Re: Senate Standing Committee on National Security, Defence and Veterans Affairs review of Bill C-26, *An Act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other Acts*

Canadian Internet Registry Authority

Executive Summary

1. CIRA, the Canadian Internet Registration Authority, is pleased to participate in the Senate Standing Committee on National Security, Defence and Veteran Affairs' study of Bill C-26, *An Act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other Acts* ("Bill C-26" hereafter).

2. CIRA strongly supports the Government of Canada's objective to raise the baseline level of cybersecurity across critical cyber systems via Bill C-26. CIRA offers two constructive recommendations to Part 2 of Bill C-26 (the *Critical Cyber Systems Protection Act*, the "CCSPA" hereafter) to better align its cybersecurity objectives with oversight and information-sharing considerations.

   Recommendation 1: To enhance oversight, the CCSPA should require proposed cyber security directions to be reviewed by the Clerk of the Privy Council, in consultation with the Deputy Minister of Justice.

   Recommendation 2: To increase confidence in the proposed information-sharing enabled by the CCSPA, conditions on the use of the information should be strengthened.

3. CIRA's recommendations reflect its unique position as Canada's country code top-level domain (ccTLD)[1] registry[2] and as a cybersecurity provider. CIRA recognizes that the CCSPA gives the Governor in Council (GiC) the authority to add "vital services and vital systems" that are not currently enumerated in the draft legislation to Schedule 1.

4. As such, CIRA's recommendations would provide additional clarity and confidence to the "appropriate regulators" and "designated operators" as currently captured in the draft legislation, as well as any that are eventually brought into scope of the supporting framework.

About CIRA

5. CIRA is a not-for-profit organization best known for operating the .CA registry, with over 3.3 million domains under management. CIRA's mission is to build a trusted internet for Canadians. According

[1] A top-level domain (TLD) is one of the domains at the highest level in the hierarchical domain name system of the Internet (e.g., .COM, .ORG. .CA). A ccTLD is a top-level domain (TLD) that indicates the country or geographic location of the domain.
[2] A registry is the database of all domain names registered under a certain TLD.

to the NetBeacon Institute, .CA is one of the safest ccTLDs in the world.[3]

6. CIRA's core mandate is the safe, stable and secure operation of the .CA domain and its underlying technologies. We also connect, protect and engage the internet community in Canada and beyond by providing high-quality registry, DNS and cybersecurity services.

7. CIRA staff are active participants in multistakeholder fora to promote the security and resilience of the internet. Domestically, this includes the Canadian Forum for Digital Infrastructure Resilience (CFDIR)[4] and the Canadian Radio-television and Telecommunications Commission's (CRTC) Interconnection Steering Committee (CISC)[5] and, internationally, the Internet Corporation for Assigned Names and Numbers' (ICANN) Security and Stability Advisory Committee (SSAC).[6]

8. CIRA also provides cybersecurity services to keep Canadians safe online. These include:

    a. *CIRA DNS Firewall*: enterprise-level DNS protection for businesses, municipalities, education, healthcare institutions and other organizations, that protects millions of Canadians from malware, ransomware and other security threats.

    b. *CIRA Anycast DNS*: routing infrastructure that brings global content closer to end-users and keeps users safe by minimizing the impact of security threats.

    c. *CIRA Canadian Shield*: free cybersecurity service that protects millions of Canadians from online threats.

    d. *CIRA Cybersecurity Awareness Training*: an integrated courseware and phishing simulation platform that enables organizations to educate their staff to protect themselves from cyber risks like social engineering and ransomware.

9. CIRA partners with several institutions to keep these services up-to-date and Canadians safe online, including the Canadian Centre for Cyber Security, Canadian Centre for Child Protection, Internet

[3] NetBeacon, "MAP Report: August 2024", *NetBeacon,* Accessed October 10, 2024, https://netbeacon.org/wp-content/uploads/2024/08/MAP-Report-August-2024-.pdf.
[4] Canada, "Canadian Forum for Digital Infrastructure Resilience," Accessed October 30, 2024. https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/learn-more/committees-and-stakeholders/committees-and-councils/canadian-forum-digital-infrastructure-resilience-cfdir
[5] CRTC, "CRTC Interconnection Steering Committee (CISC)," Accessed October 30, 2024, https://crtc.gc.ca/eng/cisc-cdci.htm
[6] ICANN, "Security and Stability Advisory Committee," Accessed October 30, 2024, https://icann.org/group/ssac/

Watch Foundation and Mozilla Firefox.

Introduction

10. CIRA strongly supports the Government of Canada's objective to raise the baseline level of cybersecurity across critical cyber systems via Bill C-26. A trusted internet underpins Canadians' ability to participate in and contribute to Canada's economic, social and political well-being. CIRA supports initiatives by the Government of Canada to put cybersecurity measures and frameworks in place that enable all Canadians to better protect their data, devices and networks.

11. As a TLD registry and cybersecurity services provider, CIRA's data shows a growing volume and sophistication of cyber threats in Canada. In 2024, on CIRA's behalf, the Strategic Counsel surveyed 500 cybersecurity decisionmakers from Canadian organizations. The survey showed that 44% of Canadian organizations experienced a cyber-attack (attempted or successful) in the previous year.[7]

12. CIRA has long advocated for the importance of robust cybersecurity measures and frameworks on the part of governments and businesses.

