August 18, 2023

BSA COMMENTS ON DRAFT ARTIFICIAL INTELLIGENCE BILL

Introduction

BSA | The Software Alliance (**BSA**)[1] appreciates the leadership by the Government of Thailand in developing draft acts to promote and support Artificial Intelligence (**AI**) innovation, in particular the Draft AI Bill on Promotion and Support of Artificial Intelligence Innovation of Thailand (**Draft AI Bill**) and the accompanying Draft Notification on Guideline for Setting Criteria and Risk Assessment Methods from the Use of Artificial Intelligence Systems (**Draft Notification for Risk Assessment)** proposed by the Electronic Transactions Development Authority (**ETDA**). We welcome the opportunity to submit comments to the Government of Thailand, including the Ministry of Digital Economy and Society (**MDES**) and the ETDA, on AI regulation and the Draft AI Bill.

BSA is the leading advocate for the global software industry. Our members are enterprise software companies that create business-to-business technologies that help other businesses innovate and grow.[2] For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, and collaboration software. BSA members are on the leading edge of providing AI-enabled products and services, and tools used by others in the development and deployment of AI systems and applications. As a result, they have unique insights into the technology's tremendous potential to spur digital transformation and the policies that can best support the responsible use of AI.

Summary of BSA's Recommendations

BSA respectfully presents our comments on the Draft AI Bill and Draft Notification for Risk Assessment to the MDES, ETDA, and other relevant stakeholders, specifically the following recommendations.

- **Develop a coordinated approach to AI regulation within Thailand**: coordination between the various government agencies to support a coherent and harmonized national approach to regulating AI within Thailand by:

  (a) setting out clear roles and responsibilities of each of the government agencies involved in governing and regulating AI;
  (b) consulting extensively with key stakeholders including private sector entities, and allowing sufficient time for robust engagement; and
  (c) communicating clear timelines and milestones for public consultation.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, 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 https://www.bsa.org/policy-filings/artificial-intelligence-in-every-sector.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

- **Set definitions that are in line with international understanding**:

  (a) adopt the definition of AI by the Organisation for Economic Co-operation and Development (**OECD**); and
  (b) define and distinguish the roles of AI developers and deployers.

- **Define roles and responsibilities in the AI ecosystem**: obligations should fall on the entity that is best positioned to both identify and efficiently mitigate the risk of harm

- **Adopt a risk-based approach to AI regulation**: AI regulatory efforts should focus on addressing high-risk use cases.

- **Impact assessments**: promote the use of impact assessments to mitigate risks arising from high-risk uses of AI systems, with appropriate documentation requirements for developers and deployers of high-risk AI.

- **Recognize the importance of contracts to supporting responsible AI**: embrace a flexible approach to AI regulation and avoid prescriptive requirements by focusing on the factors stakeholder should consider in evaluating the relevant and appropriate metrics for the AI use case.

- **Align with emerging internationally recognized standards** such as those set by the International Organization of Standardization's (**ISO**) and the US National Institute of Standards and Technology (**NIST**).

Coordinated approach to developing AI regulation within Thailand

BSA commends the Government of Thailand on the development of the National AI Strategy and Action Plan (2022-2027)[3] to promote AI development and application to enhance the economy and quality of life of Thai people through the National Electronics and Computer Technology Center (**NECTEC**), and on the efforts by MDES agencies to develop regulations and other measures related to AI.

We welcome ETDA's efforts to promote and support innovation in AI within the Draft AI Bill, and to manage risks that may arise from the use of AI systems. We also appreciate efforts by the Office of the National Digital Economy and Society Commission (**ONDE**) to consult on the draft Royal Decree on Business Operation that use AI Systems, which seeks to establish regulations, measures and standards related to AI. BSA recommends coordination between the various government agencies to support a coherent and harmonized approach to regulating AI within Thailand by (a) setting out clear roles and responsibilities of each of the government agencies involved in governing and regulating AI; (b) consulting extensively with key stakeholders including private sector entities, and allowing sufficient time for robust engagement; and (c) communicating clear timelines and milestones for public consultation. BSA is appreciative of the ETDA for holding a public hearing on the Draft AI Bill and welcomes the opportunity to provide comments.

