Briefing Document – CBA Recommendations: Bill C-27 *Artificial Intelligence and Data Act*

February 6, 2024

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Submission to Standing Committee on Industry and Technology

- The Canadian Bankers Association (CBA) is aligned with the Government's policy objectives to promote the responsible development and use of AI systems in a manner that supports existing principles under Canadian law and consistent with the OECD's AI principles.

- In a rapidly evolving field like AI, a flexible, risk-based regulatory AI framework is necessary to ensure Canadian organizations can serve consumers in a manner that fosters confidence and builds trust in the responsible development, deployment and use of AI, including Generative AI systems.

- For this reason, it is important for the *Artificial Intelligence and Data Act* ("AIDA" or the "Act) to remain principles-based and outcomes-focused, while technology-specific items (e.g., references to, and discussion of, specific technologies) should be left to regulation.

- Coordination and cooperation with domestic partners, including regulatory agencies like OSFI, and international partners, at the G7 level in particular, is also an essential component of ensuring a degree of interoperability and harmony between various AI legislative and regulatory frameworks as well as other relevant frameworks (e.g. privacy or cybersecurity).

- As a result, we believe targeted amendments in the following areas of the Act are required to provide Canadian organizations with the certainty needed for them to continue to compete globally and innovate in a data driven economy while meeting the Government's objective of protecting individuals from harms posed by AI systems.

    - **Scope of Artificial Intelligence Systems:** Amend the definition of an AI system to support AIDA's policy intent and avoid unnecessarily broadening the scope of systems captured under AIDA.

    - **Transparency Obligations and Related Provisions:** Amend the requirements related to public disclosures by the relevant actors under AIDA and include appropriate exceptions such that organizations will not be compelled to disclose proprietary or sensitive information, which will ultimately protect the public and organizations from avoidable harm that can potentially be caused by broad disclosures of risks or mitigation measures.

    - This includes the obligation on persons responsible under the Act to disclose prescribed information; as well as the right to disclose information by i) the Minister or Commissioner to others and ii) the right to publish information by the Minister or the Commissioner.

    - **Clarifying Obligations Across the AI Value Chain:** An unambiguous set of distinctions between the actors and activities, and their interdependencies across the AI value chain, developed through targeted consultations is required to avoid confusing, conflicting, or overlapping obligations. This will provide the various stakeholders with the operational clarity that is necessary to ensure they can remain accountable for their obligations throughout the lifecycle of an AI system.

  Implementation & Other Considerations: We believe it is critical to ensure that organizations are provided sufficient runway (minimum two years) to manage and implement new changes once AIDA receives Royal Assent and the bulk of the obligations under AIDA are published through regulations. We have also included recommendations related to several key considerations below that should be addressed in consultation with stakeholders on the regulations for AIDA.

  In conclusion, it is evident that the proposed changes to AIDA represent a significant step forward in the regulation and governance of emerging technologies. However, it is essential for ISED to continue engaging with experts, stakeholders, and the public through a public consultation process that ensures a comprehensive and balanced approach to AI regulation. By fostering collaboration and remaining vigilant to the evolving nature of AI, Canada can effectively address the challenges and opportunities presented by this transformative technology, ultimately benefiting Canadians and society as a whole.

The CBA recommendations below apply to and reference the original Act. Areas where the recommendations apply to the proposed amendments by ISED are identified as such.

APPENDIX: CBA Recommendation Details

1. Scope of AI Systems:

Definition of AI System

Original AIDA Text: ***artificial intelligence system*** means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.

Proposed ISED Amendment: **artificial intelligence system** means a technological system that, using a model, makes inferences in order to generate output, including predictions, recommendations or decisions.

CBA Recommendation: We support the removal of references to "another technique" in the amended definition proposed by the Government to avoid expanding the scope of AI systems as that could result in added (but avoidable) complexity and the misallocation of resources for Canadian organizations.

If there is a desire to align Canada's definition of AI systems with that of the OECD, it is important to ensure the final definition avoids overextending the parameters of the Act and focuses on the risks and impact on individuals (i.e., outcomes), rather than the data processed by an AI system.

High-impact systems:

Proposed ISED Amendment (s.37.1): Regulations made under sections 36 and 37 may distinguish among different categories of artificial intelligence systems.

