Business Software Alliance

22 August 2025

BSA RECOMMENDATIONS FOR WHITE PAPER ON NATIONAL ARTIFICIAL INTELLIGENCE ROADMAP AND ARTIFICIAL INTELLIGENCE ETHICS GUIDELINES

On behalf of the Business Software Alliance (**BSA**),[1] we appreciate the opportunity to provide our recommendations on Indonesia's Public Consultation[2] on the Draft White Paper on National Artificial Intelligence Roadmap (**AI Roadmap**) and Artificial Intelligence Ethics Guidelines (**AI Ethics Guidelines**) to the Ministry of Communication and Digital (**KOMDIGI**). BSA has engaged extensively on digital issues in Indonesia, including in relation to the Personal Data Protection Law,[3] Electronic System Operators,[4] and the National Data Center.[5]

BSA is the global trade association of the enterprise software industry. Our member companies are leaders in artificial intelligence, cybersecurity, cloud computing, and other cutting-edge technologies. Close consultation between policymakers and the affected industry and other stakeholders is critical for effective policy making. BSA offers our extensive global experience in technology policy to serve as a resource, and we hope that our recommendations below will be helpful to the Government of Indonesia as you develop the AI Roadmap and AI Ethics Guidelines that will promote and support AI innovation in Indonesia.

BSA Resources

We provide BSA resources relating to AI policy and governance that you and your team may find helpful as you continue to develop the AI Roadmap and AI Ethic Guidelines:

- **BSA Policy Solutions for Building Responsible AI:**[6] A comprehensive set of recommendations for policymakers worldwide to address the most important AI policy issues and advance the adoption of responsible AI across the economy

[1] BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, 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] Public Consultation White Paper on the National Artificial Intelligence Roadmap and Concept of Artificial Intelligence Ethical Guidelines, 8 August 2025 at https://www.komdigi.go.id/berita/siaran-pers/detail/konsultasi-publik-buku-putih-peta-jalan-kecerdasan-artifisial-nasional-dan-konsep-pedoman-etika-kecerdasan-artifisial

[3] BSA Comments on Draft Implementing Regulation of Law Number 27 of 2022 regarding Personal Data Protection, 14 September 2023 at https://www.bsa.org/policy-filings/indonesia-bsa-comments-on-draft-implementing-regulation-of-law-number-27-of-2022-regarding-personal-data-protection

[4] Comments on Draft Regulation of the Minister of Communications and Informatics Concerning Public Scope Electronic System Operators, 16 October 2023 at https://www.bsa.org/policy-filings/indonesia-comments-on-draft-regulation-of-the-minister-of-communications-and-informatics-concerning-public-scope-electronic-system-operators

[5] BSA Comments on National Data Center Issues, 26 July 2024 at https://www.bsa.org/policy-filings/indonesia-bsa-comments-on-national-data-center-issues

[6] BSA Policy Solutions for Building Responsible AI, at https://ai.bsa.org/bsa-policy-solutions-for-building-responsible-ai/

- **BSA's Framework to Build Trust in AI**:[7] BSA's bias risk management framework for AI
- **Crosswalk Between BSA Framework to Build Trust in AI and NIST AI Risk Management Framework**:[8] An analysis to illustrate the alignment between the two frameworks
- **BSA's AI and Copyright Policy:**[9] Policy recommendations for how to advance AI and creativity for the benefit of creators, innovators, and all citizens in the 21st Century Economy

AI Ethics Guidelines Should be Voluntary

BSA recommends that the Government of Indonesia clearly indicate that the AI Ethics Guidelines are non-binding in nature and intended for voluntary compliance. It is not clear, however, if this is the case. For example, if the Guidelines are voluntary, it would seem unnecessary to provide exceptions to the application of the guidelines, e.g., for national defense, national security, or non-commercial uses. If the Government intends for the provisions to be legally binding, this should be explicitly stated and accompanied by multiple rounds of robust stakeholder engagement to ensure clarity, feasibility, and alignment with international best practices. For the purposes of this submission, we will refer to the document as AI Ethics Guidelines rather than AI Regulations according to our understanding of its purpose.

Set Definitions in Line with International Understanding

Given that AI systems are developed and deployed in an international context, frameworks 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 be aligned across jurisdictions to ensure that all stakeholders have a common understanding of AI. We commend KOMDIGI for referencing global principles, including those by UNESCO, OECD, and ASEAN, in developing the AI Ethics Guidelines.

