June 10, 2022

The Honourable Jim Carr
Member of Parliament and Chair
Standing Committee on Public Safety and National Security

BlackBerry Limited is grateful for the opportunity to submit a brief on securing Canada's critical infrastructure from cybersecurity threats to the Standing Committee on Public Safety and National Security (SECU).

BlackBerry is a world leader in cybersecurity and IoT security.
For over 35 years, BlackBerry has invented and built trusted security solutions to give people, governments and business the ability to stay secure and productive. Today, our software is used to protect all G7 governments, is embedded in more than 195 million cars, and secures more than 500 million devices including mobiles, laptops, transportation, energy, medical, aerospace and defence systems.

Canada's Critical Infrastructure Sector is Ill-prepared for Cyber Attacks
Drawing on this expertise and BlackBerry's unwavering commitment to safety, security and data privacy, I would like to draw SECU's attention to the gap that currently exists between the cybersecurity preparedness of Canada's critical infrastructure to growing cyber threats. Every organization, in every industry sector, runs the risk of a cyber breach. However, few carry the same real-world risk from cyberattacks as those in the critical infrastructure sector.

Studies indicate that ransomware attacks on transportation infrastructure in North America (just one aspect of our critical infrastructure, and one category of cyberattacks) increased by 186 percent[1] between June 2020 – June 2021. This threat will only grow as our critical infrastructure increasingly relies on software and connected technology to power and support their operation.

Currently, apart from PIPEDA related obligations, Canada has no regulations in place to govern – much less obligate – critical infrastructure operators and owners to report, prepare for, and prevent cybersecurity incidents. While there is a regulatory obligation for port administrations, marine and ferry facilities to report cyber incidents to law enforcement and Transport Canada, there is no specific reporting period, and there is no guidance on the cybersecurity measures that they should put in place. The cyber attack on Newfoundland and Labrador's[2] healthcare system should be a wake-up call to authorities in Canada that raising the bar on cybersecurity protection for critical infrastructure should be made a national priority.

[1] Ontario Trucking Association, *Trucking Faces Rise in Cyberattacks: Report*, Dec. 10, 2021, https://ontruck.org/trucking-faces-rise-in-cyberattacks-report/
[2] CBC, "N.L. health-care cyberattack worst in Canadian history, says cybersecurity expert," Nov. 4, 2021: https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyber-attack-worst-canada-1.6236210

Canada is falling behind our G7 Peers on Cyber

In the wake of successive cyber attacks on US critical infrastructure (e.g., Colonial Pipeline attack[3], the SolarWinds crisis[4], the attack on Microsoft Exchange[5], the attack on meat supplier JBS[6], the New York Subway system[7]), the U.S. President Biden move swiftly to raise the bar on cybersecurity to critical infrastructure. This included issuing an Executive Order on Improving the Nation's Cybersecurity[8] in May 2021, which mandated preventive cybersecurity measures such as the implementation of a Zero Trust Architecture across US government agencies and measures to strengthen the security of the government's software and IT supply chain. In July 2021, President Biden also directed his government to develop cybersecurity performance goals for critical infrastructure owners and operators. In April 2022, President Biden signed into law the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, requiring covered critical infrastructure entities to report cybersecurity incidents to government within 72 hours, and ransomware payments within 24 hours. Europe has similar requirements for Critical Infrastructure owners and operators under the Network and Infrastructure Security Directive. It also plans to levy fines of up to €10M or 2 percent of annual revenue (whichever is greater), to those that are found non-compliant.

Businesses and industry groups in Canada have been raising concerns about the ever growing[9] set of cyber threats[10] to Canada. They have called on the government[11] to invest in cybersecurity at a level on par with Canada's G7 peers. Canada's G7 peers, including the U.S., the U.K. and European governments – are investing nearly double what Canada spends on cybersecurity on a per capita basis to secure infrastructure and bolster their economies (See Tables 1 and 2). Canada simply cannot afford to leave our critical infrastructure, much of which is owned and operated by the private sector and other levels of government, exposed to cyber threats.

