Written Submission for the Pre-Budget Consultation in Advance of the Upcoming Federal Budget

By: The Canadian Internet Registration Authority (CIRA)

October 8th, 2022

cira

- **Recommendation 1:** The government should dedicate $20 million annually to the development and operation of a ‘Canadian Internet Observatory’ – an independent, broadband policy think tank dedicated to developing mapping, routing and peering data to inform the planning of domestic internet infrastructure with a focus on maximizing resiliency and performance.
- **Recommendation 2:** The government should allocate a portion of funding from the newly established ‘Canadian Internet Observatory’ to conduct independent, third-party audits of all publicly funded broadband projects to ensure they meet the universal service objective prescribed by the Canadian Radio-television and Telecommunications Commission and offer Canadians a high degree of resiliency.
- **Recommendation 3:** The government should continue to fund the development of and promote uptake of programs like the CyberSecure Canada certification to train and certify Canada’s workforce with baseline cyber security skills.
- **Recommendation 4:** The government should promote online trust in public institutions by mandating the use of .CA domains for all federal government websites and fund the transition of non-.CA government websites to .CA domains.

About CIRA

The Canadian Internet Registration Authority (CIRA) manages the .CA top-level domain (TLD) on behalf of all Canadians and develops new, enterprise-level cyber security services such as CIRA DNS Firewall. The organization operates one of the fastest-growing country code top-level domains (ccTLD) in the world, a high-performance global domain name system (DNS) network and one of the world's most advanced back-end registry management solutions.

As a member-based, mission-driven not-for-profit, CIRA also has a goal to promote a trusted internet for Canadians. As part of this, the organization reinvests millions of dollars each year into projects like CIRA Canadian Shield, the CIRA Internet Performance Test and its annual $1.25M granting program, among others.

Recommendation 1: The government should dedicate $20 million annually to the development and operation of a 'Canadian Internet Observatory' – an independent, broadband policy think tank dedicated to developing mapping, routing and peering data to inform the planning of domestic internet infrastructure with a focus on maximizing resiliency and performance.

There is currently no single body in Canada tasked with studying the topography of Canada's networks, nor the risks of internet infrastructure failure at the national level. Telecommunications service interruptions are top of mind for Canadians affected by the nationwide Rogers outage in July, or Hurricane Fiona in September, where emergency, commercial and government services became inaccessible to millions of organizations and individuals across the country.

In January 2020, the Broadcasting and Telecommunications Legislative Review (BTLR) panel issued recommendations for modernizing the legislation governing Canada's communications sector. The report encourages the government to play an active role in studying Canada's internet infrastructure. For example, the panel encourages the government to develop, "…databases related to the functioning and location of telecommunications networks," and to facilitate "…the promotion of the security and reliability of telecommunications networks," among several others. Taken together, seven of the recommendations underscore a need for the government to closely study the architecture of Canada's internet.[1]

In response, CIRA submits that the Government of Canada should dedicate $20 million annually to the development and operation of a 'Canadian Internet Observatory' focused on improving knowledge of the Canadian internet by studying the infrastructure and technologies critical to its functioning. The observatory's research outputs would provide much-needed public resources for understanding Canada's internet and promoting its resiliency.

The observatory would focus on, for example: (i) collecting internet traffic paths (traceroutes) between Canadian networks and key internet resources to identify weaknesses or inefficiencies, including the evolution of peering among networks within Canada; (ii) mapping the deployment of fibre optic networks to help coordinate new broadband projects, improve redundancy and identify single points of failure; and (iii) 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.

CIRA submits that the creation of such an observatory would provide the public, decision-makers and network operator stakeholders at all levels with the best information possible to steward the deployment of new network facilities (including next-generation 5G networks) and manage risks facing Canada's internet infrastructure.

Recommendation 2: The government should allocate a portion of funding from the newly established 'Canadian Internet Observatory' to conduct independent, third-party audits of all publicly funded broadband projects to ensure they meet the universal service objective prescribed by the Canadian Radio-television and Telecommunications Commission and offer Canadians a high degree of resiliency.

In 2016, the Canadian Radio-television and Telecommunications Commission (CRTC) declared broadband internet a basic service and established a universal service objective that each Canadian should have access to. The CRTC specified that users should have access to speeds

[1] See recommendations 22, 23, 26, 45, 47, 48 and 86. Broadcasting and Telecommunications Review Panel, Canada's communications future: Time to act. (Ottawa: Innovation, Science and Economic Development Canada). <https://www.ic.gc.ca/eic/site/110.nsf/eng/00012.html> accessed July 26, 2021.

of 50 megabits per second (Mbps) download speed, 10 Mbps upload speed, and set minimum thresholds for other performance metrics including latency, packet loss and jitter – and emphasized that these speeds are “to be the actual speeds delivered, not merely those advertised.”

Canada must bridge a significant digital divide before it can achieve this objective. CRTC data shows that only 54.4 per cent of rural households have access to speeds that meet the Commission’s objective.[2] Similarly, data from CIRA’s Internet Performance Test shows that residents of urban areas receive speeds that are, on average, 3.8 times faster than those experienced by rural residents.

