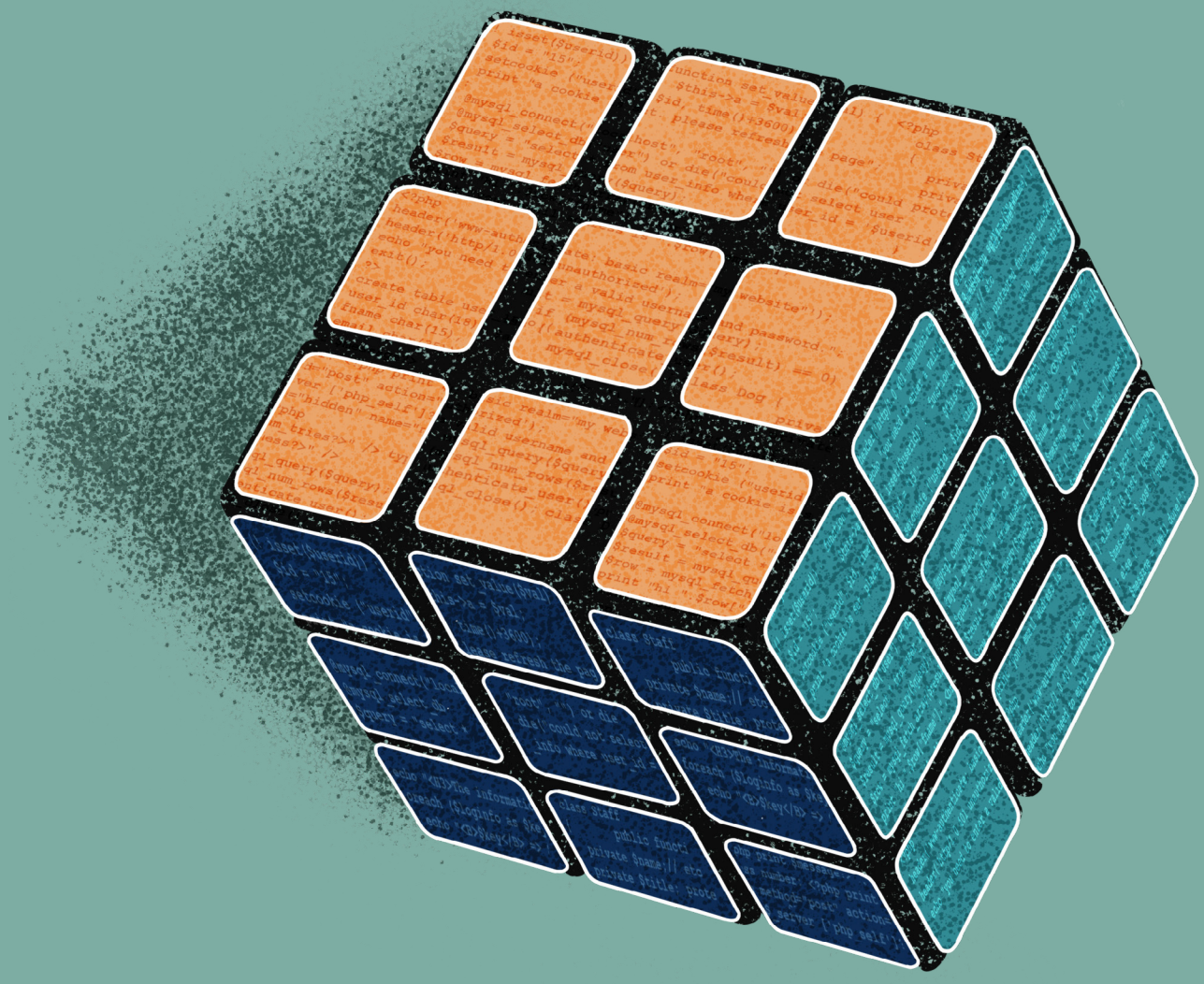

CPX Submission to the Government of Canada's Consultation on the National Cyber Security Strategy

cybersecure policy exchange
Powered by RBC

Toronto Metropolitan University

CPX Submission to the Government of Canada's Consultation on the National Cyber Security Strategy

The Cybersecure Policy Exchange (CPX) is an initiative of Toronto Metropolitan University (TMU), jointly led by the Rogers Cybersecure Catalyst and the Leadership Lab. Powered by RBC, CPX is dedicated to advancing effective and innovative public policy in cyber security and digital privacy.

