February 13, 2023

BSA COMMENTS ON BILL ON FOSTERING ARTIFICIAL INTELLIGENCE INDUSTRY AND SECURING TRUST [18726]

Submitted Electronically to the National Assembly's Science, ICT, Broadcasting, and Communications Committee, and the Ministry of Science and ICT

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to provide comments to the National Assembly's Science, ICT, Broadcasting and Communications Committee (**SIBCC**) and the Ministry of Science and ICT (**MSIT**) regarding Lawmaker Yoon Doo-Hyun's proposed *Bill on Act on Fostering AI Industry and Securing Trust (Draft No. 18726)* (the **Bill**). BSA understands that this Bill will be the foundation for the consolidated AI Bill currently being considered by SIBCC and MSIT.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing, data analytics, and AI products and services. As leaders in the development of cutting-edge technology, BSA's members have unique insights into both the tremendous potential of these new technologies and the government policies that can best support their responsible use and ensure continued innovation of such technologies.

AI has the potential to generate substantial economic growth and enable governments to provide better and more responsive government services, while addressing some of the most pressing societal challenges. However, we are concerned that binding legislation of the type proposed by the National Assembly may be premature and could inadvertently stymie efforts to develop effective mechanisms to promote these objectives in an environment that is so quickly evolving, both technologically and from a policy perspective. BSA has consistently engaged with MSIT and the SIBCC on regulating AI.[2] Our previous submissions highlighted, among other considerations, the importance of clearly distinguishing AI Developers from AI Deployers and alignment with internationally-recognized standards on AI. These considerations are still pertinent in respect of this Bill.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] See:

a) BSA Submission to the Republic of Korea on Regulating Artificial Intelligence, March 2022, https://www.bsa.org/files/policy-filings/en03182022rokregai.pdf (ENG) and https://www.bsa.org/files/policy-filings/kr03182022rokregai.pdf (KOR).

b) BSA Comments on Bill for the Act on Algorithms and Artificial Intelligence [13509], April 2022, https://www.bsa.org/files/policy-filings/en04192022algoai.pdf (ENG) and https://www.bsa.org/files/policy-filings/kr04192022algoai.pdf (KOR).

Summary of BSA's Recommendations

If the National Assembly proceeds to enact binding legislation regarding the treatment of "high-risk" AI, or if the Government of Korea decides to adjust to developing comprehensive voluntary guidelines instead, BSA recommends the following. **BSA's detailed recommendations and proposed textual amendments are described in Annex I**.

1. **Adopt the Organization for Economic Co-operation and Development (OECD)'s definition of AI.**

BSA recommends adopting the OECD's definition of AI. In its Recommendation of Council on Artificial Intelligence (**Recommendation**),[3] the OECD defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments", and specifies that AI systems are "designed to operate with varying levels of autonomy". Using a recognized and international definition, such as the OECD's, could facilitate international alignment, dialogue, adoption, and compliance.

2. **The definition of high-risk AI should be more specific.**

BSA recommends using the term "high-risk AI" instead of "artificial intelligence utilized in high-risk areas", and stating specifically that high-risk AI refers to AI that is: (i) deployed or used for any of the situations listed Article 2(3) of the Bill;[4] and (ii) poses a direct, substantial risk of harm to life or physical safety of individuals, or to the fundamental rights guaranteed to citizens of the Republic of Korea**.** In determining whether an AI is "high-risk", the focus should be outcomes-oriented and principles-based, i.e., placed on the manner in which the AI is deployed and its function, rather than categorizing an AI as "high-risk" simply because it is used in a specific sector.

