Re: Consulting on Canada's Approach to Cyber Security

Canadian Internet Registration Authority | August 19, 2022

Executive Summary

1) The Canadian Internet Registration Authority commends Public Safety Canada for its commitment to renew Canada's National Cyber Security Strategy (NCSS).

2) CIRA's comments on emerging cyber security issues and recommendations for the renewal of the Strategy reflect its role as (i) the .CA country-code top-level domain registry operator and associated domain name system, (ii) its experience in domestic and global internet governance and policy, and (iii) as a cyber security services provider.

3) CIRA believes that a robust cyber security ecosystem is necessary to protect Canadian citizens, institutions, the economy and society. In order to foster a trusted internet, Canadians must have cyber security awareness and protections in place to preserve data, devices and networks. Meaningful and effective cyber security measures necessitate that governments, industry leaders, civil society and individuals all play an active role.

4) CIRA calls for increased leadership and coordination from the Government of Canada, in particular around education, empowerment and funding for particularly vulnerable users, such as municipalities, universities and colleges, school boards, and health care organizations (i.e., the MUSH sector), SMEs, and individual Canadians.

5) Specifically, CIRA respectfully submits that:
    a) **The urgency for a strong, coordinated federal government response derives from how common networked technology has become in the lives of Canadians.** While some rightly look over the horizon at the threat potential from new or anticipated technologies like quantum computing or the metaverse, the fact is that the internet has already permeated every aspect of life, from light bulbs to the power grid. The NCSS must ensure that Canada is safe not just from criminals who target sophisticated critical infrastructure within strategic sectors of the economy, but also from those who see malicious opportunities in the most mundane transactions that comprise the daily networked lives of Canadians and Canadian institutions.

    b) **A renewed NCSS should place a priority on federally-coordinated collaboration, education and outreach**. The renewal of the NCSS is an opportunity to ensure a robust cyber security-aware ecosystem in which individual Canadians, Canadian businesses, and Canadian institutions are aware of the precise nature of cyber threats they face, and of the appropriate practices and tools available to protect their data, devices and networks. This is critically important with respect to sectors of the economy and society who do not typically think of themselves as being vulnerable or attractive to cyber criminals, such as hospitals, academia, civil society, and other charitable and not-for-profit organizations (in particular the MUSH sector) as well as individual Canadians.

c) **The NCSS should work to bolster security and resilience by monitoring, anticipating and addressing technical threats**.

- First, the Government can provide threat data to trusted cyber security service providers to raise the baseline level of cyber security across the country.
- Second, the Government should provide funds for the adoption of cyber security technologies by the MUSH sector and non-profits in particular.
- Third, the Government must work to educate individual Canadians on the risks they face and practical approaches to mitigate these.
- Fourth, the Government should establish a 'Canadian Internet Observatory' an independent, broadband policy think tank dedicated to promoting domestic internet infrastructure resiliency.

About CIRA

6) The Canadian Internet Registration Authority (CIRA) is a member-based, not-for-profit organization best known for managing the .CA country code top-level domain (TLD) on behalf of all Canadians. CIRA operates the .CA registry and associated .CA domain name system (DNS) network, with over 3.2 million domains under management. Our mission is to build a trusted Internet for Canadians. According to SpamHaus, .CA is one of the safest TLDs in the world, with an abuse rate consistently lower than 0.5 per cent, compared to an abuse rate of 3.6 per cent for .COM, for example.[1]

7) While CIRA's core mandate is the safe, stable, and secure operation of the .CA domain and its underlying technologies. The organization also connects, protects, and engages

[1] SpamHaus, "The World's Most Abused TLDs," *The SpamHaus Project*, Date Accessed June 08, 2022, https://www.spamhaus.org/statistics/tlds/

the internet community in Canada and beyond by providing high quality registry, DNS, and cyber security services.