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 both national and international alignment and interoperability which are crucial for AI governance. We recommend that the Government of Indonesia continue 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,[10] the ASEAN "Guide on AI Governance and Ethics",[11] the Expanded ASEAN "Guide on AI Governance and Ethics — Generative AI",[12] and the US National Institute of Standards and Technology's "AI Risk Management Framework".[13]

---

[7] BSA's Framework to Build Trust in AI, at https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai

[8] Crosswalk Between BSA Framework to Build Trust in AI and NIST AI Risk Management Framework, at https://www.bsa.org/policy-filings/us-crosswalk-between-bsa-framework-to-build-trust-in-ai-and-nist-ai-risk-management-framework

[9] BSA Artificial Intelligence and Copyright Policy, 29 May 2025, at https://www.bsa.org/policy-filings/global-artificial-intelligence-and-copyright-policy

[10] G7 reporting framework — Hiroshima AI Process (HAIP) international code of conduct for organizations developing advanced AI systems at https://transparency.oecd.ai/

[11] ASEAN Guide on AI Governance and Ethics at https://asean.org/book/asean-guide-on-ai-governance-and-ethics/ as accessed on 4 April 2025

[12] Expanded ASEAN Guide on AI Governance and Ethics — Generative AI at 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

[13] See NIST AI Risk Management Framework at https://www.nist.gov/itl/ai-risk-management-framework as accessed on 14 August 2025

Definition of AI. To support global adoption of AI, regulations and standards should be internationally aligned. BSA recommends that the AI Law adopts the OECD's[14] updated definition of AI 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."

Roles and Responsibilities of AI Actors. AI regulation should reflect the different roles and responsibilities of different organizations in the AI supply chain. 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 developed and deployed.[15] The AI supply chain often includes several different actors, including developers who design, code, or produce an AI system; integrators, who integrate third-party AI tools into their applications, and deployers who put systems into use in the real world.

Importantly, and as discussed in greater detail below, responsibilities and voluntary commitments should fall mostly on developers and deployers of **high-risk AI systems**, and such responsibilities and voluntary commitments should reflect the distinct roles of developers and deployers of such systems.[16]

A **developer of a high-risk AI system** is an entity that designs an AI system specifically intended for high risk uses, substantially modifies a high risk AI system by intentionally changing core capabilities in a way that materially increases the risks presented by the use of the AI system, or substantially modifies a non-high-risk AI system, such as a general purpose AI system, to become a high-risk AI system, either through further development or deployment.

In cases of substantial modification, the entity should be deemed as acting as the developer of the modified high risk AI system and is therefore responsible only for the risk it introduces and the information within its possession, custody, or control. Developers of high-risk AI systems have specific information regarding how the AI system was designed and trained, its intended uses, and the expected risks such uses present. As such, developers of high-risk AI systems may have a duty to communicate such information, including, in the case of developers that have substantially modified an AI system, information they have received to their customers.

A **deployer of a high-risk AI system** is an entity that uses a high-risk AI system developed by another entity. Deployers of high-risk AI systems have a direct relationship with their customers in a way the developers do not. They may conduct risk impact assessments to document the deployer's intended purpose for using the high-risk AI system, transparency systems and notifications provided to customers, evaluation methodology of the AI system, likely risks and mitigation measures, and post-deployment monitoring.

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

[14] Updates to the OECD's definition of an AI system explained on 29 November 2023 at https://oecd.ai/en/wonk/ai-system-definition-update

[15] 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."

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

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 within the AI ecosystem

We appreciate that the Draft AI Ethics Guidelines recognize the division of roles and responsibilities of AI actors within the ecosystem. It is important that actors in the AI supply chain assume responsibilities appropriate for their roles. For example, developers that design high-risk AI systems are well positioned to have access to information about the type of data used to train the AI systems, their capabilities, and their known limitations. In contrast, deployers using high-risk AI systems are best positioned to have access to information regarding the specific ways in which the deployers' customers use such systems.

As discussed below, we encourage AI governance frameworks and ethics guidelines to focus exclusively on responsibilities in the high-risk context where the most significant risk of harm could occur. We note, however, that even where frameworks address general-purpose AI, policies focused on supporting AI accountability should still reflect the different roles of the relevant actors and assign responsibilities accordingly. Notably, in this context, "integrators" may leverage developers' generative AI models, integrate them into their own software applications, and provide these AI systems to other companies. As in other contexts, it is equally important that the different roles companies may play in this scenario are not conflated, and that any accountability measures are performed by those that are responsible, best positioned to address relevant issues, and commensurate with the risk introduced.

