA has elsewhere underlined such existing conditions as the in-place allocation of three MNCs to the time-limited experimental testbed for the very architectures for which CIOs will use them post-experimental, and the ability of CIOs to make use of three-digit identifiers that do not depend on legacy PSTN equipment. However, in our view these arguments are ultimately ones best raised in the context of the CSCN. The CEA has now been fully on-boarded into the CSCN process, and looks forward to continuing to participate as a stakeholder in the Canadian telecommunications system and member of its community.

F. <u>The bottleneck is becoming urgent</u>

39. Finally, and again noting the ways in which smart-grid technologies continue to advance, and the lack of non-testbed MNC access continues to prevent CIOs from self-administered traffic routing in the spectrum bands best suited to these technologies, the Canadian Electricity Association respectfully requests that the CRTC consider what we have suggested is a modest request with dispatch.

40. To illustrate the ways in which this issue is rippling the Canadian electricity sector, please note Appendix B, consisting of a Web index page, a cover sheet, and an excerpt from our member Hydro Ottawa's 2021-2025 Distribution System Plan filings to the Ontario Energy Board. These filings related to application for approval of expenditures and technologies that Hydro Ottawa will implement over the next five years.

41. The excerpt is about the designation, in the 2016 Telecommunications Master Plan project executed during the 2016-2020 rate period, of certain investments for a Field Area Network

> intended to provide robust, secure, private, high bandwidth, and low latency wireless connections from field devices (e.g. automation devices, sensors, etc.) to Hydro Ottawa owned and operated towers along [its] Optical Telecommunications Network OTN). Unfortunately, during the early execution phase of the Telecommunications Master Plan, it was discovered that the technology originally selected for the FAN was not an appropriate or prudent choice (WiMAX) therefore the decision was made to postpone the FAN investment to the next rate period (2021-2025). This project is designed to deploy a FAN that will enable Hydro Ottawa to securely communicate to its existing and future field assets.

42. The excerpt goes on to address the gaps to be addressed; the transmission and other telecommunications facilities to be deployed; the goals and objectives of the project; and potential network architectures: *(i)* a "do-nothing" approach which would rely on existing MNOs "at the cost of reliability, security, and flexibility"; *(ii)* a "preferred" PVNO approach which, "[u]nfortunately ... is under regulatory review … and is not yet available in Canada and therefore, eliminated from further consideration"; *(iii)* PSBN usage, which is not recommended in view of the presence of many higher-priority public safety organisations; and *(iv)* hard-to-secure unlicensed radio.

43. The scope and scale of the intended investments in transmission facilities are notable. So is the fact that, of the four options presented, only the PVNO approach offers reliability, security, and flexibility without requiring the reconfiguration of relationships and traffic prioritization as between sectors, each with important needs to the public benefit of all Canadians.

44. The Hydro Ottawa example attached here is simply one that is at hand. The bottleneck we have described will only deepen. The CRTC, in our respectful submission, has a substantial opportunity in this proceeding to secure a "win" that will promote rural broadband deployment; foster the adoption of advanced, innovative wireless machine-to-machine applications at scale; and deliver safer, more secure, and more reliable services to Canadians in a period during which the need for them is deeper than ever.

45. We urge the Commission to seize that opportunity, which in our submission may be undertaken in a straightforward and abbreviated manner, as set out at paragraph 7 above. With electrical utilities and railways across Canada, we look forward to the Commission's decision on the limited but vital issues raised in our submissions.

Yours sincerely,

[transmitted electronically]

Francis Bradley
President and CEO
Canadian Electricity Association

Sol Lancashire
Manager—Telecom Engineering, BC Hydro
Chair, CEA Operating Technology & Telecommunications Committee

Justin Crewson
Director, Transmission and Distribution Policy
Canadian Electricity Association

*** End of Document ***