8) 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)[2], and internationally, the Internet Corporation for Assigned Names and Numbers' (ICANN) Security and Stability Advisory Committee (SSAC).[3]

9) CIRA also provides several cyber security services to keep Canadians safe online. These include:

    a) *DNS Firewall*: our enterprise-level DNS protection for small businesses, municipalities, education, and healthcare institutions that protects over 3.1 million people from malware, ransomware and other security threats.

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

    c) *Canadian Shield*: our free cyber security service for Canadian families and personal devices that protects them from malware, phishing, and other scams. In 2021, Canadian Shield blocked over 30 million malicious domains from compromising Canadians' data, devices and networks.

    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.

10) CIRA partners with several institutions to keep these services up-to-date and Canadians safe online, including the Canadian Centre for Cyber Security (CCCS), the Canadian Centre for Child Protection and ScamAdviser.

11) CIRA also operates CIRA Labs, an innovation hub that develops new solutions to build a secure, trusted and accessible internet for Canadians both domestically and abroad. CIRA Labs researches and develops new technologies that: help increase the security

[2] Canada, "Canadian Forum for Digital Infrastructure Resilience," https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11618.html
[3] ICANN, "Security and Stability Advisory Committee," https://www.icann.org/groups/ssac

and resilience of the internet; mitigate and respond to cyber attacks; and support new network, data and security standards around the world. CIRA Labs has two active projects centered on Internet of Things (IoT) security: CIRA Secure IoT Registry and CIRA Secure Home Gateway.[4]

Introduction

12) While the internet is central to Canadian life and vital for the full participation in our economy, society and democracy, there are many opportunities for abuse and harm. CIRA commends the Department of Public Safety for its commitment to bolster Canada's cyber security ecosystem through the renewal of the NCSS.

13) CIRA's unique perspective on emerging cyber security issues and recommendations for the renewal of the NCSS are derived from the role CIRA plays in the operation of the domain name system (DNS) for the .CA TLD, CIRA's understanding of internet architecture, involvement in global fora for multistakeholder internet governance, CIRA's experience as a cyber security services provider, and from results gleaned from CIRA's annual Cybersecurity Survey.

14) CIRA believes that a robust cyber security ecosystem is necessary to protect Canadian citizens, institutions, the economy and society. Part of a trusted internet means having proper cyber security awareness and protections in place to protect Canadians' data, devices and networks. Meaningful and effective cyber security measures necessitate that governments, industry leaders, civil society and individuals all play an active role.

The urgency for a strong, coordinated federal government response derives from how common networked technology has become in the lives of Canadians.

15) While some rightly look over the horizon at the threat potential from new or anticipated technologies like quantum computing or the metaverse, the fact is that the internet has already permeated every aspect of Canadians' lives, from light bulbs to the power grid. The NCSS must ensure that Canada is safe not only from criminals who target sophisticated critical infrastructure within strategic sectors of the economy, but also from those who see malicious opportunities in the most mundane transactions that comprise the daily networked lives of Canadians and Canadian institutions.

[4] CIRA, "About CIRA Labs," Accessed July 28, 2022, https://www.cira.ca/labs

16) The exponential expansion of the interconnected devices to high-speed wireless networks, commonly referred to as the Internet of Things (IoT), while creating a world of possibilities for connectivity and efficiency, will represent a security risk commensurate to its expanding reach into all aspects of the Canadian economy. From wearables to smart-home devices to IoT networks in critical infrastructure, there will be an estimated 30 billion IoT devices by 2025.[5] Security scaling will be a large challenge given this growth projection.