We understand that ISED intends to consult extensively on the different categories of AI Systems, which would allow for distinct regulatory requirements for different classes and subclasses of high-impact systems and distinct types of general-purpose systems as s. 37.1 of the proposed amendments suggests. There is currently no clarity within the Act as to which details are being referred to or captured by the term "categories" and no consideration given to the fact that certain applications of high-impact or general-purpose AI systems are going to be far less risky than others, even within a class or subclass of high-impact system or general-purpose category.

CBA Recommendation: We recommend the inclusion of specific language in the Act to clearly define what is meant by categories of high-impact systems and general-purpose AI systems and to allow for specific requirements between classes and subclasses as well as within these classes. This includes thresholds for risk to facilitate distinctions between high-impact systems and general-purpose systems that are low risk and those that pose a high risk of harm within a given class.

Stakeholder input during these consultations will be critical to ensure requirements related to the different classes and subclasses of high-impact systems, as well as machine learning models and general-purpose AI systems, ultimately support the Act's policy intent of preventing harm and unjustified biased output, account for the differences across various sectors and to ensure appropriate limitations exist to avoid the unnecessary inclusion of lower risk AI systems or use cases.

2.Transparency Obligations & Related Provisions

Public disclosures:

Original AIDA Text (s. 11(1)): A person who makes available for use a high-impact system must, in the time and manner that may be prescribed by regulation, publish on a publicly available website a plain-language description of the system that includes an explanation of

(a) how the system is intended to be used;

(b) the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make;

(c) the mitigation measures established under section 8 in respect of it; and

(d) any other information that may be prescribed by regulation.

Proposed ISED Amendment (s. 11(1)(f)): A person who manages the operations of a high-impact system must in the time and manner prescribed by regulation, publish on a publicly available website a plain-language description of the system that includes the following information:

(i) how the system is being used,

(ii) the types of output that it generates,

(iii) the mitigation measures established under paragraph (b) in respect of it, and

(iv) any other information that may be prescribed by regulation;

Proposed ISED Amendment (s. 7(1)(f)): Before a general-purpose system is made available in the course of international or interprovincial trade and commerce for the first time, the person who makes it available for that first time must ensure that

(f) a plain-language description has been prepared of

(i) the system's capabilities and limitations

(ii) the risks of harm or biased output referred to in paragraph (c), and

(iii) any other information prescribed by regulation

Proposed ISED Amendment (s. 8(1)(a)): A person who makes a general-purpose system available must

(a) make the plain-language description referred to in paragraph 7(1)(f) available to users of the system or, if the system is made available to the public, publish that description, in the time and manner that may be prescribed by regulation, on a publicly available website; and

(b) take any measures prescribed by regulation

CBA Recommendation: We recommend removing the requirement on organizations to publicly disclose mitigation measures and risks under s.11(1)(f)(iii) (s.11 of the original Act) and 7(1)(f)(ii) and s.8(1)(a) respectively, as this could result in the disclosure of sensitive or otherwise confidential information of an organization or of a third-party, and additionally introduce risk to the organization or the public (e.g. compromising the efficacy of AI systems, exposing exploitable information related to critical systems) that may not be balanced with the benefits such a disclosure is intended to provide.

More generally, if the proposed disclosure requirements under s.11(1)(f) (s.11(1) of the original Act) and s.8(1)(a) are adopted, an exception should be introduced to provide greater certainty that organizations will not be compelled to reveal confidential business information or information regarding sensitive systems as this would result in greater (and avoidable) risk for organizations and the public (e.g. systems related to security or used to prevent financial crime)[1].

As written, the proposed disclosure requirements also risk resulting in the misallocation of organizational resources for managers of high-impact or general-purpose systems that are deployed in relatively low-risk use cases.

[1] S.11(1) of the original text of AIDA refers to requirements that are now listed under S.11(1)(f) of the proposed amendments.

To strike a better balance between the intent of AIDA to enhance the transparent use of AI systems with the need to protect organizations' confidential and sensitive information, we recommend that a *general account* of AI systems, including high-impact and general-purpose AI systems, similar to the provisions outlined in CPPA's s.62 (2), would provide an appropriate level of detail to the public without divulging system specific information. Incremental information, or detailed information on specific AI systems, could be provided to the Minister or Commissioner upon request or through audits.

