

28 April 2025

BSA COMMENTS ON THE DRAFT DIGITAL TECHNOLOGY INDUSTRY LAW (VERSION DATED 22 MARCH 2025)

Respectfully to: - Committee of Science, Technology and Environment – National Assembly
-The Ministry of Science and Technology

The Business Software Alliance (**BSA**)¹ thanks the National Assembly's Committee of Science, Technology and Environment (**STE Committee**) and the Ministry of Science and Technology (**MST**) for the opportunity to comment on the draft Digital Technology Industry Law (**DTI Law**) (version dated 22 March 2025). BSA is the leading advocate for the global enterprise software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that spark the economy.

In Vietnam, BSA has actively participated in developments related to data and personal data protection,² cybersecurity,³ AI governance, and other technology policy issues.⁴ On artificial intelligence (**AI**), we commented on the DTI Law in September 2024⁵ and recently met officials from MST in Hanoi in March 2025.

BSA commends the STE Committee and the MST for continuing the dialogue with the private sector on the regulatory framework governing the tech sector, including on AI. Open dialogue helps to create regulations that are practical and aligned with policy objectives. We encourage the STE Committee and the MST to continue actively taking industry feedback into account, even after the close of the official public consultation period. Engaging with stakeholders throughout the implementation process will help create rules that are both effective and feasible. We look forward

¹ BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Dassault Systemes, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

² Examples include BSA Comments on the Draft Decree and Draft Decision to Implement the Data Law, 17 March 2025 at <https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-decree-and-draft-decision-to-implement-the-data-law>, and BSA Comments on the Draft Law on Personal Data Protection, 23 November 2024 at <https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-law-on-personal-data-protection>.

³ Examples include attending the Workshop on the Cybersecurity Administrative Sanctions Decree organized by the MPS in November 2022, and Comments on Decree 53 in September 2022 at <https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-decree-53-to-implement-the-law-on-cybersecurity>, and BSA Comments on proposed amendments to the draft Decree 72 in September December 2021 at <https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-proposed-amendments-to-draft-decree-72-0>.

⁴ See BSA Comments on proposed amendments to the draft Decree 72, December 2021 at <https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-proposed-amendments-to-draft-decree-72-0>.

⁵ See BSA Comments on Draft Digital Technology Industry Law, 4 September 2024 at <https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-digital-technology-industry-law>.

to ongoing discussions and collaboration to achieve our common goals for a vibrant digital economy.

Definition of AI

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

Article 3.9 of the Draft DTI Law defines AI systems as “digital technology product, using digital data to automatically analyze, reason, make contents, forecasts, recommendations, and decisions based on a set of goals determined by humans.”

Recommendation: The DTI Law should adopt the updated definition of AI by the Organization for Economic Co-operation and Development (OECD)⁶ which defines AI as “a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.” This definition has been referenced by regulators worldwide, including the European Union. **We recommend amending Article 3.9 to reflect the OECD definition.**

Definition and Scope of High-Risk AI Systems

As discussed in our previous submission, 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 and must 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 like helping to organize digital files, auto-populating common forms for later human review, or improving a company’s ability to forecast supply chain issues. For example, AI is a critical component of cybersecurity risk mitigation,⁷ which creates significant benefits to both organizations and to consumers.

Imposing unnecessary regulations on such low-risk systems will hamper AI innovation with few corresponding benefits and therefore limit opportunities to use AI for positive impact. 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. Because the risks of AI are inherently use-case specific, any policy solutions or regulations should focus on the impacts of specific applications and uses of the technology that pose high-risks to the public and should be flexible enough to account for the unique

⁶ Updates to the OECD’s definition of an AI system explained on November 29, 2023 at <https://oecd.ai/en/work/ai-system-definition-update>.

⁷ 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.

considerations that may be implicated by specific use cases. They should not be broad-brush in nature and should not cover entire sectors, technologies, or capabilities.⁸

Recommendation: BSA recommends regulating high-risk use cases of AI rather than high-risk AI systems. Article 53 should be amended to replace “system” with “use case.” Further, high-risk AI use cases should be limited only to those specified uses that actually pose serious risk of harm to people, rather than those that are simply capable of causing serious risk of harm. Finally, we recommend deleting Article 53.4.