3. **Recognize the different roles of AI Developers and AI Deployers and allocate obligations and responsibilities accordingly.**

The Bill should clearly distinguish entities which are involved in the development of AI (**AI Developers**) from entities which deploy and use AI (**AI Deployers**). This distinction is crucial as it allows responsibilities to be allocated in a manner which corresponds to the different roles and capabilities of stakeholders.[5] Currently, these two roles are covered by a single term under the current Bill – "AI industry". The lack of a clear distinction between AI Developers and Deployers means that their responsibilities and obligations are not clearly allocated and cannot be distinguished, which results in regulatory confusion. We recommend that MSIT and the SIBCC: 1) establish specific definitions for AI Developers and AI Deployers; 2) determine, when establishing obligations in the Bill, whether an AI Developer or AI Deployer or both are best placed to discharge the obligation; and 3) clearly state in the provisions which entities the obligation would apply to.

[3] Recommendation of the Council on Artificial Intelligence, May 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Per the Recommendation, the AI stakeholder community "encompasses all organizations and individuals involved in, or affected by, AI systems, directly or indirectly."

[4] Per Article 2(3), this includes: a) AI used for the supply of energy and drinking water; b) AI used in the provision of healthcare; c) AI used in medical devices; d) AI used in the safe management and operation of nuclear materials and facilities; e) AI used to analyze and utilize biometric information; f) AI used to make evaluations that have a significant impact on individual rights and obligations (e.g., recruitment and loan review); and g) other AI prescribed by Presidential Decree as having a significant impact on the safety and health of the people and the protection of fundamental rights.

[5] The OECD recognized the critical importance of distinguishing the multiple stakeholders involved in AI when it adopted the principles underlying the Recommendation. Specifically, the Recommendation recognizes that effective AI policies must necessarily account for "stakeholders according to their role and the context" in which AI is being deployed.

4. The definition of users should be more specific.

The existing definition of "user" leaves open the possibility that users themselves could be considered AI Deployers. BSA's proposed edits to the definition in Annex I seek to ensure that "users" are not also considered to be AI Deployers. Otherwise, this would result in tremendous uncertainty for all entities in the AI technology and service ecosystem as to which entity will need to be responsible for complying with the Bill's substantive requirements.

5. Obligation to notify users should extend only to high-risk AI Deployers.

On the obligation to notify users, BSA supports the Bill's intent of allocating the responsibility of notifying users to entities which adopt or use high-risk AI in their products and services, i.e., AI Deployers, instead of subjecting AI Developers this obligation. This allocation of responsibility reflects the reality that AI Developers are oftentimes not in a position to know the precise manner in which the technology is being deployed.

6. Clearly allocate responsibilities in respect of high-risk AI.

In the context of high-risk AI, the appropriate allocation of risk management responsibilities between AI Developers and AI Deployers should vary depending on: 1) the nature of the AI system being developed; 2) whether the AI Deployer is using the system consistent with the intended purpose for which it was developed; and 3) the extent to which the system may be substantially modified by the Deployer. BSA therefore urges MSIT and SIBCC to consider not just the roles and responsibilities of AI developers, but also the nature of the AI system being developed and the circumstances and means by which the underlying model is trained.

7. Encourage AI impact assessments

The Bill expresses support for "verification and certification activities… to secure the reliability of AI," allowing the Minister of Science and ICT to implement any projects in furtherance of this objective.[6] However, the risks that AI poses and the appropriate mechanisms for mitigating those risks are largely context-specific. The appropriate mechanisms for the collection and use of training data, record keeping, transparency, accuracy, and human oversight will also vary depending on the nature of the AI system and the setting in which it is deployed. BSA recommends that MSIT and SIBCC avoid prescribing inflexible certifications and instead encourage the use of process-based and outcome-oriented AI Impact Assessments. Impact assessments enable organizations to strengthen accountability, examine impacts of AI systems, and mitigate risks, including those related to harmful bias, product safety, and security. The recently-released Artificial Intelligence Risk Management Framework by the US's National Institute of Standards and Technology (**NIST**) is a useful reference in this regard.[7]

8. Align with internationally recognized standards to promote interoperability

AI systems are developed and deployed in an international context. It follows that AI regulations and standards should ideally operate across different jurisdictions, so as to facilitate and promote further adoption and use of AI technologies. In designing technical standards for AI, the Government should align them with the emerging body of internationally recognized standards to promote interoperability. BSA is encouraged to note that the Bill requires the Minister of Science and ICT to "maintain and

[6] Article 25 (Support of Verification and Certification of Reliability of Artificial Intelligence).

