ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Box 348, Commerce Court West
199 Bay Street, 30th Floor
Toronto, Ontario, Canada M5L 1G2
www.cba.ca

Canadian Bankers Association's Response to Public Safety Canada's Cyber Security Public Consultation

TREND 1: Evolution of the Cyber Threat

Theme - Addressing Cybercrime

Q1: How can law enforcement better address the growing challenge posed by cybercrime (for example, through training and capacity-building, equipment, partnerships, innovative initiatives)?

In today's digital environment and economy, cybercrime is an increasing threat facing Canada. It has the potential to impact our national security, economic prosperity and public safety. In order to combat the threat of cybercrime, the following is recommended:

- **Formal Definition of Cybercrime:** A proper formal definition of the term cybercrime, that covers both corporate espionage and theft of intellectual property, is required. Guidance on standard thresholds and processes for engagement is also needed.

- **Law Enforcement Strategy:** A strategy for a centralized cybercrime investigative centre to handle complex types of cybercrime across jurisdictions, both domestic and international, is necessary. Establishing global relationships with other cyber hubs (e.g. Singapore, UK, US, etc.) to develop cross-border collaboration and prosecution capabilities is necessary.

- **Investment in Cybercrime Prevention Capabilities:** Adequate resources focused on cybercrime are required. The need for continuous long-term investment in cybercrime capabilities (e.g. training, equipment, partnerships, innovative initiatives etc.) must be recognized at the federal level.

Q2: How can public and private sector organizations help protect themselves from cybercrime, such as threat of ransomware attack, fraud and identity theft, and what tools do they need to do so?

The banking industry handles cyber threats on a daily basis and they have robust systems in place. Banks continually invest in technology, staff, education and training. Collaboration with the public and private sector to protect the nation from cybercrime is vital. The following are recommended:

- **Public Sector Awareness:** Collaboration is required between the public and private sector to educate the public on cybercrime and how to protect themselves through industry best practices.

- **Encourage reporting:** Creating an online platform for consumers to submit screenshots and suspicious computer files would also encourage reporting of security issues.

- **Secure Canada brand:** A highly visible program, co-funded by the public/private sectors, can be created to deliver security awareness "commercials" via TV, radio and popular Canadian websites.

- **Messaging and Education:** The banking industry publishes cyber security information on their websites in order to help educate the consumer. Collaborating with the banking industry and other sectors to further promote cyber security awareness can be beneficial.

Q3: Are there barriers to reporting cybercrimes (or suspected cybercrime) to law enforcement agencies? If so, what are they?

Barriers exist in reporting cybercrime and our view is outlined below:

- **Jurisdictional Issues on Reporting Cyber Security Issues:** It is unclear where, and to whom, cybercrimes should be reported and what information is required or beneficial. A template method to report cyber security issues would be helpful. This method could employ a one-window principle which allows all cyber security-related incidents to be reported through a single online interface, regardless of their jurisdiction, scale or nature.

- **Lack of Evidence Upload Capabilities:** A mechanism needs to be in place requiring the public/private sectors to upload details of the suspected cybercrime activity (e.g. files, screenshots, emails etc.).

- **Effectiveness of Canadian Law and Local Law Enforcement***:* *Criminal Code* provisions as it relates to cybercrime should be strengthened to reflect the present day cybercriminal acts (e.g. online fraudulent websites, illegal copyright material online, etc.). Currently, shutting down malicious sites requires lengthy interaction with multiple service providers or specialized private firms which could result in a delay to response time and action.

- **Feedback Loop is required:** Given the discretion on the variety/severity of issues that are reported to law enforcement, it is unclear which incidents are of value. Feedback, assistance and follow-up from law enforcement, are required.

<u>Theme - Policing in Cyberspace</u>

Q4: What are your expectations for policing in cyberspace? Are they different from policing in the physical world?

We would expect law enforcement to have effective tools and sufficient laws in place to police cyberspace. As well, a clear reporting structure is required to identify who is accountable (owner of the issue). The policing workforce needs to be more agile and apt to cooperate with experts in the private sector. Where the financial sector launches new product and services to Canadians, law enforcement needs to be brought in to stay ahead of any innovations and new technologies to ensure policing tools are kept relevant and ready to support the financial sector during a critical cyber-based incident. This

type of engagement has to be balanced against Canadians' privacy rights and ability to use encryption that continues to protect their banking transactions and communications. Substantial reporting mechanisms are already in place to inform government on suspicious activity in accordance with anti-money laundering and terrorist financing laws.

