March 15, 2024

BSA COMMENTS ON PUBLIC CONSULTATION ON PROPOSED MODEL GOVERNANCE FRAMEWORK FOR GENERATIVE AI

Submitted Electronically to the Infocomm Media Development Authority

BSA | The Software Alliance (**BSA**)[1] appreciates the leadership by the Infocomm Media Development Authority (**IMDA**) in developing Model Governance Frameworks for Artificial Intelligence (**AI**).[2] We welcome the opportunity to submit comments to the Government of Singapore on the proposed Model Governance Framework for Generative AI (**Model Framework**).[3] We are glad to be a member of the AI Verify Foundation and to be involved in this important work co-developing guardrails for Generative AI.

BSA is the leading advocate for the global software industry. Our members are enterprise software companies at the forefront of developing cutting-edge services — including AI — and their products are used by businesses across every sector of the economy.[4] For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, cybersecurity 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 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.

Realising the benefits of AI requires public trust and confidence that these technologies can be developed and deployed responsibly. BSA has for years promoted the responsible development and deployment of AI, including through BSA's Framework to Build Trust in AI,[5] a risk management framework to mitigate the potential for unintended bias throughout an AI system's lifecycle. BSA has

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

[2] Including the Second Edition of the Model Artificial Intelligence Governance Framework dated January 21, 2020 at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf

[3] Proposed Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem, 16 January 2024 at https://aiverifyfoundation.sg/downloads/Proposed_MGF_Gen_AI_2024.pdf

[4] Artificial Intelligence in Every Sector, 13 June 2022 at https://www.bsa.org/policy-filings/artificial-intelligence-in-every-sector.

[5] Confronting Bias: BSA's Framework to Build Trust in AI, 8 June 2021 at https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai.

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

testified before the United States Congress[6] and the European Parliament[7] on the Framework and its approach to mitigating AI-related risks.

We support the objectives of the Model Framework, which seeks to set forth a systematic and balanced approach to address Generative AI concerns while continuing to foster innovation. We also appreciate that the Model Framework will evolve as techniques and technologies develop. As you review and update the Model Framework, we make the following recommendations, discussed in more detail below.

- ***Engage in a multi-stakeholder dialogue*** to develop a shared vision for a risk-based policy approach for addressing common AI challenges and advancing norms around responsible AI governance (e.g., risk-based approach to regulation, balanced responsibilities along the AI value chain).
- ***Adopt a risk-based approach*** that limits obligations or commitments to entities developing or deploying high-risk AI systems.
- ***Clearly distinguish between different actors in the AI eco-system.*** Obligations and responsibilities should be placed on organisations based on their role in the AI ecosystem so that they can appropriately address the risks that fall within their control.
- ***Maintain Singapore's current Copyright Act*** which provides protections for copyright owners against AI generated infringing content and allows AI developers to use legally accessible works for computational data analysis as AI training. ***Ensure that content created with the assistance of generative AI, including software code, remains protectable under Singapore's Copyright Act.***
- ***Avoid imposing third-party testing and evaluation requirements*** while ***incentivising robust testing and evaluation of high-risk AI systems*** for safety, security, accuracy, and harmful bias.
- ***Support the development and deployment of reliable content authentication and provenance mechanisms*** including efforts by the Content Authenticity Initiative (**CAI**) to promote the open Coalition for Content Provenance and Authenticity (**C2PA**) standard for content authenticity and provenance.

Open Dialogue and Co-creation with Industry

We commend the IMDA for its commitment to co-creating the Model Framework with industry and other stakeholders in this public consultation process. Singapore's commitment to fostering accountability in the AI landscape through its strong partnership with industry stakeholders is crucial to maintain its strong leadership in AI policy in the region and beyond. We encourage continued multi-way dialogue between regulatory bodies, industry stakeholders, and other relevant parties. This would put Singapore in good stead to develop AI policies, not only for the Model Framework but also for other AI-related issues including but not limited to AI and privacy, AI and copyright, and other emerging issues.

Risk-Based Approach to AI Governance

BSA recommends a risk-based approach to AI governance, and this includes AI governance for Generative AI. The Model Framework does not explicitly mention a risk-based approach nor risk management programmes. The Model Framework considers a comprehensive and systematic

[6] Hearing on "Beyond I, Robot: Ethics, Artificial Intelligence, and the Digital Age", Testimony of Aaron Cooper, Vice President, Globally Policy, BSA | The Software Alliance, 13 October 2021 at https://www.congress.gov/117/meeting/house/114125/witnesses/HHRG-117-BA00-Wstate-CooperA-20211013.pdf.