[3] Clifford Krauss, "Colonial Pipeline chief says an oversight let hackers into its system." The New York Times, June 8, 2021: https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html

[4] CISA, "Advanced Persistent Threat Compromises Government Agencies, Critical Infrastructure, and Private Sector Organizations." Dec. 17, 2020. https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html

[5] Kate Conger and Sheera Frenkel, "Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China." The New York Times, March 6, 2021: https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html

[6] Tom Polansek and Jeff Mason, "U.S. says ransomware attack on world's largest meatpacker likely from Russia," Reuters, June 1, 2021: https://www.ctvnews.ca/business/u-s-says-ransomware-attack-on-world-s-largest-meatpacker-likely-from-russia-1.5451709

[7] The Associated press, "New York transit officials confirm cyberattack: say harm limited." June 2, 2021: https://www.ctvnews.ca/sci-tech/new-york-transit-officials-confirm-cyberattack-say-harm-limited-1.5453569

[8] White House, "Executive Order on Improving the Nation's Cybersecurity." May 12, 2021: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[9] Max Fisher, "Constant but Camouflaged, Flurry of Cyberattacks Offers Glimpse of New Era," The New York Times, July 20, 2021: https://www.nytimes.com/2021/07/20/world/global-cyberattacks.html?searchResultPosition=1

[10] BlackBerry, "BlackBerry Uncovers Massive Hack-For-Hire Group Targeting Governments, Businesses, Human Rights Groups and Influential Individuals." October 7, 2020: https://www.blackberry.com/us/en/company/newsroom/press-releases/2020/blackberry-uncovers-massive-hack-for-hire-group-targeting-governments-businesses-human-rights-groups-and-influential-individuals

[11] Canadian Chamber of Commerce, Cyber Right Now: https://chamber.ca/campaign/cyber-right-now/?doing_wp_cron=1635977179.8352680206298828125000

Table 1: Cyber Funding for Civilian Agencies - selected G7 peers (Excludes Defence)

Country	Funding for Cyber
United States	C$10.95B (Source[12])
United Kingdom	C$4.45B (National Cyber Strategy[13])(Spending Review[14]) – £2.6B
France	C$1.43B (Source[15]) – €1B
Canada	CA$875.2M (Federal Budget 2022[16])

Table 2: Per Capita spending on Cyber base on Table 1 budgets

Country	Per Capita Funding for Cyber
United States	C$34.22
United Kingdom	C$52.66
France	C$37.05
Canada	C$23.03

Cybersecurity must be a priority for Government, Critical Infrastructure Owners and Operators, and Canadian Businesses

Addressing cybersecurity shortfalls is a high priority for Canadians. Notably, falling victim to a cyber attack now ranks second behind job loss on the list of things Canadians worry about most,[17] according to the 2021 Edelman survey. The federal government's chief of the Communications Security Establishment (CSE), Shelly Bruce has gone on record[18] stating that cybercrime is the "most prevalent, most pervasive threat to Canadians and Canadian businesses." This perspective is backed by evidence. Canadian businesses[19], hospitals[20], universities[21], transit[22] systems, cities[23] and government services[24] all have experienced significant cyber attacks[25].

[12] The White House Office of Management and Budget, "Budget of the U.S. Government: Fiscal Year 2022." https://www.whitehouse.gov/wp-content/uploads/2021/05/budget_fy22.pdf

[13] HM Government, "National Cyber Strategy 2022." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

[14] HM Government, "Autumn Budget and Spending Review 2021." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043688/Budget_AB2021_Print.pdf

[15] Gouvernement de France, "Un plan à 1 milliard d'euros pour renforcer la cybersécurité." https://www.gouvernement.fr/actualite/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite

[16] Government of Canada, "Budget 2022." https://budget.gc.ca/2022/report-rapport/toc-tdm-en.html

[17] Edelman, *2021 Edelman Trust Barometer* https://www.edelman.com/trust/2021-trust-barometer

[18] Mike Lapointe, "We Must Make Canadian Cyberspace a Harder Target,' says CSE Chief." The Hill Times, May 31, 2021. https://www.hilltimes.com/2021/05/31/we-must-make-canadian-cyberspace-a-harder-target-says-cse-chief/298987

[19] The Associated Press, "Major ransomware attack aimed at tech provider leaves other companies scrambling." July 4, 2021: https://www.cbc.ca/news/world/cyberattack-ransomware-kaseya-1.6089578