Key to proposed changes: **added text** and **deleted text**

Article 53: Classification of Artificial Intelligence Systems

1. High-risk artificial intelligence **use case system** is an artificial intelligence **use case system** that ~~is capable of causing~~ **poses a** serious risks ~~and of~~ harms to human health, human rights and interests, public interests, and social order and safety.
2. Artificial intelligence ~~**use cases systems that may otherwise be considered high-risk**~~ are not **considered** high-risk when they fall into one of the following cases: [...]
3. A high-impact artificial intelligence **use case system** is an artificial intelligence **use case system** with a large number of registered users, a large number of parameters, and a large computational volume used for training.
- ~~4.—Other artificial intelligence systems.~~

Roles and Responsibilities within the AI ecosystem

Legislation should reflect the different roles and responsibilities of the various organizations within the AI ecosystem. As discussed in our earlier submission, the AI ecosystem is complex and often involves multiple organizations that may develop an AI model, integrate that model into a particular AI system, and use the AI system for a specific task. We welcome the introduction of the concepts of an entity that develops AI and an entity that deploys AI within Article 56 of the draft DTI Law.

While we are encouraged that STE Committee and MST defined different roles and responsibilities of entities in the AI ecosystem, we caution against Vietnam-specific definitions that would compromise interoperability of the DTI Law with AI-related rules of other jurisdictions. In the current draft DTI Law, Article 56 defines an “entity developing an AI system” as the entity carrying out research and development activities of the AI system, an “entity providing the AI system” as the entity that brings the AI system to the market, and an “entity deploying the AI system” as the entity directly managing the AI system. Rather than creating these specific concepts, we encourage STE Committee and MST to follow emerging practice and establish two broad categories describing entities that “develop” AI systems and those that “deploy” them.

Recommendation: We recommend defining the roles of “developer” and “deployer” of an AI system as set forth below.

- **AI developer:** An AI developer is an entity that designs, codes, or produces an AI system.
- **AI deployer:** 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.)

⁸ For example, facial recognition as a technology that relies on AI may be deployed in different use cases. Low risk use cases could include background blurring in video conferencing systems, while high risk use cases could include public video surveillance. As such, undue regulation on facial recognition technology would hamper innovative use of such technology in instances that are not high risk.

We recommend deleting Article 56.1(b) which defines an “entity providing an AI system” as the entity that brings the AI system to the market and other provisions the reference such entities (i.e., Article 56.3). This introduces unnecessary complexity to the draft DTI Law and would introduce a category of AI-related entity that is not widely recognized internationally. Defining “AI developer” and “AI deployer” is consistent with the ASEAN Guide on AI Governance and Ethics⁹ which focuses on the definition of “developers” and “deployers” of AI systems.

In addition, STE Committee and MST should amend the assignment of responsibilities to the entities to be more appropriate according to their distinct roles.

Article 51 describes broad principles with which all players in the AI ecosystem are expected to comply. Such obligations should be tailored to the appropriate entity, as described above, rather than generally applying to every entity involved in the ecosystem. For example, equitable and non-discriminatory access and transparency may not be appropriate for developers, given that they are not the party that controls or uses the AI system, neither are developers able to provide transparency directly to an end user that they are not directly interacting with.

Article 56.2 and other clauses requiring compliance with Article 51 should be deleted. Requirements for impact assessment should apply only to high-risk use cases and clearly distinguish requirements for developers and deployers. Both developers and deployers should be required to conduct impact assessments for high-risk use cases of AI systems, but the obligations should be based on their roles. A developer’s impact assessment will focus on how the AI system is designed and a deployer’s impact assessment will focus on how the AI system is used. For more information, please refer to BSA’s position papers on “AI Developers and Deployers: An Important Distinction”¹⁰ and “Impact Assessments: A Key Part of AI Accountability”.¹¹

Recommendation: We recommend:

- removing reference to “providers” of AI (e.g., Article 56.1(b)),
- revising Article 51 so that it is clear that obligations that are neither feasible nor appropriate for developers or deployers of AI systems do not apply to such entities,
- removing references to Article 51 in Articles 56.2 and 56.3 and elsewhere, and
- limiting the obligations of Article 56.3 (e.g., impact assessments and risk management systems, among others) to defined “high-risk” uses of AI.

Clear Identification Signs for Products Created by AI Systems

Article 55 states “Digital technology products created by artificial intelligence for the purpose of direct interaction with humans must have clear identification signs,” and that the STE Committee and MST will promulgate the “List of digital technology products created by artificial intelligence that must have identification signs and regulations on identification sign specifications.” Our interpretation of this provision is that “Digital technology products created by artificial intelligence for the purpose of direct interaction with humans” refers to text and audiovisual content that is generated by AI.

⁹ See ASEAN Guide on AI Governance and Ethics <https://asean.org/book/asean-guide-on-ai-governance-and-ethics/> as accessed on 4 April 2025.

¹⁰ See AI Developers and Deployers: An Important Distinction, 16 March 2023, at <https://www.bsa.org/policy-filings/ai-developers-and-deployers-an-important-distinction>.