Risk-Based Approach

We appreciate that the Draft AI Ethics Guidelines recognize the need for a risk-based approach. For example, an AI system may be high risk if it makes consequential decisions that determine an individual's eligibility for and result in the provision or denial of housing, employment, credit, education, access to physical places of public accommodation, healthcare, or insurance. Because the risks of AI are inherently use-case specific, any guidelines should focus on the types of risks to address, and the specific applications of the technology that pose high-risks to the public. The guidelines should be flexible enough to account for the unique considerations that may be implicated by specific use cases.

The application of the guidelines 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-populate common forms for later human review, or improve a company's ability to forecast supply chain issues. AI governance efforts should focus on addressing high-risk AI use cases based on the likelihood of harm.

Self-Assessment and Reporting

Self-assessments and incident reporting can be valuable tools for ensuring the safety, accountability, and trustworthiness of AI systems. But such tools should be applied in a targeted and proportionate manner. Any self-assessment requirements should be limited to high-risk AI use cases that are identified using clear and objective criteria. Self-assessment responsibilities should be assigned to the party that is best positioned to conduct the assessment, based on that party's role in the AI lifecycle and its level of control over relevant factors. For example, developers of high-risk AI systems are best placed to assess elements such as the quality of training data and known limitations related to the training data. In contrast, deployers of high-risk

AI systems are best placed to assess operational elements such as the context in which the system will be used, the adequacy of human oversight, and the nature of the decisions that the AI will inform.

Incident reporting is common in other contexts, such as cybersecurity, critical infrastructure, and product safety. As a result, governments should not create new reporting frameworks for AI incidents, as these could result in duplicative reporting requirements, and the costs would outweigh any benefits for companies required to address burdensome, overlapping requirements. For example, if a security incident arises in connection with an AI-enabled system assisting with a dam, a company may already be subject to obligations across different jurisdictions that require reporting to different agencies regulating cybersecurity and critical infrastructure. The use of AI, while a component of the software application, does not warrant a separate reporting channel. Accordingly, we recommend removing reporting from the voluntary guidelines.

To the extent KOMDIGI decides to retain incident notification in the voluntary guidelines, we emphasize that incident reporting should be proportionate to the level of risk and focused on actual, material incidents rather than hypothetical concerns. Reporting commitments should apply only to a subset of high-risk AI systems where an incident causes significant physical damage, safety risks, or bodily harm. Notification should not be expected when an AI system merely produces an undesirable or unexpected response triggering a complaint. Furthermore, a responsibility to report AI incidents should not duplicate reporting where other notification requirements may exist, such as cybersecurity incidents or personal information breaches. They should be triggered only when an incident is known to have actually occurred and risks significant harm to individuals or society. Reports should provide enough detail for regulators to understand the nature of the incident, its root causes, and the remedial measures that have been taken, while avoiding overly prescriptive requirements that could discourage timely disclosure or reveal sensitive information or impose unnecessarily short timelines that pose administrative burdens or interfere with determining the cause and implementing remediation efforts. Limiting incident reporting expectations to these targeted contexts will help ensure that compliance resources are allocated effectively, reduce unnecessary reporting burdens, and maintain focus on addressing the most significant AI governance challenges.

Engagement with Stakeholders

A rushed timeline for finalizing the AI Roadmap and AI Ethics Guidelines risks overlooking valuable feedback from experts, industry players, civil society, and other key stakeholders. This could result in gaps in the framework or recommendations that are impractical to implement. Lessons can be learned from the early passage of the EU AI Act, and the subsequent realization of the significant complexity involved that led to delays in developing and publishing implementation rules. Allowing more time for dialogue and collaboration with interested and informed stakeholders supports the development of balanced and effective guidelines that align with global best practices while reflecting Indonesia's unique context and priorities. An extended timeline would also create space to refine the provisions and ensure they are consistent with other national strategies and policies related to digital transformation, data governance, and

emerging technologies. This approach will help ensure the AI Roadmap and AI Ethics Guidelines serve as a practical and credible reference for developing AI in Indonesia.

Recommendation: Extend the deadline for consultation by one month to 19 September and provide clear milestones for the implementation of the AI Ethics Guidelines.

Conclusion

BSA thanks KOMDIGI for considering our recommendations. We stand ready to support the Indonesian government and hope that our comments will assist in developing Indonesia's AI Roadmap and AI Ethics Guidelines. We reiterate our support to KOMDIGI and our wish to act as a resource on international developments and best practices for AI governance policy. Please do not hesitate to contact me at waisanw@bsa.org or +65 9729 1253 to make arrangements for further discussion. Thank you once more for your time and consideration.

Yours sincerely,

Wong Wai San
Senior Manager, Policy – APAC