[3] See https://www.nectec.or.th/en/about/news/cabinet-national-ai-strategy.html.

BSA's Perspective on AI

BSA's views are informed by our recent experience working with member companies to develop the BSA Framework to Build Trust in AI,[4] a risk management framework to mitigate the potential for unintended bias throughout an AI system's lifecycle. Built on a vast body of research and informed by the experiences of leading AI developers, the BSA Framework outlines a lifecycle-based approach for performing impact assessments to identify risks of AI bias, and highlights corresponding risk mitigation best practices. BSA has testified before the United States Congress[5] and the European Parliament[6] on the Framework and its approach to mitigating AI-related risks. BSA and its members are eager to work with the Government of Thailand to enable AI to be developed and used responsibly in support of Thailand's economic growth, competitiveness, and job creation.

While the adoption of AI provides unquestionable benefits for organizations, consumers, and society, we also recognize that if this technology is not developed and deployed responsibly, it can result in significant risks. BSA recognizes that AI can be used in harmful ways. For example, AI systems may unlawfully discriminate against individuals. As such, the public should be assured that such systems have been thoroughly vetted to identify and mitigate risks such as unintended bias.

To achieve this objective, we provide the following recommendations and attach relevant documents which we hope will be useful resources to MDES, ETDA, ONDE, and relevant agencies in developing AI regulation. These include "Confronting Bias: A Framework to Build Trust in AI" (**BSA Framework**), a first-of-its-kind risk identification and mitigation impact assessment framework for AI systems,[7] and "AI Developers and Deployers: An Important Distinction," which explains the different roles of developers and deployers upon considering tailored obligations to an organization's role in the AI marketplace.[8]

Overview of developments in AI around the world

We at BSA have been monitoring the developments on AI-related policy and regulation all over the world. In the United States (**US**), the Biden Administration has pursued a deliberative approach on AI policy, conducting several consultations on a range of issues, including a request for information on national priorities for AI issued by the White House Office of Science and Technology Policy and a request for comment on AI accountability issued by the National Telecommunications and Information Administration.[9] In January 2023, after consultation with a wide array of stakeholders including industry and civil society, NIST – which is part of the US Department of Commerce – released an AI Risk Management Framework.[10] The NIST AI Risk Management Framework is a voluntary framework that provides guidance on how to identify and mitigate AI risks. In Congress and state legislatures, AI legislation has been introduced on several topics, including government use of AI, employment, and impact assessments for high-risk uses of AI.

---

[4] See https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai

[5] See https://www.congress.gov/117/meeting/house/114125/witnesses/HHRG-117-BA00-Wstate-CooperA-20211013.pdf

[6] See https://www.europarl.europa.eu/cmsdata/244265/AIDA_Verbatim_30_November_2021_EN.pdf

[7] https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai

[8] https://www.bsa.org/policy-filings/ai-developers-and-deployers-an-important-distinction

[9] BSA submitted comments on both consultations. See BSA | The Software Alliance, BSA | The Software Alliance Comments on the White House Office of Science and Technology Policy Request for Information on National Priorities for Artificial Intelligence (July 6, 2023), available at https://www.bsa.org/files/policy-filings/07062023ostpai.pdf; BSA | The Software Alliance, BSA | The Software Alliance Comments on the National Information and Telecommunications Administration's AI Accountability Policy Request for Comment, available at https://www.bsa.org/files/policy-filings/06092023ntiaaicmt.pdf.

[10] See https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

In the European Union (**EU**), the EU AI Act is undergoing the "Trilogue" negotiation process, with final approval expected towards the end of 2023. The debate on AI has largely centered around the definition of AI, high-risk AI use cases, conformity assessments, quality management systems, and most recently foundation models.