We welcome the opportunity to contribute to the Government of Canada's public consultation on Canada's National Cyber Security Strategy (the "Strategy"), both regarding renewal of the Strategy and emerging issues on the medium- and long-term horizon. The Mid-Term Review of the 2019-2024 Strategy was useful in providing context and analysis that has helped guide our input.

Our submission responds to most of the consultation questions, focusing on the issues that CPX has examined through our policy research, cyber ecosystem engagement, and education and training activities. We have tried to be as clear and concise as possible in providing input and actionable recommendations, while providing links and guidance to our CPX research and analysis products for more in-depth review.

Goal 1: Secure and Resilient Canadian Systems

1. What concerns do you have related to cyber security, cybercrime, etc.? How can the Government of Canada help you to better protect yourself, your family, and your organization, if applicable?

Cyber Security of Critical Infrastructure

The health and livelihood of Canadians depend on the uninterrupted functioning of our critical infrastructure systems such as energy, water and transportation. The proposed *Critical Cyber Systems Protection Act* through Bill C-26 is a welcome move toward a clear framework to require federally-regulated operators of critical infrastructure to implement cyber security programs, mitigate supply-chain and third-party risks, immediately report cyber security incidents and comply with government directives, and puts in place significant fines for non-compliance. It also creates a framework for businesses and government to confidentially exchange information about vulnerabilities, risks and incidents.

We anticipate that the government will be consulting on the bill's regulations should this become law, including the timeline for mandatory incident reporting. Canada's bank regulator recently modified its incident reporting timeline from 72 to 24 hours, which we believe should be considered. We would also urge greater clarity on the transparency and oversight of these fairly sweeping powers, such as review through the National Security and Intelligence Review Agency.

Our research (see CPX report Secure Smart Cities: Making Municipal Critical Infrastructure Cyber Resilient) found that Canadian municipalities are struggling to find the guidance, funding, and staff necessary for protecting their critical infrastructure from cyber threats. Since provincial and territorial governments are responsible for regulating municipal water, energy and transportation services, provinces have a major role to play in advancing the cyber resilience of the municipal critical infrastructure in their jurisdictions. Despite this, we found a significant absence of provincial regulations and guidance that require municipalities to put cyber resilience measures in place for the critical infrastructure that they manage.

The Government of Canada should prioritize its continued efforts to work with provinces to develop strategies for strengthening the cyber security of critical infrastructure under their purview. We also recommend new and sustainable investment schemes to support municipal critical infrastructure owners and operators in their cyber security efforts, which can include prioritizing cyber security when providing federal funding for new infrastructure.

Implementing a Coordinated Vulnerability Disclosure program in Canada

Security flaws in digital systems used by governments, public institutions and critical infrastructure can have far-reaching impacts — and many cyber security researchers want to help. However, the Government of Canada is falling behind its global peers by failing to provide clear guidelines and reporting structures for cyber security researchers who disclose security flaws they find in the government's digital systems. Our research (see CPX report See Something Say Something: Coordinating the Disclosure of Security Vulnerabilities in Canada) shows that while 60 percent of G20 member countries have distinct and clear processes for reporting security vulnerabilities in public infrastructure, Canada does not — ultimately putting the Government of Canada, security researchers, and the general public at greater risk of harm.

Bill C-26 is a promising step forward. This is because it would require institutions to identify and manage "cyber security risks" as one high-level requirement to better ensure the security of federally-regulated vital systems and infrastructure, such as those used for transportation, energy and banking. However, significant legal risks remain in Canada for cyber security researchers who find and disclose information about security flaws. More than this, Bill C-26 in its current state leaves it unclear whether institutions should — or are required to — implement coordinated vulnerability disclosure (CVD), which is an explicit part of the backbone of the requirements for organizations set out in the EU's NIS 2.0. In this way, Canada may be falling behind its global peers by failing to account for CVD in its legal frameworks.

A cybersecure Canada requires working with experts who identify the security risks faced by our institutions and infrastructure, and providing them the legal protections and disclosure pipelines they need to do their vital work. Bill C-26 represents an opportunity for Canada to implement a policy framework that provides increased legal clarity for security research and vulnerability disclosure that occurs in good faith. The Government of Canada should consider strengthening its internal and external disclosure procedures for vulnerabilities involving federal computer systems. Canada should move towards an approach that facilitates transparent and accountable procedures when it handles disclosed vulnerabilities.