17) Since 2019, CIRA has partnered with The Strategic Counsel to conduct a comprehensive, annual online survey of 500 cyber security decision-makers across Canada with the goal of identifying industry trends in perceptions and attitudes.[6] The survey found that:

- 95 per cent of survey respondents indicate that at least some of their COVID-19 related cyber security protections will be permanent.
- Of the 17 per cent of survey respondents that experienced a ransomware attack in 2021, 69 per cent of those say they paid the ransom.
- 64 per cent support legislation that would prohibit paying ransom demands.
- 36 per cent indicate that the number of cyber attacks has increased during the COVID-19 pandemic, up from 29 per cent saying so the previous year.
- 59 per cent of organizations have cyber security insurance coverage as part of their business insurance. 29 per cent have a cyber security-specific policy.
- Most organizations with cyber security coverage say their provider has increased premiums or requested new forms of proof of the corporate cyber security measures in place.

18) Further, in 2021, CIRA Canadian Shield blocked more than 36 million DNS requests to malicious domains for the more than 150,000 users that utilize its blocking service.[7] Botnets and ransomware have posed serious threats to Canadian networks.

[5] IoT Analytics, "State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT devices for the first time," https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

[6] CIRA, "2021 CIRA Cybersecurity Survey," https://www.cira.ca/resources/cybersecurity/report/2021-cira-cybersecurity-survey

[7] CIRA, "Q4 2021: CIRA Canadian Shield Insights," https://www.cira.ca/resources/cybersecurity/report/cira-canadian-shield-insights-q42021 Note that while CIRA Canadian Shield had more than 2 million users by the end of 2021, many of those utilize the "privacy" service, which provides a DNS resolver but does not block malware.

19) In October 2021, scam protection was added to Canadian Shield through a partnership with ScamAdviser.[8] From October to December, the scams most commonly blocked by Canadian Shield pertained to sites involved with cryptocurrencies. As cryptocurrencies rapidly evolve, expanding and exciting the public, so too does it capture the attention of cyber criminals, who made $14 billion from cryptocurrency scams in 2021.[9] This is one example of how emergent technologies create opportunities for malicious actors to exploit.

20) As the innovation of internet-enabled technologies progresses and interconnection increases, security risks will grow in parallel. To reap the full benefits these technologies present, Canadian cyber security must anticipate and address the security challenges posed by them to avoid the negative technological, social and economic consequences of cyber attacks.

21) Where virtually every consumer device with a processor is connected to the internet, each one represents a potential weak link or backdoor that can be exploited by bad actors to steal private data, send spam and introduce destructive malware into both home and business networks.

22) In addition to the IoT, the growing metaverse – in which private companies are creating a variety of digital worlds – presents new fronts in the fight to keep Canadians, their devices and networks safe. Cyber criminals are already exploiting the unknown and unregulated nature of the metaverse to exploit individuals and organizations.[10] Cyber security must expand as the metaverse scales up.

23) Market concentration among 'Original Equipment Manufacturers' or OEMs furthers the risk that malicious attacks will propagate across networks and devices. As the number of unique vendors of network equipment, processors and devices narrows because of marketplace developments or policy preferences, the increasing homogeneity in network operators' and internet users' choices of equipment increases the risk of automated and

[8] CIRA, "CIRA teams up with ScamAdviser to warn online shoppers against potential fraudulent sites," https://www.cira.ca/newsroom/canadian-shield/cira-teams-scamadviser-warn-online-shoppers-against-potential-fraudulent#:~:text=Today%2C%20CIRA%20is%20proud%20to,online%20scams%20and%20fraudulent%20websites.

[9] Ibid.

[10] Stu Sjouwerman, "Metaverse As The New Attack Vector and Other Security Headlines to Come in 2022," *Forbes,* https://www.forbes.com/sites/forbestechcouncil/2022/02/15/metaverse-as-the-new-attack-vector-and-other-security-headlines-to-come-in-2022/?sh=5276abb43d00
CIRA, "The cybersecurity dangers of the metaverse," https://www.cira.ca/blog/metaverse-cybersecurity

manual infections spreading to other devices and networks using a common operating systems (OS) or software.