¹¹ See Impact Assessments: A Key Part of AI Accountability, 1 August 2023, at <https://www.bsa.org/policy-filings/impact-assessments-a-key-part-of-ai-accountability>.

BSA supports the development and deployment of reliable content authentication and provenance mechanisms that can help users identify the history and origin of AI-generated content. We support efforts by the Content Authenticity Initiative (**CAI**)¹² to promote the adoption of the Coalition for Content Provenance and Authenticity (**C2PA**) technical standard known as Content Credentials.¹³ The C2PA standard, which is expected to be approved by the International Standards Organization (**ISO**) this year, is openly available. Anyone, including governments, can use this standard to incorporate digital provenance information into their products and processes. Creators can indicate whether AI was used in their work and how it was used — the content credentials will display information about how the content was created, the date it was made, and any edits that were made along the way. This standard will help consumers decide what content is trustworthy and promote transparency around the use of AI.

Many other countries and jurisdictions are adopting or considering adopting provenance standards, including Japan, Australia, Singapore, and the European Union. Embracing open standards like that developed by C2PA facilitates international interoperability and enhances the integrity of digital content ecosystems. We acknowledge that what constitutes state of the art in ensuring solutions for content provenance will evolve over time so any governance framework must be designed to accommodate such developments and should provide scope for organizations to assess what is the most relevant solution for them when it comes to content authentication and provenance mechanisms.

Relatedly, the STE Committee and MST should avoid developing a Vietnam-specific standard for content authentication, as it could limit the ability of businesses to leverage widely accepted internationally recognized standards, such as C2PA, and could lead to increased compliance burdens for companies operating in multiple jurisdictions.

Importantly, these content authentication and provenance tools should be used on types of content where the technology supports latent, machine-readable designations, such as images and videos. Such approaches may not yet be feasible for text or other types of content. It is also important to note that these types of tools, which provide reliable, cryptographically-signed content credentials within metadata about the origin and history of AI-generated content, are distinct from visible labels or watermarks, which are impractical to implement and otherwise interfere with the visible presentation of the output. Notably, visible watermarks are easily removed, which undermines their effectiveness as a reliable content authentication mechanism while creating a false sense of security among consumers. We recognize that, in some circumstances, it may be appropriate to disclose a business's use or the existence of an AI service that is interacting with consumers.

Recommendation: First, the STE Committee and MST should align content authentication requirements with emerging internationally recognized standards like the C2PA, avoid implementing Vietnam-specific standards, and engage the industry on implementing practical and workable solutions to demonstrate accountability and transparency. Second, we recommend that the types of content subject to these “identification signs” be limited to those created by specifically identified generative AI systems so that the requirements apply to relevant AI-generated content only. The requirements should be limited to the types of content where they are technically feasible to implement, such as images and videos, rather than text.

¹² Content Authenticity Initiative, a global cross-industry coalition supported by over 4,500 members, at <https://contentauthenticity.org/>.

¹³ C2PA Specifications at <https://c2pa.org/specifications/specifications/2.1/index.html>.

Fostering International Cooperation and Interoperability in AI Governance

BSA supports policies that ensure AI systems are developed and used responsibly. The global nature of today's technology ecosystem demands coordinated policy responses to foster innovation, and we encourage international alignment and interoperability which are crucial for AI governance. We recommend the Government of Vietnam take a risk-based approach, applying legislation only to high-risk uses of AI and to pursue harmonization with international norms using international best practice frameworks, such as the OECD's reporting framework for the code of conduct under the Hiroshima AI Process,¹⁴ the ASEAN "Guide on AI Governance and Ethics",¹⁵ and the Expanded ASEAN "Guide on AI Governance and Ethics – Generative AI".¹⁶

Risk-Based Approach to Controlled Testing Mechanism

The controlled testing mechanism outlined in Articles 42 to 45 of the draft DTI Law establishes a structured approval process for new digital products and services, including AI and cloud-based solutions, that fall outside current legal frameworks. If the intent is for all new digital products and services to be approved before entering the Vietnamese market, such an approach will have a chilling effect on the digital economy as it impedes access to cutting edge technology solutions available in the global marketplace.

Recommendation: Adopt a risk-based approach where testing would be required only for use cases that pose a serious risk of harm to human health, human rights and interests, public interests, and social order and safety.

Ensuring Equitable Access to Non-Personal and Depersonalized Data for Innovation and Research

While the draft DTI Law establishes a foundation for managing and promoting digital data (Articles 19–21, 30–31), it lacks explicit provisions requiring the Government to provide clear, equitable access to government-owned and generated non-personal and depersonalized data for purposes such as innovation, research, and digital service development. Although Article 19 prohibits technical and commercial barriers to user data access, and Article 20 sets conditions for depersonalization, the Law does not define rights or procedures for third-party access to data held in government-managed databases. This gap may inadvertently restrict opportunities for startups, SMEs, and research institutions to leverage data in lawful and socially beneficial ways.