Publication without consent: S.28(1) permits publication of information by the Minister without consent or notification to the person to whom the information relates.

CBA Recommendation: We recommend that an obligation be added under this section to first notify and consult with the impacted organization (or organizations) and institute some form of confirmation or resolution process, prior to the Government having the right to publish such information, which may be competitively sensitive, highly confidential, or both.

Disclosure to recipients: Under s.26(2), there is no legislative restriction on the recipient disclosing the data.

Recommendation: Such a restriction should be added along with a requirement for the recipient to maintain confidentiality of the information under the recipient's governing legislation.

3. **Clarifying Obligations Across the AI Value Chain**:

Original AIDA Text (s. 5 (2)): For the purposes of this Part, a person is responsible for an artificial intelligence system, including a high-impact system, if, in the course of international or interprovincial trade and commerce, they design, develop or make available for use the artificial intelligence system or manage its operation.

Proposed ISED Amendments[2]*:*

(s. 9 (1)): Developing machine learning models intended for high-impact use and associated requirements in sections 9(1)(a) to 9(1)(d)

(s. 10 (1)): Making a high- impact system available and associated requirements in sections 10(1)(a) to 10(1)(h)

(s. 11(1)): Managing operations of a high-impact system and associated requirements in sections 11(1)(a) to 11(1)(i)

(s. 7(1)): Making a general-purpose system available for the first time and associated requirements in sections 7(1)(a) to 7(1)(h)

(s. 8(1)): Making a general-purpose system available and associated requirements in sections 8(1)(a) to 8(1)(b)

(s. 8.2 (1)): Managing the operations of a general-purpose system and associated requirements in sections 8.2 (1)(a) to 8.2 (1)(g)

CBA Recommendation: We recommend greater clarity in the Act or under the regulations of AIDA to facilitate an unambiguous mapping of how the various roles / actors under the legislation relate to practical activities throughout the AI value chain of persons involved in the research, development, distribution, procurement, operationalization, and use of AI systems across different use-cases.

ISED will need to provide organizations with precise clarity on the distinctions and interdependencies between the various actors that the legislation aims to regulate, including, for example, developers of machine learning models intended for high-impact use, developers of high-impact systems (under the original text of the Act), persons making high-impact AI systems or general-purpose AI systems available for use (under the proposed amendments), and persons managing the operation of high-impact AI systems or general purpose AI systems. It is also unclear what role those who are responsible for changing a high-impact or general-purpose system (under s.10.2(1) and s.8.1(1) of the amendments) play under the Act and what their corresponding obligations are.

[2] This section lists the relevant clauses related to the various actors under AIDA and references their associated requirements under the Government's proposed amendments.

Without this clarity, organizations, and persons responsible, particularly those in heavily regulated industries, will be unable to effectively determine what they are and are not accountable for under the Act as well as the level of coordination and due diligence that is required to meet their proposed obligations.

We underscore the importance of ensuring that the Government does not assign unclear or overlapping responsibilities to multiple actors, particularly actors that would not have the requisite level of control or responsibility to carry out the prescribed activity.

Additionally, the significant interdependencies between various actors in the AI value chain prescribed under the amendments (including requirements to ensure other parties met their obligations under the law) need to be both clarified and minimized, as such contingencies could restrict or disincentivize Canadian organizations and other entities from using third-party AI systems and impact the ability of vendors to sell or license AI systems to Canadian organizations. This would negatively impact the ability of Canadian organizations to innovate and compete both locally and globally.

To avoid this outcome, greater clarity is ultimately needed on how organizations can meet requirements under sections 8.2(1), 9(1) and 10(1) of the proposed amendments (particularly as it relates to ensuring that other actors in the AI value chain have met their obligations under the law).

4. Other Considerations

a. **Serious Harm and Ceasing System Operations:** Supporting the Act's policy intent will require greater clarity on the meaning of and thresholds for both harm (physical, psychological, economic) and serious harm to provide the various actors with the operational certainty needed to ensure that they understand what obligations they are and are not accountable for under the Act.

Without the additional clarity on what constitutes serious harm, organizations will lack the operational certainty required when implementing Sections 8.2 (1)(e) and 11(1)(g) of the proposed amendments.