In Japan, the ruling Liberal Democratic Party released a White Paper on AI to provide recommendations on Japan's National AI Strategy. Subsequently, the Government of Japan established an AI Strategy Council to set direction on how to accelerate AI adoption and promote the use of AI, enhance AI development capabilities in Japan, and address concerns and risks on AI.

In Singapore, the Personal Data Protection Commission released the Model AI Governance Framework[11] and the Infocomm Media Development Authority (**IMDA**) developed AI Verify, an AI governance testing framework and software toolkit. The IMDA also set up the AI Verify Foundation to develop AI Verify testing tools for the responsible use of AI,[12] as well as released a discussion paper on "Generative AI: Implications for Trust and Governance".[13]

Multilateral groupings are also coming together to develop plans on governing AI. For example, the Group of Seven Nations (**G7**) recently agreed on the "Hiroshima AI process" to create a ministerial forum to discuss issues around AI regulation. Closer to home, ASEAN is developing a Guide to AI Governance and Ethics, which will focus on the responsible and ethical use of AI. BSA supports these multilateral initiatives as they promote harmonized approaches to AI governance and regulation.

There has been some convergence in policy and regulatory developments around the world. Examples include definitions of AI-related terms, including increasing support for defining AI in line with the OECD's definition of an AI system, taking a risk-based approach to regulating AI by focusing regulatory requirements on high-risk uses of AI, and recognizing the different roles that developers of AI systems and deployers of AI systems play in identifying and mitigating risks associated with AI systems. Convergence in these areas can be found in the EU AI Act and the NIST AI Risk Management Framework.

Definitions for AI-related terms

Given that AI systems are developed and deployed in an international context, regulations and standards that apply to AI should operate across different jurisdictions to facilitate and promote further adoption and use of AI technologies. Definitions pertaining to AI should ideally be aligned across jurisdictions to ensure that all stakeholders have a common understanding of AI.

Definition of AI. BSA proposes that Thailand adopts the definition of AI by the OECD. In its Recommendation of the Council on Artificial Intelligence (**Recommendation**),[14] 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 EU.[15] The US NIST also adapts the OECD definition for use in its AI Risk Management Framework. Further, as part of the work of the US-EU Trade and Technology Council, the US and the EU are agreeing on shared interpretations of key defined terms. For example, the EU-US Terminology and Taxonomy for Artificial Intelligence defines machine learning as

[11] See https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf.

[12] See https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework.

[13] See https://aiverifyfoundation.sg/downloads/Discussion_Paper.pdf.

[14] 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."

[15] 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".

a branch of AI "and computer science which focuses on development of systems that are able to learn and adapt without following explicit instructions imitating the way that humans learn, gradually improving its accuracy, by using algorithms and statistical models to analyse and draw inferences from patterns in data."[16]

Definition of Developers and Deployers of AI Systems. To reflect the inherently dynamic nature of AI systems, it is crucial to define, and consequently distinguish, the AI developer and the AI deployer. Policies pertaining to AI must account for the array of stakeholders that may play a role in various aspects of a system's design, development, and deployment. The OECD's Recommendation states that effective AI policies must necessarily account for "stakeholders according to their role and the context" in which AI is being deployed.[17] While the Draft AI Bill defines an AI entrepreneur who sells goods or provides services related to AI, the definition does not take into account the roles and responsibilities of the various stakeholders involved.

In general, there are at least two key stakeholders with varying degrees of responsibility for managing the risks associated with an AI system throughout its lifecycle:

- **AI developers:** An AI developer is an entity that designs, codes, or produces an AI system.
- **AI deployers:** An AI deployer is an entity that uses an AI system. (If an entity develops an AI system for its own use, it may be both the AI developer and the AI deployer.)

BSA recommends that the Draft AI Bill separately define AI developers and AI deployers.