24) Whereas in the past developers, operators and users could take some solace in the notion that an as-yet undetected exploit would by nature be reasonably limited to a narrow range of network operations or equipment, today these so-called 'zero-day exploits' have the potential to spread unchecked across entire network ecosystems, before they are detected and mitigated.

25) Already CIRA is seeing evidence of state-level attacks on individual Canadian businesses and institutions. While state-level cyber attacks have long been assumed to be targeted to another state, as network devices proliferate and permeate over the next decade, individual Canadians will be as vulnerable to sophisticated, coordinated and directed attacks as those in strategic sectors of the economy.

26) To be clear, emerging network technology and applications do bring with it a rise in cyber threats, but CIRA strongly submits that the more immediate threat (one requiring urgent government action) lies in how vulnerable small business and the MUSH sector already are to attacks on a scale previously experienced by government institutions and big business.

27) Small- and medium-sized enterprises (SMEs) and the MUSH sector are particularly vulnerable to cyber threats. Thirty-five per cent of security professionals in the MUSH sector stated that the number of cyber attacks they face increased during the pandemic.[11]

The renewed NCSS should place a priority on federally-coordinated collaboration, education and outreach

28) The renewal of the NCSS is an opportunity to ensure a robust cyber security-aware ecosystem in which individual Canadians, Canadian business, and Canadian institutions are aware of the precise nature of cyber threats they face, and of the appropriate practices and tools available to protect their data, devices and networks.

[11] CIRA, "2021 CIRA Cybersecurity Survey,"

29) The NCSS must address the particular vulnerabilities of critical infrastructure sectors. Many such providers, whether from the energy, telecommunications or transportation sector, are private organizations that operate without oversight of their cyber security practices, placing them, their customers and critical portions of Canada's economy at risk. CIRA recognizes that Bill C-26 could represent a first step in putting in place a regulatory framework to address this challenge, which should consider requirements such as cyber security standards and related reporting to ensure baseline cyber security practices are in place.

30) The NCSS, however, must go beyond to address sectors of the economy and society who do not typically think of themselves as being vulnerable or attractive to cyber criminals, such as hospitals, academia, civil society, and other charitable and not-for-profit organizations, as well as SMEs and individual Canadians.

31) CIRA recognizes that the regulation and oversight over these sectors rests largely with other levels of government, but submits that for this very reason, the Government of Canada must ensure the NCSS presents a coordinated and cohesive framework to protect not only federally regulated and/or strategic sectors of the economy, but those smaller economic and social segments and stakeholders who face threats beyond the scope of individual provinces or municipalities to address.

32) In particular, the Government of Canada should prioritize education and outreach to strengthen vulnerable sectors and equip individuals with the cyber skills needed to thrive in the 21st century.

33) For example, the CyberSecure Canada program which serves as the development of a national cyber security training certification program for SMEs could be expanded and promoted more heavily. As noted, many SMEs are underserved and unprepared when it comes to cyber security. The creation of a national cyber security awareness training and certification program would equip workers across Canada with a baseline cyber security knowledge, decrease the risk of adverse cyber events facing these organizations, and boost SMEs' cyber security posture country wide. As well, making the certification program transferable, would enable Canadian workers to carry the skills learned through the program with them throughout their careers.

34) Finally, the NCSS should work to bolster cyber security awareness and protection of individuals and households, particularly vulnerable individuals with a lower level of internet literacy. Especially in the age of hybrid and remote work, ensuring that individuals are properly protected against cyber threats and that they know how to practice proper cyber hygiene is a critical piece of the Canadian cyber security landscape that will make a world of difference for Canadian citizens and organizations.

A renewed NCSS should work to bolster security and resilience by anticipating and addressing technical threats.

35) The renewal of the NCSS presents a key opportunity to formalize the Government of Canada's role in addressing harmful technical threats, like botnets and malware.