Addressing Online Harms including Crimes such as Cyber Fraud

Both the Strategy and Mid-Term Review note that advances in information and communication technologies have enabled more and more people to connect and communicate through a plethora of electronic services. As our day-to-day lives continue to migrate online, we increasingly open ourselves to various risks. CPX research on Canadians' use and opinions of social media (see CPX report Rebuilding Canada's Public Square) has shown that over the past three years: more than one-third of Canadians have encountered harmful content such as hate speech and violent material online; racialized Canadians are 50 percent more likely than non-racialized to encounter racist content online; and three in four Canadians support requirements for platforms to delete illegal content in a timely manner.

Further, our year-over-year surveys reveal a growth in Canadians reporting exposure to several categories of cybercrimes. The rise in online fraud, as a subset of cybercrime, is an area that particularly requires greater government attention and resource allocation, specifically as it relates to the handling of such crimes by law enforcement. Cyber fraud incidents, which include extortion, identify fraud and personal information scams, are among the most common online harms. Meta's Transparency Center, which tracks how Facebook and Instagram are enforcing community policies, flagged up to 1.7 billion fake accounts, vastly larger than the number of incidents they found of other online harms such as hate speech, violent content, child endangerment and terrorism. While this hints at the scale of the challenge, it is also reported that cybercrimes, like hate speech and fraud, are underreported.

Some positive steps have been taken, specifically through the creation of the National Cybercrime Coordination Unit (NC3) and Canadian Anti-Fraud Centre (CAFC). Further, the Government is currently considering important ways to improve online safety through enhanced oversight, governance and victim support for large online platforms. However, the current scope is focused on a narrow set of illegal activity, namely violent and terrorist content, hate speech, non-consensual sharing of intimate images and child sexual exploitation. Given the pervasiveness of cyber fraud, and the lack of justice often felt by victims through current law enforcement mechanisms, we believe the Government should consider including fraud in the scope of its approach to regulating online harms, while also bolstering the capacity and capabilities of law enforcement to effectively investigate online fraud when and where it does take place.

Goal 2:
An Innovative and Adaptive Cyber Ecosystem

2. What initiatives are needed to help increase cyber security awareness for all, and to build good cyber security hygiene for both individuals and organizations, in order to minimize the risks of cybercrime?

Aligning a Renewed Strategy with Privacy and Data Protection Legislation

As issues of cyber security and digital privacy are closely connected, we encourage the government to consider the points of alignment between a renewed Cyber Security Strategy and the important and far-reaching privacy and data protection legislation tabled in Bill C-27. There are many elements of the bill that will have important implications for cyber security.

For example, core principles and obligations set out in the new *Consumer Privacy Protection Act* — such as establishing the accountability of organizations for personal information, privacy management, limited data collection and use (minimization), data retention and disposal, consent requirements, and stronger investigative and enforcement tools where organizations fail in their obligations — will all be important in enhancing cyber security and improving cyber hygiene across the economy and for individuals, including managing the risks of cybercrime (e.g., minimizing data collection and retention to limit the risks of large data breaches that compromise the information of Canadians).

As artificial intelligence systems are reliant on the collection and use of large amounts of data, the provisions in Bill C-27's *Artificial Intelligence and Data Act* — such as requirements around data anonymization, algorithmic assessments, or risk management — should also be examined through a cyber security lens, and considered for their alignment with the renewed Strategy.

Agile and Adaptive Cyber Security Capabilities

3. What steps should be taken to secure networks, emerging technologies, and to better protect Intellectual Property and consumer products (like Internet-of-Things and apps)?

Western law enforcement and intelligence agencies, including in Canada, have issued public warnings about their inability to gain access to the content of individuals' private electronic communications due to the widespread use of encryption technologies in consumer electronics. Although the Strategy does recognize that "privacy and security are not a zero-sum game," we continue to encourage the Government to adopt a public position that protects and promotes the design, deployment and use of strong encryption systems, without calling on tech companies to develop technical solutions that provide law enforcement with access to unencrypted user data (i.e., "backdoors").