[7] Artificial Intelligence Risk Management Framework (AI RMF 1.0), National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

strengthen the cooperation system with international standards organizations or international standards institutions related to AI technology standards".[8] The International Organization of Standardization's (**ISO**) Standards Committee on AI[9] has completed work on 10 sets of standards, including on bias in AI systems and approaches to enhance trustworthiness in AI,[10] and is currently developing 27 additional standards. The risk of establishing domestic standards that are not well aligned, or are too far ahead of international standards development, is that requirements will be out of step with emerging practices, deterring development of AI in Korea and impeding efforts to ensure that the technology is developed and deployed responsibly. **Consequently, BSA strongly encourages leveraging and supporting international standards bodies' ongoing work in this regard and cautions against the development of a Korea-specific standard.**

Conclusion

BSA works closely with governments around the world to promote the development of policies that encourage the responsible development and use of AI.[11] To that end, BSA has identified five key pillars for Responsible Artificial Intelligence. These pillars reflect how both industry and government have important roles to play in promoting the benefits and mitigating the potential risks involved in the development, deployment, and use of AI:

1. **Building Confidence and Trust in AI Systems:** Highlighting industry efforts to ensure AI systems are developed in ways that maximize fairness, accuracy, data provenance, explainability, and responsibility.

2. **Sound Data Innovation Policy:** Promoting data policies that are conducive to the development of AI and other new data-driven technologies including reliable legal mechanisms that facilitate cross-border data transfers, legal certainty for value-added services (e.g., text and data mining, machine learning), and enhanced access to non-sensitive government data.

3. **Cybersecurity and Privacy Protection:** Advocating for policies that strengthen enhanced security measures and respect informed consumer choices while ensuring the ability to deliver valuable tailored products and services.

4. **Research and Development:** Supporting investment in efforts that foster confidence and trust in AI systems, promote coordination and collaboration between industry and government, and help grow the AI workforce pipeline.

5. **Workforce Development:** Identifying opportunities for government and industry to collaborate on initiatives to prepare the workforce for the jobs of the future.

BSA acknowledges both the importance of AI and the risks associated with certain uses of the technology. In response to the risk of bias, BSA published a report titled "**Confronting Bias: BSA's Framework to Build Trust in AI"**[12] to provide a guide that organizations can use to perform impact

[8] Article 15(3) (Standardization of AI Technology).

[9] See ISO/IEC JTC 1/SC 42 at https://www.iso.org/committee/6794475.htm.

[10] See ISO/IEC TR 24027: 2021 (Bias in AI systems and AI aided decision making) at https://www.iso.org/standard/77607.html?browse=tc and ISO/IEC TR 24028:2020 (Overview of trustworthiness in artificial intelligence) at https://www.iso.org/standard/77608.html?browse=tc

[11] BSA AI Policy Overview, accessible at https://ai.bsa.org/

[12] Confronting Bias: BSA's Framework to Build Trust in AI, June 2021, https://ai.bsa.org/wp-content/uploads/2021/06/2021bsaaibias.pdf (ENG) and https://ai.bsa.org/wp-content/uploads/2021/07/2021bsaaibiaskr.pdf (KOR).

assessments to identify and mitigate risks of bias that may emerge throughout an AI system's lifecycle.

We appreciate the opportunity to provide recommendations on the Bill. Please do not hesitate to contact BSA if you have any questions regarding this submission or if we can be of further assistance.