[20] Maria Sarrough, Megan Ogilvie, " Cyberattack leads to computer system failure at Humber River Hospital, impacting patient care." Toronto Star, June 15, 2021: https://www.thestar.com/news/gta/2021/06/15/computer-system-failure-at-humber-river-hospital-impacts-patient-care.html

[21] Alex Coop, "York University cyber attack looks like ransomware, says security expert." IT World Canada, May 6, 2020: https://www.itworldcanada.com/article/york-university-cyber-attack-looks-like-ransomware-says-security-expert/430370

[22] Ben Spurr, " TTC begins restoring systems after suspected cyber attack," Toronto Star, Nov. 1, 2021: https://www.thestar.com/news/gta/2021/11/01/fallout-from-suspected-cyber-attack-hits-ttc-for-fourth-day-while-agency-stays-silent.html

[23] Laura Lyall, "Hackers demanded $17 million worth of bitcoin as ransom from city of Saint John," CTV News, April 1, 2021: https://atlantic.ctvnews.ca/hackers-demanded-17-million-worth-of-bitcoin-as-ransom-from-city-of-saint-john-1.5372347

[24] Colin Freeze, "Newfoundland cyberattack an 'alarm bell' for Canada," The Globe and Mail, November 1, 2021: https://www.theglobeandmail.com/canada/article-newfoundland-cyberattack-an-alarm-bell-for-canada/

[25] Ian Austen, "As Hackers Take Down Newfoundland's Health Care System, Silence Descends." The New York Times, November 12, 2021: https://www.nytimes.com/2021/11/12/world/canada/newfoundland-cyberattack.html

BlackBerry was pleased to see the recent announcement[26] by Minister Marco Mendocino regarding new legislation that will "establish a framework to better protect the systems vital to our national security" particularly in finance, energy telecommunications and transport sectors. However, it is critical that these measures be applied to **all of Canada's critical infrastructure sectors**, including sectors that are currently not designated critical infrastructure such as Education and Research; Space and Emergency Services.

Cyber Attacks can be Prevented

Preventing cyber attacks requires putting in place robust cybersecurity resilience. At a minimum SECU should consider recommending that CI operators do the following:

1. **Put in place measures that have proven to mitigate cyber risks and incidents**. These include
    a. Undertaking continuous diagnostics of vulnerability and compromise;
    b. Developing cybersecurity readiness assessments and incident response plans;
    c. Designating a cybersecurity coordinator to oversee cyber investments and workloads;
    d. Adopting a Zero Trust security model that requires continuous authentication for all users and devices - including users inside the network perimeter; a constant monitoring of threats and risks; and dynamic cyber policy adaptation to the evolving cybersecurity landscape.
2. **Proactively sharing information on cybersecurity risks and incidents** with government and other CI operators/owners. CI operators/owners should notify cybersecurity risks and incidents in a timely manner (i.e. within 72 hours);
3. **Ensure that CI operators/owners deploy mature AI/ML-driven cybersecurity technologies** that:
    a. Proactively and continuously protect CI systems, networks, devices and organizations from malware based on AI/ML models that have been trained for years and on billions of files (good and bad);
    b. Can be installed on any operating system (Linux, Windows etc.)and device types (desktops, mobiles); and
    c. Are capable of preventing malware from executing regardless of connectivity status to the Internet (i.e., in connected and unconnected (offline/air gapped) environments). This is critical for CI systems, many of which are disconnected.

4. **Strengthen the security of software used to operate our critical infrastructure.** The software supply chain involves a complex web of dependencies with numerous third-party developers and components. In many cases, critical infrastructure operators have little knowledge of the software components that are embedded in their control systems. To that end the Government should:
    a. **Require manufacturers of software used in CI to create a Software Bill of Materials[27] (SBOM) so that operators can monitor software components for vulnerabilities.** An SBOM will help operators easily identify and respond to new security risks, decommission products that run software that are no longer supported by the supplier (i.e. Windows XP), make code easier to review, and help operators avoid blacklisted components that have a history of security, performance or reliability issues. This

[26] Catherine Tunney, Richard Raycraft, "Canada bans Chinese tech giant Huawei form 5G network," CBC, May 19 , 2022, https://www.cbc.ca/news/politics/huawei-5g-decision-1.6310839