As more and more Canadians begin to adopt new technologies, including IoTs, ensuring the privacy of communications carried out on these devices is critical. Trust in the security of one's communications is also a prerequisite for individuals to feel they can safely exercise their basic rights and freedoms of expression, thought, opinion, belief, and association. This protection is particularly important for marginalized and vulnerable groups, who are disproportionately targeted and surveilled through technology by industry and state security actors. In addition to undermining basic rights and trust in democracy, a failure to ensure the privacy of personal data can have immediate consequences for national security — paving the way for malicious actors, including cybercriminals, terrorists, and hackers, to engage in nefarious activities.

Our CPX Policy Brief (see Why Canada Must Defend Encryption) joins with the wide-ranging network of researchers and experts who advocate for strong encryption; that is, encryption that has not been purposely injected with a known vulnerability to gain access to readable content and facilitate government surveillance. It also presents an alternative policy framework that could enable law enforcement and intelligence agencies to achieve their objectives by applying less invasive measures. Strong encryption provides a broad range of social, political and economic benefits, and will undoubtedly promote the security of Canadian systems and emerging technologies.

Securing Data Sovereignty for Canadians

In our report published in November 2020, Home Ice Advantage, we found that most social media companies provide little to no meaningful information about where they store people's personal data. This data can include biometric information and private messages, both of which are sensitive in nature and particularly in need of protection from prying eyes. There is also limited legal oversight in Canada on the storage location of personal data. This means that data can easily be stored outside of the country and can potentially be accessed, used and processed without consent or may be subject to weaker legal protections than if it were stored in Canada or countries with comparable protections. Our findings also showed that improvements to Canada's privacy and cyber security policy and legal frameworks are needed in order to ensure that personal data receives adequate protection when it is stored outside of the country.

These findings have implications in a wide array of sectors and not just in the realm of social media. Specifically, more precise requirements and enforcement related to cyber security and privacy laws would be needed across the private sector to ensure that data receives protection comparable to what it would receive if it were clearly subject to Canadian laws by being stored in Canada. Companies and institutions should also be required to both obtain consent for the transfer of their personal data to jurisdictions that do not provide comparable protection and to provide information about the specific data and countries involved. The Strategy would ideally address storage location requirements as a critical component of cyber security related to personal data, which is important given the increasing amounts of personal — and at times highly sensitive — data being harvested and that can be subject to improper access, attack, and misuse in an increasingly digitized world.

Cyber Skills and Talent Pipeline

4. What can be done to increase Canada's cyber security workforce capacity and create job-ready workers? (For example, is there a mismatch between the in-demand skills and the skills of post-secondary graduates, is there a misalignment between job descriptions and the experience of candidates, is there a need for standardized curricula and outcomes, access to work-integrated learning opportunities, and short-cycle training and upskilling for workers and graduates, etc.)

Education and Training for Cyber Talent and Responsible Technology

The talent and skills gaps in Canada's cybersecurity industry, and in related fields of technology and digital governance, are well established. Deloitte has described a growing cyber risk gap, with the rate of technology change and resulting cyber risk growing much faster than organizational cyber capacity. Across Canada's major industries including financial services, retail, energy and resources, and the public sector, demand for cyber talent was estimated to be growing at 7 percent annually (Deloitte, 2018). Addressing this gap requires both the development of new, job-ready workers in cyber and related fields, and the upskilling of the existing workforce in these domains. Other research has highlighted the closing of gender and diversity gaps as a key priority, with benefits to focused interventions to do so (Raytheon, 2016).

A renewed Strategy and related policies and investments of the federal government should continue to prioritize initiatives to build workforce capacity as part of efforts to ensure the security, integrity and resilience of Canada's critical public and private sector systems. Filling this talent pipeline requires new and sustained education, training and workforce development initiatives that reach a diversity of learner types and profiles across Canada - ranging from youth as they're considering career options, to learners entering or at the postsecondary level, to new and working professionals across industry sectors. Interventions must also recognize and address diversity gaps in the workforce, resulting from factors such as the disinclination of young women to pursue careers in cyber security and STEM fields generally. They should also seek to infuse technical education with an understanding of the broad social context for digital technology and security, and with robust training on topics such as ethics, professional responsibility, human rights, privacy and security risk assessment.

