Re: House of Commons Standing Committee on Public Safety and National Security's review of Bill C-26

Canadian Internet Registration Authority

Executive summary

1. The Canadian Internet Registration Authority (CIRA) is pleased to participate in the House of Commons' Standing Committee on Public Safety and National Security's study of Bill C-26, *An Act respecting cyber security, 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 three 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, information-sharing and transparency 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.

   Recommendation 3: To promote transparency, the CCSPA should be amended so that information on the cyber security directions issued in the year immediately prior are made public.

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.

[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.

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 to the DNS Abuse 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.

---

[3] DNS Abuse Institute, "A new phase of measuring DNS abuse," *DNS Abuse Institute*, Accessed June 19, 2023, https://dnsabuseinstitute.org/wp-content/uploads/2023/06/V3-FINAL-DNSAI-Compass-Report-Combined.pdf
[4] Canada, "Canadian Forum for Digital Infrastructure Resilience," Accessed June 19, 2023, 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 June 19, 2023, https://crtc.gc.ca/eng/cisc-cdci.htm
[6] ICANN, "Security and Stability Advisory Committee," Accessed June 19, 2023, https://www.icann.org/groups/ssac

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

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 2022, on CIRA's behalf, the Strategic Council surveyed over 500 information technology and cybersecurity decision-makers from Canadian organizations. The survey showed that 29% of surveyed organizations experienced a security breach in the year prior.[7]

12. CIRA has long advocated for the importance of robust cybersecurity measures and frameworks on the part of governments and businesses. During Public Safety Canada's recent consultation on the National Cyber Security Strategy, we recommended that the government: provide threat intelligence data to trusted cybersecurity service providers, continue to fund the adoption of cybersecurity technologies for organizations of all types, and work to educate Canadians on cyber risks.[8]

13. As such, CIRA's 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.

[7] The Strategic Council, "Perceptions and attitudes of Canadian organizations toward cybersecurity," Accessed June 19, 2023, https://static.cira.ca/2022-10/CIRA%202022%20Cybersecurity%20Report%20Aug%2031.pdf?VersionId=HP489japmgg3q8vDhTmwNEm2UaU8EGWs

[8] CIRA, "Protecting Canadians: renewing Canada's approach to cyber security," Accessed June 19, 2023, https://www.cira.ca/blog/state-internet/protecting-canadians-renewing-canadas-approach-cyber-security

14. As currently drafted, cyber security directions made under Section 20 of the proposed CCSPA would be exempt from sections 3, 5 and 11 of the *Statutory Instruments Act*.

15. 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)).

16. 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)).

17. CIRA recognizes the need for secrecy 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, the exception of cyber security directions 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.*

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

18. There are several provisions in the CCSPA that would allow for information-sharing between a range of persons and entities. 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.

19. In addition, section 23 of the CCSPA would provide broad authority for the sharing of information provided pursuant to a cyber security direction issued under section 20. 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."

20. Though there may be indications of legislative intent, the CCSPA does not explicitly limit how recipients use the collected information under these sections.

21. 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. CIRA is of the view it would not be appropriate for the CSE to use data collected under section 16 of the CCSPA for the purposes of pursuing aspects of its mandate other than the 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.

Recommendation 3: To promote transparency, the CCSPA should be amended so that information on the cyber security directions issued in the year immediately prior is made public.

22. Orders made under Section 20 of the CCSPA are exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*. Section 20's exemption from section 11 of the SIA exempts cyber security directions from being published in the *Canada Gazette*.

23. As outlined earlier, CIRA recognizes the need for some level of secrecy and timeliness in matters of national security and public safety. However, secrecy should be counter-balanced by the addition of provisions in the CCSPA that would promote some transparency around the issuance of cyber security directions.

24. Were the CCSPA to become law, this transparency would further public trust and confidence in the legislation and enhance appropriate regulators and designated operators' understanding of the legislation's implementation over time.

25. The CCSPA should be amended so that the number of cyber security directions issued the year immediately prior, along with other related information, is made public. Specific wording for this proposed amendment can be found below.

Proposed amendment to section 146 of the CCPSA underlined:

146 The Minister must, within three months after the end of each fiscal year, prepare a report on the administration of this Act for that fiscal year and cause a copy of the report to be laid before each House of Parliament on any of the first 15 sitting days of that House after the report is completed.

This report must outline:

(a) the number of cyber security directions issued in the immediately preceding year;
(b) the number of cyber security directions revoked in the immediately preceding year;
(c) the number of designated operators that received a cyber security direction in the immediately preceding year;
(d) the vital services and vital systems in respect of the designated operators that received a cyber security direction in the immediately preceding year.

Conclusion

26. CIRA thanks the House of Commons Standing Committee on Public Safety and National Security for the opportunity to participate in its study of Bill C-26.

27. To reiterate, CIRA offers three constructive recommendations to Part 2 of Bill C-26 ("CCSPA") to better align its cybersecurity objectives with oversight, information-sharing and transparency 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.

Recommendation 3: To promote transparency, the CCSPA should be amended so that information on the cyber security directions issued in the year immediately prior is made public.

28. Additional information or citations are available upon request.

29. CIRA respectfully requests to appear before the House of Commons Standing Committee on Public Safety and National Security in connection with its study of Bill C-26.