Prioritizing international alignment in defining AI-related terms will: (a) reduce discrepancies and conflicts between different legal frameworks, thus promoting compliance; (b) serve as foundation for dialogue and cooperation between governments on AI-related risks; and (c) support the international development of best practices and benchmarks for using AI systems safely, allowing AI systems to be deployed responsibly on a global scale.

Roles and responsibilities in the AI ecosystem

In addition to separately defining the developers of an AI system and the deployers of an AI system, the Draft AI Bill should assign both types of entities obligations that reflect their different roles. Effective management of risks among these different actors will depend on the nature of the AI system being developed. Distinguishing between AI developers and AI deployers ensures that specified obligations reflect an entity's role in the AI ecosystem. Tailoring obligations to an entity's role as an AI developer or AI deployer enables the company to fulfill the corresponding obligations and better protect consumers.

For example, an AI developer that creates an AI system is well-positioned to have access to information about the type of data that is used to train an AI system, the system's known limitations, and its intended use cases. However, the AI developer would *not* have insight into how the AI system is used after another organization has purchased and deployed the AI system. Instead, the AI deployer – the entity using the AI system – is generally best positioned to provide details on how the system is being used, the outputs from the AI system, the nature of any customer complaints, and other real-world factors affecting the system's performance. AI deployers are also best positioned to understand the risks that a specific use of an AI system may present to individuals. Ensuring AI policies create obligations that reflect these different roles will enable all stakeholders to better understand how their organizations can identify and address harmful bias in AI systems.

---

[16] EU-US Terminology and Taxonomy for Artificial Intelligence, May 2023, https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence.

[17] OECD Recommendation (2019). Per the Recommendation, the AI stakeholder community "encompasses all organizations and individuals involved in, or affected by, AI systems, directly or indirectly."

Both types of entities should have their respective obligations to ensure responsible AI innovation, and those obligations should be tailored to their different roles in the ecosystem.

In summary, BSA recommends that as ETDA develops its AI regulatory and governance approach, the proposed obligations should fall on the entity that is best positioned to both identify and efficiently mitigate the risk of harm.

Risk-based approach

The AI ecosystem is broad, encompassing a diverse range of technologies and use cases and a wide array of stakeholders. Because the risks of AI are inherently use-case specific, any regulations should focus on specific applications of the technology that pose higher risks to the public but should be flexible enough to account for the unique considerations that may be implicated by specific use cases.

As a general principle, the scope of any regulatory obligations should be a function of the degree of risk and the potential scope and severity of harm. Many AI systems pose extremely low, or even no, risk to individuals or society, while creating potentially significant benefits. Imposing onerous regulations on such low-risk systems would hamper AI innovation with few corresponding benefits and therefore limit opportunities to use AI for positive impact. For example, AI is a critical component of cybersecurity risk mitigation,[18] which creates significant benefits to both companies and to consumers. Policymakers should be mindful of the unintended consequences of regulations that could inadvertently limit the deployment of AI in beneficial use cases, such as detecting and responding to ever-evolving cybersecurity threats.

AI regulatory efforts should focus on addressing high-risk AI use cases. For example, AI systems may be high-risk if they are used to make decisions to hire, promote, or terminate an individual's employment, or in other contexts, to determine eligibility for credit, healthcare, or housing. In sum, BSA recommends that regulatory efforts should be focused on high-risk AI use cases. Indeed, this would be in line with regulatory approaches around the world such as the EU AI Act, which focuses on regulating high-risk AI use cases.

In line with the risk-based approach discussed above, BSA supports the requirement under Chapter 5 of the Draft AI Bill for organizations to assess the level of risk an AI system poses in the first instance. Following the determination that an AI system is high-risk, it would then be necessary to conduct an AI impact assessment. Those would be unnecessary for low-risk use cases. BSA welcomes the alignment of impact assessment requirements and checklists as detailed under the Draft Notification on Guideline for Setting Criteria and Risk Assessment Methods from the Use of Artificial Intelligence Systems (**Draft Notification for Risk Assessment**) with the NIST AI Risk Management Framework.