Sincerely,

Tham Shen Hong

Tham Shen Hong
Manager, Policy – APAC
shenhongt@bsa.org
+65 91719408

ANNEX I: DETAILED RECOMMENDATIONS

Align definition of AI with the OECD's definition

Original	Suggestion
Article 2 (Definition) (2) The term “artificial intelligence (AI)” refers to the ability of implementing human intellectual capabilities such as learning, reasoning, perception, judgment, and understanding of language in electronical ways.	**Article 2 (Definition)** (2) The term “artificial intelligence (AI)” ~~refers to the ability of implementing human intellectual capabilities, such as learning, reasoning, perception, judgement and understanding of language in electronical ways.~~ means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.
Explanation: AI systems are developed and deployed in an international context. It follows that the regulations and standard that apply to AI should operate across different jurisdictions, to facilitate and promote further adoption and use of AI technologies. In this regard, we propose using the OECD's definition of AI. In its Recommendation of Council on Artificial Intelligence (**Recommendation**),[13] the OECD defines AI as “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments”, and specifies that AI systems are “designed to operate with varying levels of autonomy”. This definition has been referenced by regulators worldwide, including the European Union.[14] Using a recognized and international definition, such as the OECD's, could facilitate international alignment, dialogue, adoption, and compliance.	

Definition of high-risk AI should be more specific

Original	Suggestion
Article 2 (Definitions) (3) The term “AI utilized in high-risk areas” means AI that falls under any of the following items and that is likely to have a significant impact on the protection of human life, physical safety, and fundamental rights.	**Article 2 (Definitions)** (3) The term ~~“AI utilized in high-risk areas”~~ “high-risk AI” means AI that: (i) ~~falls under any of the following items,~~ is deployed or used for any of the following situations; and (ii) ~~that is likely to have~~ poses a direct, substantial risk of harm to ~~significant impact on the protection of human~~ the life or~~,~~ physical safety of individuals, or to

[13] Recommendation of the Council on Artificial Intelligence, May 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Per the Recommendation, the AI stakeholder community “encompasses all organizations and individuals involved in, or affected by, AI systems, directly or indirectly.”

[14] The European Union's draft Artificial Intelligence Act currently defines “artificial intelligence system” as “software that … can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with”.

<table>
<tr><td></td><td>~~and protection of~~ the fundamental rights guaranteed to citizens of the Republic of Korea.</td></tr>
<tr><td colspan="2"><b>Explanation:</b>
To make the policy intention clearer, we propose stating specifically that high-risk AI refers to AI that is used in a manner that has a legal or similarly significant effect on an individual.
BSA also notes that, as currently drafted, the requirements for determining what is AI used in high-risk areas should apply cumulatively. In other words, the AI must: (a) harm a person’s safety/infringe on basic rights; AND (b) must be deployed or used in a manner that is considered “high-risk” (e.g., “used to supply energy”). This avoids situations where low-risk AI (e.g., payroll processing AI) that are used in certain industries, such as energy or healthcare, are categorized as “high-risk AI” by default.
<b>BSA supports this approach of determining whether an AI is “high-risk” based on the manner in which the AI is deployed and its function rather than categorizing an AI as “high-risk” simply because it is used in a specific sector.</b></td></tr>
</table>

Provide specific definitions for AI developers and AI deployers and allocate responsibilities accordingly

<table>
<tr><th>Original</th><th>Suggestion</th></tr>
<tr><td><b>Article 2 (Definitions)</b>
(5) The term “AI industry” means an industry that develops, manufactures, produces, or distributes AI technologies or products (hereinafter referred to as "AI products") or provides service(s) related thereto (hereinafter referred to as "AI services").
(6) The term “AI business operator” means a person engaged in economic activities related to the AI industry.</td><td><b>Article 2 (Definitions)</b>
~~(5) The term “AI industry” means an industry that develops, manufactures, produces, or distributes AI technologies or products (hereinafter referred to as "AI products") or provides service(s) related thereto (hereinafter referred to as "AI services").~~
~~(6) The term “AI business operator” means a person engaged in economic activity related to the AI industry.~~
(5) The term “AI Developers” means entities that design, code, produce, or modify AI systems, whether for internal use or for use by third parties.
(6) The term “AI Deployers” means entities that adopt and use AI systems. If a deployer develops its own AI system, it is both the AI developer and AI deployer.</td></tr>
<tr><td colspan="2"><b>Explanation:</b>
<b>The Bill should clearly distinguish entities which are involved in the development of AI (i.e., AI Developers) from entities which deploy and use AI (i.e., AI Deployers).</b> This distinction is crucial as it allows responsibilities to be allocated in a manner which corresponds to the different</td></tr>
</table>

roles and capabilities of stakeholders.[15] Currently, these two roles are covered by a single term – “AI industry”.