13. Most recently, CIRA's President and CEO Byron Holland appeared at the House of Commons Standing Committee on Public Safety and National Security (SECU). Notably, CIRA and other witnesses advocated for enhanced transparency provisions, which were adopted by Parliamentarians and are now currently reflected in the legislation.

14. As such, CIRA's current recommendations to the CCSPA would provide additional clarity and confidence to the "appropriate regulators" and "designated operators" as currently captured in the draft legislation, as well as any that are eventually brought into scope of its supporting framework.

Recommendation 1: To enhance oversight, the CCSPA should require that proposed cyber security directions be reviewed by the Clerk of the Privy Council, in consultation with the Deputy Minister of Justice.

15. There have been notable changes made to the proposed Bill C-26 to improve oversight. The amendments outlining necessary considerations the Governor in Council (GiC) must make before

[7] CIRA, "2024 CIRA Cybersecurity Survey," Access October 30, 2024, https://www.cira.ca/en/resources/documents/cybersecurity/2024-cira-cybersecurity-survey/

making a compliance order in the revised cyber security directions ensures greater oversight on how mandatory directions are issued and enforced.[8]

16. While steps have been taken to increase oversight in the proposed legislation, as it is currently drafted, cyber security directions made under Section 20 would still be exempt from sections 3, 5 and 11 of the *Statutory Instruments Act* (section 22(1)).

17. The *Statutory Instruments Act* sets out the key facets of the regulation-making process. Section 3 of the *Statutory Instruments Act* outlines the process by which the Clerk of the Privy Council, in consultation with the Deputy Minister of Justice, examines proposed regulation to, among other things, ensure "it is authorized by the statute pursuant to which it is to be made" (section 3(2)(a)).

18. The checks and balances outlined in the *Statutory Instruments Act* provide oversight, accountability and transparency in the regulation-making process. Section 3 serves as a check that proposed regulations do not constitute any "unusual or unexpected use of authority" ((2)(b)) and do not "trespass unduly on existing rights and freedoms" ((2)(c)). By exempting these checks, the Act limits oversight, accountability and transparency in the regulation making process.

19. As a cyber security provider CIRA recognizes the need for discretion and timeliness in matters of national security and public safety, including in the issuance of cyber security directions. However, to further enhance public trust and confidence in the eventual framework, cyber security directions exemption from section 3 of the Statutory Instruments Act should be removed. Specific wording for this proposed amendment can be found below.

Current text of Section 22 (1) of the CCSPA
22 (1) An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the Statutory Instruments Act.
Proposed amendment to Section 22 (1) of the CCSPA:
22 (1) An order made under section 20 is exempt from the application of sections 5 and 11 of the Statutory Instruments Act.

[8] These changes can be found in more detail in the first reading and third reading *of Bill C-26 An Act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other Acts*, 44th Parliament, 2023, Part 2, para. 20-25.

Recommendation 2: To increase confidence in the proposed information-sharing enabled by the CCSPA, conditions on the use of the information should be strengthened.

20. There are several provisions in the CCSPA that allow for information-sharing between a range of persons and entities, without explicit delineation of bounds for this information-sharing.

21. For example, section 16 would empower appropriate regulators requesting advice, guidance or services in certain contexts from the Communications Security Establishment (CSE) to provide the CSE with certain information, including confidential information.

22. Section 23 would provide broad authority for the sharing of information disclosed pursuant to a cyber security direction issued.

23. This information could be shared with a range of persons or entities, including the Chief or an employee of the CSE, the Director or an employee of the Canadian Security Intelligence Service (CSIS) and “any other person or entity that is prescribed by the regulations.”

24. Though there may be indications of legislative intent, the CCSPA does not explicitly limit the use of information by recipients.

25. For example, the CSE Act articulates the Establishment’s five-part mandate, which, alongside cybersecurity and information assurance, includes foreign intelligence, defensive cyber operations, active cyber operations, and technical and operational assistance.

26. CIRA believes that the additional guardrails outlined below would mitigate concerns that CSE could use data collected under section 16 of the CCSPA to pursue aspects of its mandate other than cybersecurity and information assurance.

Amendment i)

Proposed amendment to section 16 of the CCSPA underlined:

(16) An appropriate regulator may provide to the Communications Security Establishment any information, including any confidential information, respecting a designated operator's cyber security program or any steps taken under section 15, for the purpose of requesting advice, guidance or services from the Communications Security Establishment in accordance with the cyber security and information assurance aspect of the mandate of the Communications Security Establishment as set out in section 17 of the CSE Act, in respect of the exercise of the appropriate regulator's powers or the performance of its duties and functions under this Act.

Amendment ii)

Proposed addition to section 23 of the CCSPA:

(23.1) Any information shared in accordance with section 23 can only be used by the recipient person for the purposes set out in section 5.

.

Conclusion

27. CIRA thanks the Senate Standing Committee on National Security Defense and Veteran Affairs for the opportunity to participate in its study of Bill C-26.

28. To re-iterate, CIRA offers two constructive recommendations to Part 2 of Bill C-26 ("CCSPA") to better align its cybersecurity objectives with oversight and information-sharing considerations.

    Recommendation 1: To enhance oversight, the CCSPA should require that proposed cyber security directions be reviewed by the Clerk of the Privy Council, in consultation with the Deputy Minister of Justice.

    Recommendation 2: To increase confidence in the proposed information-sharing enabled by the CCSPA, conditions on the use of the information should be strengthened.

29. Additional information or citations are available upon request.