Q5: In a digital age, security and privacy go hand in hand. How can cybercrime be addressed in a manner that respects Canadians' privacy rights and protects public safety?

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) balances the privacy rights of individuals with the need of organizations to collect, use and disclose personal information in the course of carrying out their business. However, the *Digital Privacy Act* recently amended PIPEDA and some of the amendments may impede the ability organizations need to share personal information to detect, prevent and suppress cybercrime. Clarity on the amendments may be required to provide adequate protection for organizations to share suspicious information.

Theme: Protecting Against Advanced Cyber Threats

Q6: What do public and private sector organizations need to protect themselves from advanced cyber threats (for example, tools, capacity, information)?

Public and private sector organizations need to collaborate and share information to protect against advanced cyber threats. The following are recommended:

- **Improving cyber security workforce is vital:** A talent pool to address increased cyber security demands is required. This includes improved educational options for careers in cyber security, training for existing staff, mature career-development management practices, and creative cross-pollination with high-demand disciplines that are closely tied to cyber security (e.g. data science, analytics, business intelligence, state & military intelligence).

- **Effective intelligence sharing:** Rapid intelligence sharing of observed threats is a highly effective means of minimizing the impact of advanced and rapidly evolving attacks. In order to achieve timely sharing between public sector and government agencies, improved sharing protocols and control integration is required. The government of Canada can explore initiatives such as the Canadian Cyber Threat Exchange (CCTX) to promote the exchange of cyber security information and best practices between government and businesses.

- **Align to International Standards:** The banking industry has robust systems in place to protect against cyber threats. We encourage the government to leverage and promote a recognized common industry standard such as the National Institute of Science and Technology (NIST) Cyber security Standard across all critical infrastructure sectors to assess and manage cyber risks that are comparable to the requirements for federally-regulated financial institutions.

- **Single Government Point of Contact:** Within the current cyber security landscape there are many Federal Government agencies with similar goals. An opportunity exists to streamline all governmental cyber security information sharing activities among all critical sectors into one single government agency.

- **National capability to filter out malicious Internet traffic:** Telecommunication companies should be empowered to proactively block known malicious traffic before it reaches individual company networks without fear of liability, but also include an appeal process for entities that have been inadvertently disconnected.

- **A coordinated public/private response to cyber-attacks is critical:** The Canadian economy and national security are co-dependent; one cannot exist without the other. Attacks against industries or nations require a coordinated defensive response between the government and the private sector, particularly among critical infrastructure partners and stakeholders such as financial services, telecommunications, energy, healthcare, retail and transportation.

Q7: What are the constraints to information sharing on advanced cyber threats and associated vulnerabilities?

The constraints to information sharing on advanced cyber threats and associated vulnerabilities include:

- **Access to Information:** There are concerns that certain information shared with government entities may be subject to a Freedom of Information/Access to Information request. While we understand there are certain access exemptions available under current legislation, we believe clearer exemptions from access legislation going forward would foster increased sharing of cyber threats.

- **Lack of Safe Harbour:** There are concerns that sharing of cyber threat information may result in civil litigation or adverse enforcement action from regulators (e.g., privacy regulators). A safe harbour provision, similar to the US's *Cybersecurity Information Sharing Act of 2015* that prohibits causes of action for activity relating to the sharing or receipt of cyber-threat information, would foster increased sharing of cyber threats.

- **Amend Legislative and regulatory rules to allow telecommunication companies to share threat information with commercial customers:** The telecommunications industry plays a critical role to interconnect Canadian consumers and businesses, and it is vital that they safeguard the security of their infrastructure to ensure a safe and secure Canada. A capability to secure its infrastructure and to deliver valuable traffic is necessary to ensure the safety and productivity of Canada.

- **Inconsistent Global Cyber Legislation:** Multinational organizations need to comply with a wide array of legislation when contemplating the sharing of cyber threat related information. For example, in Canada there is no comprehensive safe harbour for sharing certain cyber threat information, while in the U.S., companies may rely on the safe harbour provision in the *Cybersecurity Information Sharing Act of 2015*, that prohibits causes of action for activity relating to the sharing or receipt of cyber-threat information, decisions made to enhance cyber security based on such information, and authorized network monitoring. The Act also prohibits federal and state agencies from using cyber-threat indicators provided by the private sector to regulate (including by enforcement action) the otherwise lawful activities of private sector entities.