The lack of a clear distinction between AI Developers and Deployers means that their responsibilities and obligations are not clearly allocated, which results in regulatory confusion and entities taking on, or compelled to meet, obligations they are ill-suited to discharge. For example, Article 27 requires persons who intend to provide products or services using high-risk AI to notify its users to that fact. AI Developers, however, would find this obligation difficult, if not impossible, to meet because an AI Developer will not know in advance how their customers will train or use the AI in their own commercial or organizational contexts.

On the other hand, there are also circumstances in which an AI Developer and AI Deployer are the same entity. For instance, if a company develops an in-house AI system and proceeds to deploy it in the course of its business operations, it is both an AI developer and AI deployer.

In light of the above considerations, BSA urges MSIT and the SIBCC to: 1) establish specific definitions for AI Developers and AI Deployers; 2) determine, when establishing obligations in the Bill, whether an AI Developer or AI Deployer or both are best placed to discharge the obligation; and 3) clearly state in the provisions which entities the obligation would apply to.

Definition of “users” should be more specific

<table>
<tr><th>Original</th><th>Suggestion</th></tr>
<tr><td><b>Article 2 (Definition)</b>
(7) The term “user” means a person who receives AI products or AI services.</td><td><b>Article 2 (Definition)</b>
(7) The term “user” means a person who receives AI products or AI services, and who uses the product or service as the final user of the product or service and is not an AI Deployer.</td></tr>
<tr><td colspan="2"><b>Explanation:</b>
The existing definition of “user” leaves open the possibility that users themselves could be considered AI Deployers. <b>The proposed edits to the definition seek to ensure that “users” are not also considered to be AI Deployers.</b> Otherwise, this would result in tremendous uncertainty for all entities in the AI technology and service ecosystem as to which entity will need to be responsible for complying with the bill’s substantive requirements.</td></tr>
</table>

Article 26 should be amended for consistency with the definition of “high-risk AI” proposed above

Original	Suggestion
Article 26 (Confirmation of Artificial Intelligence Used in High-risk Areas) (1) A person who intends to develop, utilize, or provide AI or products or services using the AI under each item of Subparagraph 3 of Article 2 may request the Minister of Science and ICT to	**Article 26 (Confirmation of Artificial Intelligence Used in High-risk Areas)** (1) A person who intends to develop, utilize, or provide AI or products or services using the AI under each item of Subparagraph 3 of Article 2 may request the Minister of Science and ICT to

[15] The OECD recognized the critical importance of distinguishing the multiple stakeholders involved in AI when it adopted the principles underlying the Recommendation. Specifically, the Recommendation recognizes that effective AI policies must necessarily account for “stakeholders according to their role and the context” in which AI is being deployed.

confirm whether the AI is utilized in high-risk areas or not. (2) Upon request pursuant to Paragraph (1) hereof, the Minister of Science and ICT shall confirm whether AI is utilized in high-risk areas or not, and may establish an expert committee to make the person receive relevant advice, if necessary. (3) The Minister of Science and ICT may establish and disseminate the guidelines on standards, examples, etc. of AI utilized in high-risk areas. (4) Matters necessary for confirmation procedures, etc. pursuant to Paragraphs (1) and (2) hereof shall be prescribed by the Presidential Decree.	confirm whether the AI is ~~utilized in~~ high-risk AI~~areas~~ or not. (2) Upon request pursuant to Paragraph (1) hereof, the Minister of Science and ICT shall confirm whether AI is ~~utilized in~~ high-risk AI~~areas~~ or not and may establish an expert committee to make the person receive relevant advice, if necessary. (3) The Minister of Science and ICT may establish and disseminate the guidelines on standards, examples, etc. of ~~AI utilized in~~ high-risk AI~~areas~~. (4) Matters necessary for confirmation procedures, etc. pursuant to Paragraphs (1) and (2) hereof shall be prescribed by the Presidential Decree.
Explanation: These proposed amendments seek to ensure consistency with our proposal for the term "high-risk AI" to be used (see "*Definition of high-risk AI should be more specific*" above).	