As of Budget 2022, the Government of Canada has committed $2.75 billion to the construction of high-speed internet projects across the country through its Universal Broadband Fund (UBF), which aims to connect 98 per cent of Canadians to the CRTC’s minimum standards by 2026.

CIRA supports this investment and submits that its impact can be optimized through independent, post-construction performance audits of broadband projects that receive public funding. Audits can help maximize return on public investment and ensure Canadians receive the network performance they are promised.

Presently, there are no post-construction testing requirements to ensure that UBF projects deliver on their promised performance, or that they meet the CRTC’s universal service objective. Failure to test whether a given broadband project’s real-world speeds meets the CRTC’s universal service objective means that residents in currently underserved areas may not receive the performance they were promised from a completed UBF-funded project.

Thus, CIRA recommends that the government dedicate a portion of the $20 million annual budget for the newly-created ‘Canadian Internet Observatory’ to independent, third-party assessments of publicly funded projects to ensure they meet the CRTC’s universal service objectives. This would help evaluate whether the advertised speeds promised by internet service providers are actually delivered to end users and ensure that government and taxpayers receive maximum return on their investment.

[2] Canadian Radio-television and Telecommunications Commission. Current trends - High-speed broadband. <https://crtc.gc.ca/eng/publications/reports/PolicyMonitoring/ban.htm> accessed September 23, 2022.

Recommendation 3: The government should continue to fund the development of and promote uptake of programs like the CyberSecure Canada certification to train and certify Canada's workforce with baseline cyber security skills.

The Canadian Centre for Cyber Security (CCCS) warns that the COVID-19 pandemic presents a heightened security risk for Canadian organizations.[3] Similarly, CIRA's 2022 Cybersecurity Survey shows that data breaches in Canadian organizations have nearly doubled since 2020.

Unfortunately, small and medium-sized businesses (SMBs) and their employees are notoriously underserved and unprepared when it comes to cyber security. These vulnerabilities were exacerbated by the pandemic; as lockdowns took hold and SMBs were forced to suddenly accommodate remote work, few were set up to operate fully remote with strong cyber security practices or trained staff in place. We expect many of these gaps to persist as workplaces maintain hybrid in-office/remote work environments.

No organization is immune to cyber threats. Despite this, cyber security awareness training for organizations and their employees is at best inconsistent across all sectors of the economy. In its "Baseline Cyber Security Controls for Small and Medium Organizations" handbook, the CCCS recommends cyber security best practices for SMBs. These include providing employees with cyber security awareness training and deploying software firewalls to protect the organization from DNS-based cyber attacks, among others.[4]

CIRA submits that the government should continue to fund the development of and promote uptake of programs like CyberSecure Canada. These cyber security awareness training programs are a key means of equipping workers across Canada with a baseline cyber security knowledge following the CCCS's best practices. CIRA was pleased to see recently proposed changes to the CyberSecure Canada program to introduce three new organizational and two new baseline controls. Programs like CyberSecure Canada will require continued support to keep pace with the constantly evolving nature of cyber threats.

[3] Canadian Centre for Cyber Security. Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity. (Ottawa: Canadian Centre for Cyber Security). <https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threatactivity> accessed July 27, 2021.

[4] Canadian Centre for Cyber Security, Baseline Cyber Security Controls for Small and Medium Organizations. (Ottawa: Canadian Center for Cyber Security) <https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-mediumorganizations> accessed July 27, 2021.

Employers could also indicate that new staff must obtain the certification prior to hiring, if permitted by the programs themselves. Moreover, the credential should be transferable—a certification employees can take with them throughout their career.

Recommendation 4: The government should promote online trust in public institutions by mandating the use of .CA domains for all federal government websites and fund the transition of non-.CA government websites to .CA domains.

During the pandemic, the CCCS has removed thousands of fraudulent Canadian government websites, emails and apps that have taken advantage of the COVID-19 pandemic by trying to compromise Canadians' finances or personal information. In some cases, the fraudulent sites pretended to be the Canada Revenue Agency, or the Public Health Agency of Canada.[5]

To help mitigate this, CIRA recommends that the government mandates the use of .CA domains consistently across all federal websites and set aside funding to facilitate the transfer of Government of Canada websites from non-.CA websites to .CA domains. For example, websites like cppib.com should be transferred to .CA domains to make it clear that they are Government of Canada websites, and thus, are secure and trustworthy.

The .CA TLD is a safe, secure and reliable domain, with one of the lowest incident rates for distributing spam, malware and other threats. Mandating .CA as the official TLD of the Canadian government should provide internet users with a new way to understand whether a government website is legitimate, trusted and secure.

Conclusion

CIRA thanks the members of the House of Commons Standing Committee on Finance for the opportunity to contribute to its consideration of recommendations for Budget 2023.

Additional information or citations are available upon request.

[5] Burke, David. 'Fake COVID notification apps and websites aim to steal money and personal data', CBC News (2021), online: https://www.cbc.ca/news/canada/novascotia/covid-apps-phones-scammers-fraudulent-personal-data-1.5877496