- **Standardization:** There are inconsistent standards for trust relationships and these standards are almost entirely ad-hoc. Few mechanisms exist that afford clear vetting standards and granular guidelines for the types of data to be shared; most sharing venues rely on either personal relationships (not scalable) or coarse traffic light protocols and broad audiences, reducing the value of information being shared.

Theme: Increasing Public Engagement

Q8: How can public and private sector organizations work together to build Canadians' awareness of cyber security issues (for example, joint online training initiatives)?

Educating businesses and consumers in a timely fashion is increasingly complex with the rapid change of technology. Public awareness campaigns are one aspect of a comprehensive education/awareness strategy. The following are recommended:

- **Education and Awareness:** Similar to the government's initiative to improve financial literacy, an initiative to improve cyber literacy as part of a national cyber literacy program is also required. A national cyber literacy program, that educates and helps protects consumers, is necessary to the overall security of the nation. The majority of significant compromises and baseline security threats rely on exploitation of human nature. As part of a national cyber literacy program, there should be greater focus on human behaviour-based applied research and curricula (rather than technology). Focusing on human behaviour as part of a cyber-literacy program could have a significant impact on increasing security-aware cultures that would reduce risk.

- **Cyber Threat Exchange Capabilities:** The support of initiatives such as the Canadian Cyber Threat Exchange (CCTX,) to promote the exchange of cyber security information and best practices between government and businesses, is necessary. These initiatives can be built by leveraging best practices from mature cyber threat exchange organizations that encourages communication of cyber threat information and practices to a much broader community.

- **Online Resource Centre:** The government should consider establishing an online resource centre staffed to assist consumers and organizations in reporting cybercrimes, sharing related information and educating consumers on cyber security.

Q9: How can individuals be better informed about how to recognize and react to a cybercrime (like spear phishing) or a cyber security vulnerability (for example, security of networked cars or connected health devices like pacemakers)?

Information is key to recognize and react to cybercrimes and cyber security vulnerabilities. The following is recommended:

- **Professional Consumer Communications and Advertising Firm:** Engagement with a professional consumer communications and advertising firm to develop a multi-year campaign to drive cyber-awareness amongst average Canadians.

- **Threat Intelligence Hub:** Developing a threat intelligence hub, that can cater to the public and private sector, is required. Consumers would be able to subscribe to a threat feed via different channels such as email, SMS messages or web updates in order to receive timely updates on the latest attacks/issues and receive guidance on how to protect themselves.

- **News Flash:** As part of the “Secure Canada” brand/program develop a “cyber news flash” for new and emerging security threats for Canadians. Short, multi – channel bulletins (e.g. TV, Radio, and

SMS etc.) can be leveraged to communicate cyber news and other cyber security information to Canadians.

- **Cyber Crime Stoppers:** The government needs to have a web-based resource that describes existing laws and cybercrime threats to Canadians. This includes cybercrime prevention, detection and response scenarios that educate Canadians on how best to protect themselves. Incentives could be offered to Canadians for those who report cybercrime activity that leads to a successful prosecution.

TREND 2: Increasing Economic Significance of Cyber Security

Theme: Strengthening Consumer Confidence in E-Commerce

Q10: How can Canadian businesses be encouraged to adopt better cyber security regimes – particularly small and medium enterprises?

Cyber security is a challenging problem and concern due to the sophistication of cybercrime activity. In order to assist Small Medium Enterprises (SMEs) with this issue, a strong public-private partnership is required. This includes policy enhancement and cyber security-focused government programs/initiatives which would result in a strong security posture for SMEs. We recommend that the government consider a series of measures to enable SMEs to enhance their security posture, such as the below.

- **Small Medium Enterprises (SMEs) Cyber Security Program:** Launch a Small-Medium Enterprise cyber security program, whereby SMEs would engage with an industry expert from a list of preapproved security providers to conduct a security audit. A Canadian Cyber security Seal of Approval (CCSA) would be awarded based on the successful completion on implementing recommendations issued as a result of the audit. The creation of an accreditation program for Cyber security providers that will give SMEs a directory of approved providers with expertise would also be beneficial.