Through CPX, and founding partners Rogers Cybersecure Catalyst and Leadership Lab at TMU, a suite of programs have been introduced that contribute to addressing this national workforce challenge across the spectrum of learners:

- The Catalyst Cyber Camp delivers free, online programming to **youth (ages 13-18)** in Brampton, Ontario, offering campers access to 400 hours of virtual programming, including cutting-edge games, activities and puzzles that build cyber awareness, hygiene and career interest. Initially supported by partners Rogers Communications, the City of Brampton, and SANS Institute, the world's leading cybersecurity training, the program is expanding nationally with support from Public Safety Canada.

- The Accelerated Cybersecurity Training Program is a 28-week intensive cybersecurity training and certification program designed to give **promising learners from diverse backgrounds**, including women, new Canadians, and displaced workers, the skills they need to launch careers in the cybersecurity sector. The Program is supported through the generous partnership of the Government of Canada, Rogers Communications and RBC.

- The Secure and Responsible Tech Policy professional education program - the first of its kind in Canada - was designed to upskill **leaders and professionals across the policymaker and technology communities**, building understanding of the technology policy landscape in Canada and globally, and introducing a secure and responsible tech lens for critically assessing current issues in domains including cybersecurity, the digital economy, and disruptive technologies like artificial intelligence. The microcredential program is supported by Public Safety Canada and RBC, and delivered in partnership with the Council of Canadian Innovators and the Ontario's Cyber Security Centre of Excellence.

- The Catalyst Corporate Training and Cyber Range provides onsite or virtual training opportunities to **organizations across Canada** and offers a combination of tailored Workshops, Tabletop Exercises (TTX) and Catalyst Cyber Range technical scenarios that help prepare teams to defend against and respond to emerging cybersecurity threats. Training services are offered to teams and organizations of all types and sizes, and from all sectors.

- The Catalyst Simply Secure program offers the highest-quality resources and training that **small- and medium-sized businesses (SMBs)** need to drive the cybersecurity of their organizations. These resources and training are designed to help SMBs become more cybersecure and turn their cybersecurity into a competitive advantage and positive differentiator.

- Public education and policy initiatives aim to build broad awareness and learning about cyber security for a **broad cross-section of Canadians**. As a key resource, information partner and convener, the Catalyst distributes accessible and easy-to-use cybersecurity best-practice resources, in particular for SMEs, seniors, youth and teachers.

CPX and its founding TMU partner organizations are eager to continue growing these national education and training programs in partnership with Public Safety Canada and other educational institutions and industry collaborators across the country.

Goal 3: Effective Leadership, Governance and Collaboration

5. What is needed to strengthen collaboration and engagement on common interests between the provinces, territories, Indigenous communities and municipal governments, regulators, private sector, academia, not-for-profits, labour organizations and the Government of Canada?

Building the Cyber Startup Ecosystem

With world class academic institutions, talent, expertise, innovation centers, and active entrepreneurship among Canadians, Canada has the major elements needed to foster an internationally competitive cyber security industry. Several barriers continue to obstruct Canada from reaching its potential as a global cyber security innovator and industry leader, however. Although cyber security innovation development is strong in Canada, startups struggle to scale and commercialize within the country. As a result, Canadian cyber security startups move or sell their businesses abroad, leaving Canada at a loss of potential productivity gains and home-grown cyber resilience.

Fostering a more sustainable cyber security startup ecosystem can bring great benefits to Canada's national security, economy, and international reputation. An upcoming CPX research and policy report (to be published later in 2022) will examine the challenges and opportunities for strengthening the country's cyber security startup space. The Catalyst has also established a first-in-Canada technology accelerator program solely committed to supporting Canadian cybersecurity scale-ups: The Catalyst Cyber Accelerator. This program provides critical assistance to help these early stage cybersecurity firms succeed: workspace, support, mentorship and access to clients and advisors.

The renewed Strategy should prioritize the development of Canada's cyber ecosystem and support efforts to commercialize Canadian cyber companies. CPX is eager to contribute to these efforts with the Government and other partners across the country.

We hope that these contributions are helpful, and would be eager to engage further on these issues with Public Safety Canada and other federal government entities, or through multi-stakeholder discussions.

Our aim is to inform and support good public policy for Canada, in the interest of Canadians - and believe the renewal of the National Cyber Security Strategy will be critically important in serving those ends.

cybersecure
policy
exchange

Powered by RBC

Toronto
Metropolitan
University