[27] National Telecommunications and Information Administration, "Software Bill of Materials." https://www.ntia.gov/SBOM

requirement will be an invaluable tool[28] for managing cybersecurity and software supply chain risk and will help developers and operators uncover vulnerabilities baked into CI software that malicious actors can exploit. An SBOM will help CI owners/operators easily identify and respond to new security risks, decommission products that run software that are no longer supported by the supplier (i.e. Windows XP), make code easier to review, and help CI owners/operators avoid blacklisted components that have a history of security, performance or reliability issues. This is important because by some accounts, the average software application depends on more than 500 open source libraries[29] and components. Experts indicate that more than 90 percent[30] of commercial applications contain outdated or abandoned open source components. As the Government of Canada invests billions of dollars in next generation infrastructure, connected transport infrastructure, smart cities, smart grid technology, EV charging stations and EV infrastructure – an SBOM will be a critical tool to ensure the security of our infrastructure.

Canada should improve its governance of cyber risks

As it stands today, cyber responsibilities in the Federal Government are distributed across at least 12 Federal departments and agencies. Creating coherence across government to ensure that all departments operate with a unity of effort and purpose is essential to fostering cyber resilience. The US appointed its first White House National Cyber Director in July to serve as the President's principal advisor on cybersecurity and the UK has a Parliamentary Under Secretary of State for Digital and Broadband who is responsible for cybersecurity and cyber skills. **Canada should consider stablishing a Cabinet position responsible for ensuring government-wide coherence and action on cybersecurity**. Such a position in Canada would send a strong signal that Canada is serious about cybersecurity and foster cyber resilience by enhancing coherence and collaboration across government on cybersecurity policy and action.

Canada should also act to enhance public-private sector collaboration to prevent cyber attacks. This can be done by establishing a Canadian Cybersecurity Collaborative that is mandated to bring together private and public sector actors to proactively plan and respond to cybersecurity related threats and incidents. In 2021, the US Congress authorized the creation of the Joint Cybersecurity Defense Collaborative. This entity, housed within the Cybersecurity and Infrastructure Security Agency, is mandated to "lead collaborative, public-private sector cyber defense planning, cybersecurity information fusion, and the purposeful dissemination of cyber defense guidance to reduce cyber risk to and increase the resilience of National Critical Functions in the United States. This entity has proven effective, particularly in the wake of the crisis in Ukraine in enhancing information sharing and public-private collaboration on cybersecurity. These efforts have been bolstered by high-level meetings on cybersecurity convened by the White House. In August 2021, President Biden convened U.S. business and education leaders for a White House Cybersecurity Summit, which underscored the importance of close collaboration between government and industry on Infrastructure cybersecurity. This was followed by a second White House meeting with private sector actors on Software Security in January 2022 and a third in May 2022 on open-source software security. In the same way, the Canadian Government should

[28] See National Telecommunications and Information Administration, "Software Bill of Materials: Transparency in the Software Supply Chain," January 26, 2021: https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_energy_jan2021overview_0.pdf

[29] Robert Lemos, "Dependency Problems Increase for Open Source Components," Dark Reading, April 14, 2021: https://www.darkreading.com/application-security/dependency-problems-increase-for-open-source-components/d/d-id/1340665

[30] Security, "Synopsys Study Shows 91% of Commercial Applications Contain Outdated or Abandoned Open Source Components." May 12, 2020: https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-of-commercial-applications-contain-outdated-or-abandoned-open-source-components

consider convening government and private sector stakeholders to discuss opportunities to strengthen collaboration on cybersecurity. Through a Canadian Cyber Summit convened by the Prime Minister, for example, Canada could leverage the deep expertise and talent of Canada's private sector to explore how to collectively raise the bar on cybersecurity in our country.

SECU can act now to help infrastructure operators and owners prioritize cybersecurity investments to **prevent infrastructure from being compromised by cyberattack**. Cybersecurity is essential to sustaining innovation and securing trust in a digital and data-driven world. It is core to ensuring our national and economic security.

BlackBerry welcomes the opportunity to elaborate on these ideas and to continue collaborating with the Government of Canada to ensure that we remain secure and prosperous.

Sincerely,

John de Boer
Senior Director, Government Affairs and Public Policy
BlackBerry Limited