Q11: What factors do you think are important to consider before sharing your personal and financial information with businesses online (for example websites displaying a *Secure* logo, web addresses beginning with https)?

Canadians should consider the following factors before sharing their personal and financial information with businesses online:

- **Trustworthiness of Online Merchants:** Use established online merchants; do they use established online payment service providers such as well-known banks, PayPal and others?

- **Legitimacy of a Website:** Does a website use encrypted connection (padlock icon, “HTTPS” and/or green highlight in the address line), or are they “certified” by a regulated cyber security program?

- **Privacy Policy:** Does a website solicit excessive personal information (e.g., date of birth) without reasonable explanation of why it is being requested? The ability to limit required information related to products or services is essential.

Theme: Embracing New Cyber-Secure Technologies

Q12: What steps should be taken to ensure that networked and emerging technologies (like internet-of-things and apps) are cyber secure?

Canadian adoption of emerging technologies such as the Internet of Things (IoT), mobile apps and networked devices is ever increasing. With the sophistication of such devices, Canadians need to be assured that appropriate cyber-security mechanisms are in place to ensure data protection. Therefore, businesses must take appropriate steps and measures to ensure their products are secure for the entire lifecycle. Below is a list of recommendations:

- **Independent Lab Testing**: Independent lab testing is required to ensure security of the IoT and other emerging technologies. This is similar to the Canadian Standards Association (CSA) evaluation for product safety.

- **Continuous Support**: Manufacturers should be required by law to provide continuous support including security patches for their products for a given amount of time, and customers must be notified when support expires. A penalty should also be enforced by the government for failure to comply.

- **Canadian Cyber security Seal of Approval (CCSA):** This would carry liability similar to the equipment manufactures liability stipulated by the CSA certification process.

Theme: Protecting Critical Infrastructure

Q13: What are the barriers to strengthening cyber systems in critical infrastructure (within and across sectors)?

Critical infrastructure needs to be cyber secure in order to protect the health, safety, security and economic well-being of Canadians. Collaboration and communication is essential between all levels of government and privately/publicly held critical infrastructures. The following is recommended:

- **Single point of contact to drive collaboration:** A single point of contact is required to promote collaboration among critical infrastructure.

- **Uniform testing requirements across all sectors:** Mandatory security testing by an independent lab for all infrastructure cyber implementations. This requirement is vital to secure cyber systems within Canadian critical infrastructure.

- **Cyber Security Standards:** Well-defined and published cyber security common standards and best practices, as they apply to critical infrastructure, is required.

- **Public / Private sector Infrastructure Protection Plan:** Establish a partnership for critical infrastructure Security and Resilience. Define how government and private sector participants in the critical infrastructure community can work together to manage risks and achieve security and resiliency.

- **Remove barriers to strengthening critical infrastructure:** Establish federal policy to strengthen the security and resilience of its critical infrastructure from physical and cyber threats. Working with critical infrastructure to manage risk and strengthen the security and resilience of Canada's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability and public safety is required. Business continuity planning and exercises are also an important element to enable a robust and resilient critical infrastructure. The goals of these efforts will reduce vulnerabilities, minimize impact, identify and disrupt threats, and increase response and recovery efforts.

Q14: What are the constraints to information sharing and engagement related to protecting cyber systems of Canada's critical infrastructure?

Information sharing is essential to protecting cyber systems of Canada's critical infrastructure. The Federal Government should proactively develop and implement cyber threat and information sharing programs. Through these programs, the Federal Government can develop partnerships with the private sector in order to share information. These programs can also be used to share information between provincial and municipal governments, as well as international partners, as cyber security threat actors are not constrained by geographic boundaries.

The following constraints hinder deeper information sharing and engagement:

- **Legal / Policy Considerations:** Potential (perceived or actual) liability concerns may be preventing broader information sharing. The Federal Government needs to issue clear guidance in relation to information sharing, encouraging involved parties to share cyber security information without fear of penalties.

- **Protection against Information Disclosure:** Protection against information disclosure will allow open cyber security information sharing.

Key aspects to overcoming constraints to information sharing include:

- **Establish threat information gathering and monitoring capability:** Establishing threat information gathering and monitoring capability that spans Federal Government, Intelligence communities and law enforcement, is required.

- **Public and Private sector information sharing on cyber threats, incidents, vulnerabilities, etc.:** Public and private sector information sharing enhances the security of networks and systems and also promotes and supports the shared security of participating organizations. Furthermore, it provides a collaborative environment where organizations can learn and better understand current / emerging cyber risks and mitigating defensive methods.