Impact assessments

Impact assessments should play a significant role in ETDA's approach to AI risk management. Impact assessments are an important accountability mechanism used in other fields – from environmental protection to data protection – and can be applied to AI, as they can be used to help AI developers and deployers of AI systems for high-risk uses identify and mitigate risks throughout the lifecycle of an AI system. By allowing personnel across the organization to examine the objectives, data preparation, design choices, and testing results, impact assessments help to drive internal changes to an organization's risk management program. Implementing these changes enables organizations to better address existing concerns and adapt to new risks as they emerge. The fact that assessments are being performed for high-risk uses of AI systems also promotes trust for external stakeholders because they will know that an organization is conducting a thorough examination of AI systems, and that the assessments are available to regulators upon request in the event of an investigation.

[18] An organisation could face millions of indicators of compromise per day and security teams demand contextual awareness and visibility from across their entire environments. Cybersecurity providers that leverage AI can detect and respond to both known and unknown threats in real-time, with speed and scale to match.

A recent report on AI accountability also concluded that impact assessments had several advantages over other accountability tools, noting that: 1) they are familiar to organizations already conducting impact assessments for privacy and data protection; 2) they are practical because they do not rely on technical standards, which are currently nascent; and 3) they are future-proof because they can adapt as AI systems and AI governance evolve.[19]

In Article 8 of the Draft Notification for Risk Assessment, there is a requirement for the ETDA to arrange for a review of the risk assessment and management checklists "when it is necessary or when the technology changes to be effective in proper security protection based on the factors of technology, context, environment, required resources and the possibility of a combination of operations." BSA recommends either deleting "when it is necessary" from Article 8 or providing specific scenarios for when such a review by ETDA would be necessary.

Article 8 of the Draft Notification for Risk Assessment further requires that the review of AI risk assessment and management checklist shall be "comprehensively done through hearing from individuals involved and affected people." Although developers and deployers may consult affected individuals to, for example, assess potential harms, it is important to note that one reason that impact assessments create a strong accountability tool is that they are conducted internally through confidential assessments. One of the goals of impact assessments is to drive internal changes, and organizations will likely conduct less thorough reviews to surface problems if the results ultimately will either be made public or be shared with third parties. In addition, impact assessments will likely contain confidential business information that organizations want to protect. Further, sharing sensitive information with third parties could result in privacy and security concerns. Accordingly, we recommend that the process of conducting an impact assessment remain an internal exercise without third-party auditors or publication of the results.

For the reasons discussed above, BSA strongly supports the use of impact assessments to mitigate risks arising from high-risk uses of AI systems. The BSA Framework similarly recommends the use of impact assessments for high-risk uses of AI systems and is appropriate for organizations to implement to enhance AI accountability. For example, when using impact assessments to manage AI risks, both AI developers and deployers should document key aspects of AI systems, which are important reference points for understanding the operation of AI systems. However, the information to be documented will be different for developers that design an AI system than for deployers using an AI system:

- **Developers of high-risk AI systems** should document information including, as appropriate:
    - The intended purpose of the AI system;
    - Known limitations of the AI system;
    - Known, likely, and specific high risks that could occur and steps taken to mitigate those risks;
    - An overview of the data used to train the AI system; and
    - A summary of how the AI system was evaluated prior to sale.

[19] Impact Assessments: Supporting AI Accountability & Trust, January 2023, https://accesspartnership.com/impact-assessments-supporting-ai-accountability/

- **Deployers of high-risk AI systems** should document information including, as appropriate:
    - The purpose for which the deployer intends to use the AI system;
    - Transparency measures, including notices to impacted individuals about the AI system's use;
    - A summary of how the AI system is evaluated, if applicable;
    - Known, likely, and specific high risks that could occur and steps taken to mitigate those risks; and
    - Post-deployment monitoring and user safeguards, if applicable.