The proposed amendments (under Sections 8.2(1)(e) and 11(1)(g)) also introduce an obligation to cease the operations of a system if there are reasonable grounds to suspect that the use of the system has resulted, directly or indirectly, in serious harm or that the mitigation measures are not effective in mitigating risks of serious harm that could result from the use of the system.

We additionally recommend introducing exceptions to both of these proposed amendments (Sections 8.2 (1)(e) and 11(1)(g)) to address the need to mitigate the potential public harm that could result from the premature cessation of certain AI systems or general-purpose AI systems that perform a critical function (e.g., functions related to public safety, critical organizational, industry or public infrastructure or security).

Failing to include such exceptions could unintentionally expose organizations, individuals, or the public to avoidable harm. Therefore, it is crucial to strike a balance between the obligation to cease operations and the need to prevent unintended consequences that could potentially be more widespread or cause harm more serious than if the system continued operating.

b. **Overlap & Inconsistencies between AIDA, CPPA & Other Regulatory Expectations**: Addressing and avoiding any potential overlap between CPPA and AIDA (e.g., transparency requirements, measures respecting the use of data in the development of AI systems and varying thresholds of harm) will be critical to ensure that both operate effectively, to avoid inconsistencies, minimize complexity, and to avoid making it operationally difficult to comply with both laws, particularly for organizations that already operate in heavily regulated environments. We similarly recommend consideration be given to avoiding overlap and conflict between AIDA and other laws and regulations (such as human rights laws and sector specific laws).

Accountability Framework: We support the intent to ensure organizations are accountable for their own risk management practices within the Government's proposed Accountability Framework (s.12 in the Government's proposed amendments) but caution against introducing overly prescriptive requirements that risk adding avoidable complexity, without strengthening the accountable use of AI. For example, it is unclear how the benefits of a description of the roles and responsibilities and reporting structure for *all* personnel who contribute to making the artificial intelligence system available or who contribute to the management of its operations outweigh the avoidable complexity of doing so, for organizations of all sizes.

Consequently, we support the amendment introduced under section 12(6) that notes a person must take into account the nature and size of their business and the risks of harm or biased output that could result from the use of the artificial intelligence system under the Accountability Framework. As part of consultations for regulations, if the amendments are adopted, further exemptions will be required where duplicative obligations under the Accountability Framework overlap or conflict with existing regulatory expectations that organizations are expected to comply with.

c. **Administration & Enforcement**: We appreciate that the proposed amendments by ISED intend to create greater clarity around the role of the AI and Data Commissioner, yet we remain concerned about the Commissioner's lack of independence from the Minister, which will likely result in the same office being responsible for AIDA's policy and enforcement functions. Such a concentration of function could potentially result in enforcement being influenced by the policy intention, or other factors, rather than an impartial interpretation of the policy itself.

We remain concerned that significant aspects of the enforcement regime have been left to regulation, rather than being addressed in the statute (this stands in contrast to the CPPA portion of Bill C-27 which contains critical details related to the Act's administration and enforcement). Absent from AIDA are any procedural details for commencing or conducting the proceedings (which have been pushed to regulations). Other gaps that contribute towards greater uncertainty and heightened risk for organizations, given the significant penalties imposed by AIDA, include the lack of a tribunal (similar to what is contained in the privacy portion of the bill); no provisions with respect to evidence or other procedural requirements; and no informal dispute resolution mandate.

d. **Anonymization**: We support the proposed amendment to remove s.6 of AIDA, which avoids the introduction of duplicative or contradictory anonymization obligations between CPPA and AIDA.

e. **Implementation**: We urge the Government to provide organizations with a reasonable timeframe (at minimum two years) to implement AIDA's provisions as they are likely to impact the design, development, procurement, and deployment of AI systems, particularly given the potentially significant penalties for noncompliance.

We appreciate that many details of AIDA will be contained within forthcoming regulations and note this lack of clarity within the Act itself poses substantive challenges to organizations seeking to assess the implications of requirements under the Act. However, we understand that ISED intends to consult extensively on these regulations for AIDA. We are committed to actively participating in these discussions and to address key concerns that may arise from AIDA's regulations, including the various obligations applicable to and criteria for high-impact systems, machine learning models and general-purpose AI systems, record keeping requirements, measures with respect to the use of data, oversight and enforcement of AIDA, alignment, and regulatory details regarding biased output.