August 16, 2022

Submitted via cyberconsultation-consultationcyber@ps-sp.gc.ca

Public Safety Canada
269 Laurier Avenue West
Ottawa ON
Canada K1A 0P8

RE: Consulting on Canada's Approach to Cyber Security

The Cybersecurity Coalition ("the Coalition") submits the following comments in response to the public consultation issued by Public Safety Canada ("the Government"), *Consulting on Canada's Approach to Cyber Security* ("the consultation"). The Coalition appreciates the Government's openness in engaging industry on this important topic and looks forward to working with the Government to further explore the adoption of recommendations outlined in this submission.

The Coalition further commends the Government for its global leadership on cybersecurity issues, including engagement in forums such as the UN Government Group of Experts ("UNGGE"), the UN Open Ended Working Group ("OEWG") and through its early ratification of the Budapest Convention on Cybercrime ("Budapest Convention").

The Coalition is composed of leading companies with a specialty in cybersecurity products and services. We are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community.

The Coalition has worked with more than 20 governments around the world on the development of national cybersecurity policies, many of which were designed to address issues that are raised in the paper. Given the complexity of cybersecurity, we are acutely aware of the need to effectively address the challenges that you identify, as well as the difficulty of doing so in an effective manner.

We provide the following responses to the survey questions with a view to advancing our shared objective of safeguarding publicly- and privately-owned infrastructure from malicious cybersecurity activity. The Coalition thanks the Government for its careful examination of these issues. As the conversation around cybersecurity in Canada continues to evolve, we would

welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that these proposals are successful in achieving the Government's objectives.

Respectfully Submitted,
The Cybersecurity Coalition

August 16, 2022

CC: Ari Schwartz, Venable LLP
Alexander Botting, Venable LLP

Response to Survey Questions

Q1. 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?

The rapid pace of innovation among cyber criminals, the high profitability of such activities, and the lack of consistent implementation of cybersecurity best practices within industry has created a breeding ground for widespread malicious cyber activity. This has been further exacerbated by the COVID crisis, which has increased our dependence upon digital systems.

To address these concerns adequately will require a multi-pronged approach from the government, to include:

1) Reducing the ability of international cyber criminals to operate with impunity;

2) Enhancing the resiliency of industry against cyber threats through the consistent implementation of security best practices, more effective threat information sharing, and enhanced cyber security understanding across industry; and

3) Ensuring that there are sufficient human resources with the necessary skills to meet the cybersecurity needs of Canadian and international companies.

We provide additional guidance regarding each of these recommendations in our answers to subsequent questions.

Q2. 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?

Given their importance to society more broadly, Canadian critical infrastructure entities should be subject to clear baseline cybersecurity requirements. In addition, the government should communicate clear guidance to non-critical entities regarding steps that they can voluntarily take to better protect themselves against cyber threats, taking into account the potentially limited resources of smaller companies.

For any sized company, requirements or recommendations should be grounded in consensus-based international standards and a risk management-based approach to cybersecurity. In addition to the security benefits that such an approach fosters, it aligns with the cybersecurity commitments of Article 19.15 of the U.S.-Mexico-Canada Free Trade Agreement, to which Canada is a signatory. In particular, the NIST Cybersecurity Framework and its associated

international standards[1] clearly embody these principles and have the benefit of being widely utilized by industry in both the U.S. and Canada.

In addition, the government should identify a clear point of contact for support and oversight within the government to reduce friction for organizations seeking to interact with government counterparts. The Canadian Government may choose to develop a centralized approach, leveraging the Canadian Center for Cyber Security's ("CCCS") cybersecurity expertise, or a sectoral approach to leverage the expertise of regulators in sectoral risks.

Regardless of the approach taken, collaboration should be seamless and avoid the kind of duplication that wastes scarce public and private sector resources.

Q3. 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)?

As outlined above, the government should develop clear baseline cybersecurity requirements for critical infrastructure to ensure that entities are taking minimum steps to ensure that their networks are secured. These requirements should leverage a risk management-based approach, be technology neutral, and leverage existing international standards where possible. The latter point is particularly relevant when considering the international nature of many critical infrastructure operators and the global nature of cyber threats.

Leveraging the NIST Cybersecurity Framework and its associated international standards would be helpful in promoting alignment of security measures across North America.

Q4. 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.)

Cyber workforce development is a global challenge, with an estimated 2.72 million cybersecurity jobs unfilled in 2021.[2] This is a critical challenge for both government and the private sector as we seek to defend against malicious actors that are launching attacks at scale.

The need for cyber literacy is also illustrated by the high percentage of data breaches and business compromises that could have been avoided with better education around cyber risks and threats.[3]

---

[1] ISO/IEC 27110 and 27103

[2] https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey

[3] https://enterprise.verizon.com/resources/reports/dbir/2020/results-and-analysis/

We encourage the Government to work with the private sector both to identify and address cybersecurity workforce needs, and to collaborate to raise cyber literacy more broadly across society. We're confident that investments in these two areas will provide a substantial return on investment for the Government by enhancing Canada's cyber resilience.

Q5. 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?

As outlined in our answer to Question 2, the Government should clearly identify the responsibilities of each agency with regards to collaboration with the private sector and provide points of contact for industry, to make collaboration more seamless for industry. Ideally, the entities responsible for support and collaboration will have no regulatory or oversight function, to ensure that industry is comfortable with open collaboration.

Threat intelligence sharing should be a two-way process, such that industry can see clear benefits from collaborating with government. As such, the CCCS should identify ways that they can better share information with industry to enhance the resilience of the Canadian ecosystem.

To enhance industry intelligence sharing with government, the Government can enhance trust through the implementation of best practices such as:

- Keeping information sharing voluntary, thereby allowing companies to identify the most relevant information to share
- Providing legal protections for any information shared by companies
- Keeping a separation between those Government agencies that are tasked with support and threat intelligence aggregation, and those tasked with regulatory oversight

Q6. What can the Government of Canada do to help shape the international cyber security environment in Canada's favour and advance Canada's international cybersecurity interests?

The objectives outlined above must be advanced not just domestically but internationally, as cybersecurity is an inherently global endeavor. The government can positively shape the international cybersecurity environment by:

1) Continuing to advance the implementation of norms of responsible state behavior in forums such as the UNGGE and OEWG

2) Ensuring that cyber criminals can be held to account for malicious cyber activity through advancing international mechanisms such as the Budapest Convention and/or the UN Cybercrime Convention

3) Continuing to advance the global adoption of cyber policy best practices in forums such as the WTO JSI on E-Commerce, future free trade agreements to which Canada is a signatory, and in organizations such as the OECD

   Given the interconnected nature of digital supply chains, the ecosystem as a whole benefits from the consistent adoption of cybersecurity best practices.

Q7. Are you responding as an individual or someone representing an organization?

We are responding on behalf of an organization: The Cybersecurity Coalition.

Q8. What province or territory do you live in?

n. outside Canada