Obligation to notify users should extend only to high-risk AI deployers

Original	Suggestion
Article 27 (Duty of Notification of AI Utilized in High-Risk Areas) (1) A person who intends to provide a product or service using AI utilized in high-risk areas shall notify users in advance that the product or service is operated based on AI utilized in high-risk areas. (2) The notification pursuant to Paragraph (1) hereof shall be provided in a way that users can easily understand, such as posting it on the website of the person who provides the product or service or including it in the manual of the product or service.	**Article 27 (Duty of Notification of AI Utilized in High-Risk Areas)** ~~(1) A person who intends to provide a product or service using AI utilized in high-risk areas shall notify users in advance that the product or service is operated based on AI utilized in high-risk areas.~~ (1) When an AI Deployer adopts or uses high-risk AI in the course of providing its products and services to users, it shall notify users that it is adopting or using high-risk AI. (2) The notification pursuant to Paragraph (1) hereof shall be provided in a way that users can easily understand, such as posting it on the website of the person who provides the product or service or including it in the manual of the product or service.
Explanation:	

Article 27 requires persons who intend to provide products or services using high-risk AI to notify its users to that fact. The wording of Article 27 suggests that entities that *develop* AI are not subject to this obligation. If so, BSA supports the policy intent behind this provision, as it allocates the responsibility of notifying users to entities which adopt or use high-risk AI in their products and services, i.e., AI Deployers, instead of subjecting AI Developers to an obligation that would be difficult, if not impossible, to meet because an AI Developer will not know in advance how their customers will train or use the AI in their own commercial or organizational contexts. This allocation of responsibility reflects the reality that AI Developers are oftentimes not in a position to know the precise manner in which the technology is being deployed. BSA's proposed amendments are intended to make this policy intention clearer.

Clearly allocate responsibilities in respect of high-risk AI

If the final legislation were to include an Article setting out further responsibilities of "AI-related businesses" in high-risk areas, e.g., requiring such businesses to take measures to ensure the reliability and safety of their AI systems, such an Article should clearly state the distinct roles and responsibilities of AI Developers and AI Deployers in ensuring that high-risk AI are developed and deployed in a safe and secure manner. This will help both sets of entities understand which measures would apply to them. It is also important to specify if a measure would apply to AI Developers, AI Deployers, or both, as the measure should correspond to their different roles and capabilities. We propose including the following language:

Suggestion
Article XX (Responsibility of AI Developers and AI Deployers in respect of high-risk AI) (1) AI Developers shall take measures to ensure the reliability and safety of high-risk AI that they have designed or developed. AI Deployers shall take measures to ensure the reliability and safety of high-risk AI that they have adopted, used, or otherwise deployed. For the avoidance of doubt, such measures shall specify whether a measure will apply to AI Developers, AI Deployers, or both.

In the course of determining the measures that AI Developers and AI Deployers may need to undertake with regard to high-risk AI, it also bears noting that the appropriate allocation of risk management responsibilities between AI Developers and AI Deployers will vary depending on the nature of the AI system being developed, whether the Deployer is using the system consistent with the intended purpose for which it was developed, and the extent to which the system may be substantially modified by the Deployer. **BSA therefore urges MSIT and SIBCC to consider not just the roles and responsibilities of AI developers, but also the nature of the AI system being developed, as well as the circumstances and means by which the underlying model is trained.**