For ways in which making government data available to third parties can promote innovation, research, and the development of some of societies' most pressing challenges, please see BSA's open data agenda, "Open Data: Bridging the Data Divide."¹⁷

Recommendation: We recommend including a provision mandating MST to establish transparent frameworks for data access and requiring that government-managed non-personal or

¹⁴ See G7 reporting framework – Hiroshima AI Process (HAIP) international code of conduct for organizations developing advanced AI systems at <https://transparency.oecd.ai/>

¹⁵ See ASEAN Guide on AI Governance and Ethics <https://asean.org/book/asean-guide-on-ai-governance-and-ethics/> as accessed on 4 April 2025.

¹⁶ See Expanded ASEAN Guide on AI Governance and Ethics – Generative AI <https://asean.org/wp-content/uploads/2025/01/Expanded-ASEAN-Guide-on-AI-Governance-and-Ethics-Generative-AI.pdf> as accessed on 4 April 2025.

¹⁷ See BSA Open Data: Bridging the Data Divide at <https://www.bsa.org/policy-filings/bsa-open-data-agenda>

depersonalized data be made available under clear eligibility and use conditions. Such a measure would promote innovation, ensure responsible use of data, and align the DTI Law with international best practices on open data governance and digital economy development.

Ensuring Interoperability

The draft DTI Law introduces several requirements that would benefit from interoperability: the data portability requirement in Article 19, a controlled testing mechanism in Articles 42-45, and identification signs for products created by AI Systems in Article 55. Where possible, the STE Committee and MST should adopt internationally recognized standards to ensure interoperability with other jurisdictions. We caution against adopting domestic-specific standards, which would result in siloed systems that would not be able to exchange information across platforms.

Recommendation: The DTI Law should encourage the adoption of internationally recognized standards where applicable, including but not limited to open application programming interfaces (APIs), standardized data formats, and those developed by bodies such as ISO.

Extend the Period of Stakeholder Consultation

Extending the legislative timeline for the DTI Law is critical to allow comprehensive stakeholder engagement and thoughtful development of the law. A rushed timeline risks overlooking crucial feedback from experts, industry representatives, civil society, and other key stakeholders. This could lead to unintended consequences such as regulatory gaps or unnecessarily burdensome compliance requirements. Allowing more time for dialogue and collaboration with all relevant stakeholders will enable the creation of a more balanced and effective legal framework that aligns with global best practices while addressing Vietnam's unique context and requirements.

As discussed in our previous submission, an extended timeline would also provide sufficient opportunity to refine and harmonize the provisions within other technology laws under development such as the Data Law and the Personal Data Protection Law, together with the existing Law on Cybersecurity. This will lead to a more robust data governance regime and a predictable policy environment that builds trust among businesses and customers.

Once the law is enacted, there must be a sufficient period of time before enforcement of binding obligations goes into effect. A two-year transition period will improve the ability of industry participants to implement changes to business operations that may be necessary to comply with new requirements. Similarly, STE Committee and MST should provide ample opportunities for interested stakeholders to consult on implementing rules related to any new legislation.

Recommendation: We recommend including sufficient time for engagement with stakeholders before promulgating the DTI Law and recommend a two-year transition period from the time the law is enacted to the commencement of its effective date. Further, we encourage sufficient time for consultation with the industry on subsequent implementing regulations.

Conclusion and Further Resources

We hope that our comments will assist the STE Committee and MST as it continues its important work on developing the DTI Law and subsequent implementing regulations. We look forward to serving as a resource as you continue to engage in policy discussions on this issue. Further to the recommendations above, we recommend referencing the BSA Policy Solutions for Building

Responsible AI, available in English¹⁸ and Vietnamese,¹⁹ which the STE Committee and MST may wish to consider as a further resource. Please do not hesitate to contact me at waisanw@bsa.org or +65 9729 1253 if you have any questions regarding this submission or if I can be of further assistance. Thank you once more for your time and consideration.

Yours sincerely,

Wong Wai San
Senior Manager, Policy – APAC

¹⁸ See BSA Policy Solutions for Building Responsible AI (English version), 9 April 2024 at <https://www.bsa.org/policy-filings/global-bsa-policy-solutions-for-building-responsible-ai>.

¹⁹ See Giải Pháp Chính Sách của BSA về Xây Dựng Trí Tuệ Nhân Tạo Có Trách Nhiệm, 9 April 2024 at <https://www.bsa.org/files/policy-filings/vt2024bsaapolicysolutions.pdf>.