- **Voluntary sharing of information to help protect public and private entities against cyber threats:** The voluntary sharing of information is required, and may include sensitive and potentially classified threat information gathered by the Federal Government or Law Enforcement agencies.

- **Faster sharing of threat information:** Faster sharing of threat information is necessary. Automating the sharing of anonymized threat indicators in real (or near-real) time enables improved situational awareness about emerging threats. It also facilitates rapid detection, prevention, and mitigation of threats without compromising the trust and confidentiality of the participants.

- **Establish communities of trust:** Establish communities of trust through the sharing of information between critical infrastructure owners, operators and Federal Government is required. Building protection mechanisms, where member organizations can be confident the information shared with the government will not compromise the confidentiality or proprietary nature of the information, is important.

- **A contact network portal that allows information sharing with Small Medium Enterprises:** Large enterprises are able to establish relationships through industry forums and networks to share information. SMEs do not necessarily have access to such venues to participate in cyber information sharing. SMEs may need to be provided with sharing/driven incentives to build the necessary infrastructure to facilitate cyber information intelligence sharing. Establishing a network of contacts or developing a subscription portal that facilitates the connection between SMEs, could also be helpful.

TREND 3: Expanding Frontiers of Cyber Security

Theme: Building a 21st Century Knowledge Base

Q15: What information (e.g., data, metrics) would contribute to a better understanding of cyber security issues in Canada? Please explain your response.

Financial institutions and government agencies collect valuable cyber security information. Data analytics that generate metrics such as event type, rate of occurrence, impact, magnitude and trend analysis is beneficial to Canada's cyber security strategy and drives policy decision making. The following items with respect to metrics are recommended:

- Aggregating metrics around incidents (volume and impact) and type of attacks (e.g. phishing, perimeter attacks, insiders, etc.) allows organizations to profile the size and nature of the problem in Canada.

- Data related to Canadian end-user attacks, such as information on identity theft and account takeover, would be useful.

- Aggregating spending and investment levels by industry would be useful to assist benchmarking activities.

- Compulsory disclosure of resilience level for key shared infrastructure components within critical infrastructure (e.g. power distribution, telecommunications, payment systems, etc.) would allow industries to better manage systemic risks against catastrophic impacts.

- Value-added analytics (e.g. Link analysis) to develop greater insights on attack profiles and organized crime linkages.

Theme: Encouraging Growth and Innovation

Q16: What is needed to improve Canadian innovation in cyber security?

Canadian innovation should be encouraged at all levels of government and the private/public sector. Given the dramatic increase in sophisticated threats and malware, there is a need for skilled security professionals that can deal with advanced threats and advanced adversaries. New innovative strategies for identifying attacks and innovative ways to share information are necessary to strengthen our cyber defences.

- **Education and Competition:** Canada has a highly educated work force which needs to be attracted and retained within Canada's security industry. The Federal Government needs to develop and invest in both formal cyber security education and cyber safety programs. These programs should be tailored to students at all levels including K-12, colleges and undergraduate, graduate and post graduate students. In addition, the creation of cyber competitions that are interactive and scenario-based, and that generate interest in pursuing cyber security careers, is valuable.

- **Research and Development:** The Federal Government needs to assist in establishing hubs at key intersection points between public sector, private sector and research institutions. As an example, the Israel Government has created the Cyber security innovation ecosystem. In addition, focused programs and incentives to bring research and industry together to solve challenging issues in cyber security, are required. Examples of issues include cryptographic advancements, protection of financial infrastructure, emerging financial technologies, protection of industrial control systems and the IoT.

Q17: What measures could be taken to improve the availability, relevance, and quality of cyber security training?

The government needs to promote cyber security as an important profession in Canada. Furthermore, there is a diversity gap within the cyber security workforce. Increasing gender diversity and other diversities would introduce create and innovative thinking and resiliency which follows diversity.

- **Cyber Security Training and Availability:**
    - Establish a cyber security training curriculum evaluated and vetted by the industry to ensure quality and adequacy.
    - Establish nationwide accreditation programs related to both individual skills development via post-Secondary education and security service providers.
    - Establish grass-roots education for the K-12 schools to both build more cyber-aware culture and engage next generation of cyber security professionals.