36) The current NCSS and its accompanying Action Plan demonstrate a dearth of plans and initiatives to combat the most common technical threats facing Canadians today. For example, the word 'ransomware' does not appear in the current NCSS, despite numerous examples of disruptive and expensive ransomware attacks on Canadian hospitals, universities, businesses and individuals.

37) Public Safety Canada should look upon the NCSS as an opportunity to formalize a stronger, centralized coordination across federal departments and agencies, as well as other levels of government, to educate all Canadians on the need to identify, prevent and address cyber attacks, and in funding for the adoption of cyber security technologies to enhance network resilience and security awareness within the most vulnerable sectors of society and the economy.

- First, the Government can provide threat data to trusted cyber security service providers to raise the baseline level of cyber security across the country. Increased collaboration with industry and civil society to assess and address technical threats will boost the cyber security posture of Canadian households, organizations, and institutions.
- Second, the Government can provide funds for the adoption of cyber security technologies by the MUSH sector and non-profits, like how they are eligible expenses under the Canadian Digital Adoption Program (CDAP). Moreover, CIRA supports the continuation of CDAP to continue supporting the secure digitization of Canadian SMEs.

- Third, the Government of Canada should establish a ‘Canadian Internet Observatory’ an independent, broadband policy think tank dedicated to promoting domestic internet infrastructure resiliency. The observatory would focus on monitoring the overall health of Canada’s internet by coordinating data from the country’s network operators about network failures, cyber attacks, and other indicators of network health from a critical infrastructure perspective.

Conclusion

38) CIRA believes that a robust cyber security ecosystem is necessary to protect Canadian citizens, institutions, the economy and society. Part of a trusted internet means having proper cyber security awareness and protections in place to protect Canadians’ data, devices and networks. Meaningful and effective cyber security measures necessitate that governments, industry leaders, civil society and individuals all play an active role.

39) Accordingly, CIRA calls for increased leadership and coordination from the Government of Canada, in particular around education, empowerment and funding for particularly vulnerable users, such as the MUSH sector, SMEs, and individual Canadians. Cyber threats faced by the smallest, least commercial organizations, institutions and individuals are every bit as clear and present today as they are for the biggest businesses and organizations in so-called strategic sectors of the economy.

40) Therefore, CIRA reiterates that:

    d) **The urgency for a strong, coordinated federal government response derives from how common networked technology has become in the lives of Canadians.** While some rightly look over the horizon at the threat potential from new or anticipated technologies like quantum computing or the metaverse, the fact is that the internet has already permeated every aspect of life, from light bulbs to the power grid. The NCSS must ensure that Canada is safe from both criminals who target sophisticated critical infrastructure within strategic sectors of the economy, and those who see malicious opportunities in the most mundane transactions that comprise the daily networked lives of Canadians and Canadian institutions.

    e) **A renewed NCSS should place a priority on collaboration, education and outreach**. The renewal of the NCSS is an opportunity to ensure a robust cyber security-aware ecosystem in which individual Canadians, Canadian business, and Canadian institutions are aware of the precise nature of cyber threats they face, and of the appropriate practices and tools available to protect their data, devices and networks. This is critically important with respect to sectors of the economy and society who do not typically think of themselves as being vulnerable or attractive to cyber criminals, such as hospitals, academia, civil society, and other charitable and not-for-profit organizations (i.e. the MUSH sector).

f) **The NCSS should work to bolster security and resilience by monitoring, anticipating and addressing technical threats**.

- First, the Government can provide threat data to trusted cyber security service providers to raise the baseline level of cyber security across the country.
- Second, the Government can provide funds for the adoption of cyber security technologies by the MUSH sector and non-profits.
- Third, the Government must work to educate individual Canadians on the risks they face and practical approaches to mitigate these.
- Fourth, the Government should establish a ‘Canadian Internet Observatory’ an independent, broadband policy think tank dedicated to promoting domestic internet infrastructure resiliency.

41) CIRA appreciates the opportunity to provide its comments in this important proceeding.

*****End of Document*****