As such, we recommend that the Draft Notification for Risk Assessment include appropriate documentation requirements for developers and deployers of high-risk AI.

Recognize importance of contracts to supporting responsible AI

BSA recommends avoiding prescriptive requirements, whether on setting standards for AI in Chapter 3 of the Draft AI Bill, or setting standards for contracts governing entities offering AI services in Chapter 4. Further, the introduction of domestic certification in the absence of established internationally recognized standards may result in several drawbacks, such as fragmentation and the lack of international interoperability, reduced market access for domestic companies to expand overseas, and missed opportunities for international collaboration.

One of the primary reasons to embrace a flexible approach to AI regulation is the dynamic and diverse nature of AI applications. Each sector may have unique challenges and requirements that cannot be adequately addressed with rigid and highly specific requirements. Prescriptive requirements will be rapidly outmoded as the technology develops, and, if out of step with internationally recognized standards, will affect interoperability and the development and deployment of AI solutions across borders. This will run the risk of stifling AI innovation, which undermines Thailand's desired outcome.

As highlighted earlier, the risks that AI poses and the appropriate mechanisms for mitigating 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. A prescriptive approach could impede efforts to address the very risks policy makers and governments intend to prevent, add unnecessary costs, and require extremely complex compliance checks. Regulation should focus instead on the factors stakeholders should consider in evaluating which metrics are relevant or appropriate for their use case. Regulators should avoid inflexible approaches and instead focus on process-based and outcome-oriented policy solutions that facilitate risk-based assessments. Prescriptive standards, whether for AI systems or for contracts governing AI services, could act as unjustified market-entry barriers. Rather, a governance-based and self-attestation approach which identifies broad objectives and processes that developers and deployers should follow to achieve fairness in AI systems will be more effective. To this end, many global AI developers and deployers have taken voluntary steps to establish AI ethics principles and a formal review process built into companies' structure to help ensure that AI technologies are built and used safely and responsibly. The BSA Framework is an example of how industry stakeholders can come together to create a methodology for identifying and addressing AI risks.

Align with emerging internationally recognized standards

As the Government of Thailand considers its approach to AI regulation, it is important to ensure that its efforts are aligned with the emerging body of internationally recognized standards. This alignment will improve international interoperability of Thailand's regulations on AI and promote the ability of organizations in Thailand, both AI developers and deployers, to benefit from the most advanced resources, concepts, and options available. The ISO Standards Committee on AI[20] has completed work on 10 sets of standards, including on bias in AI systems and approaches to enhance trustworthiness in AI.[21] The ISO Committee is currently developing 27 additional standards. The risk of establishing domestic standards that are not well aligned with, or are too far ahead of, internationally recognized standards, is that requirements will be out of step with emerging practices, deterring development of AI in Thailand and impeding efforts to ensure that the technology is developed and deployed responsibly.

BSA recommends that the Government of Thailand should align AI standards to those developed or currently being developed by international standards development organizations such as the ISO. In addition to promoting trust, confidence, and marketplace efficiencies, international standards have the added benefit of mitigating the risks that can accompany country-specific standards. Indeed, the proliferation of national standards can undermine global commerce and stunt the development of technology. For example, it can give rise to a patchwork of inconsistent national standards that act as an unintentional barrier to international trade, making it more costly for companies to develop and sell their AI-related products and services to the global marketplace. Alignment with international standards avoids these challenges and helps ensure interoperability.

Conclusion

BSA appreciates the opportunity to provide our comments and recommendations on the Draft AI Bill. We hope that our comments will assist in the development of clear and rigorous regulations for AI in Thailand and look forward to continue working with the MDES, the ETDA, and relevant agencies on AI Governance policies. Please do not hesitate to contact the undersigned at waisanw@bsa.org if you have any questions or comments regarding our suggestions.

Yours faithfully,

Wong Wai San

Wong Wai San

Senior Manager, Policy – APAC

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

[21] 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.