[7] Special Committee on Artificial Intelligence in a Digital Age, Public Hearing on "AI & Bias", 30 November 2021 at https://www.europarl.europa.eu/cmsdata/244265/AIDA_Verbatim_30_November_2021_EN.pdf.

approach to safety evaluations,[8] establishing the structures and processes to enable incident reporting,[9] and safety techniques and evaluation tools to address the potential risks of AI.[10] In addition to these, we recommend including the implementation of risk management programs and focusing these programs on high-risk AI use cases.

Risk management programs enable organisations to identify the personnel, policies, and processes necessary to manage AI risks. As part of a risk management program, organisations should clearly assign roles and responsibilities, establish formal policies, use evaluation mechanisms, ensure executive oversight, and perform impact assessments for high-risk uses of AI. Organisations should have internal independent review mechanisms, such as interdepartmental governance or ethics committees, to evaluate and address AI uses that pose high risks. Organisations can incorporate these practices as part of a broader corporate risk management program or as a separate AI program. BSA recommends referencing risk management programs such as the US National Institute of Standards and Technology (**NIST**) AI Risk Management Framework[11] and the companion Risk Management Framework that the NIST is developing for Generative AI.[12] BSA has also developed our own bias risk management framework[13] and a crosswalk of this framework against the NIST Risk Management Framework.[14]

AI governance efforts should focus on high-risk use cases. 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 – including Generative AI – are inherently use-case specific, any policy solutions should focus on specific applications of the technology that pose high-risks to the public and should be flexible enough to account for the unique considerations that may be implicated by specific use cases. We recommend that the need for comprehensive AI risk impact assessments should be limited to high-risk use cases.

Whether for "traditional" AI or Generative AI, BSA recommends impact assessments for high-risk uses of AI. An impact assessment is an accountability mechanism that promotes trust by demonstrating that a system has been designed and deployed in a manner that accounts for potential risks it may pose to the public. By establishing a process to document key design and deployment choices and their underlying rationale, impact assessments enable organisations to identify and mitigate risks that can emerge throughout a system's lifecycle. BSA supports commitments by organisations that develop or deploy high-risk AI to conduct impact assessments and publicly affirm that they have complied with this practice.

Roles and Responsibilities in the AI Ecosystem

It is essential to distinguish clearly between different actors in the AI eco-system. Organisations should commit to responsibilities based on their role in the AI ecosystem so that they can appropriately address the risks that fall within their control. For example, entities such as AI developers and AI deployers should commit to responsibilities consistent with their roles. AI developers, AI deployers, and other parties within the value chain will have different information about how the AI system was developed, operates, or is used during deployment. The Model Framework

---

[8] Proposed Model AI Governance Framework for Generative AI, page 11.

[9] Ibid., page 13.

[10] Ibid., page 19.

[11] AI Risk Management Framework, 26 January 2023 at https://www.nist.gov/itl/ai-risk-management-framework.

[12] NIST AI Public Working Groups, Generative AI Public Working Group (GAI-PWG) at https://airc.nist.gov/generative_ai_wg.

[13] Confronting Bias: BSA's Framework to Build Trust in AI, June 2021 at https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai.

[14] Crosswalk Between BSA Framework to Build Trust in AI and NIST AI Risk Management Framework, 12 April 2023 at https://www.bsa.org/policy-filings/us-crosswalk-between-bsa-framework-to-build-trust-in-ai-and-nist-ai-risk-management-framework.

should recognise these distinctions. We agree that AI developers (termed "model developers" in the Model Framework) are well placed to lead the development of a potential AI shared responsibility approach.[15] However, this does not imply that AI developers ought to take on the majority of responsibilities in the AI ecosystem. While AI developers may be most knowledgeable about their own models and how they are trained, AI developers do not have sufficient information about how these models are deployed. Such knowledge lies within the domain of the AI deployer. Organisations may also take on other roles, such as integrating an existing AI model into the organisation's products and services. Any commitments taken on by these organisations should similarly reflect their role in integrating the AI system into the organisation's products and services. It is important to understand the role each entity plays to allocate responsibility proportionately and achieve the objective of ensuring accountability across the AI value chain.

BSA supports the concept of sharing relevant information along the AI value chain, though policymakers should avoid requirements to disclose confidential commercial information. This collaborative approach ensures transparency and accountability while fostering innovation. For instance, when an AI deployer takes an AI system that is not designed for high-risk use cases and implements it in a way that creates high risk, the AI deployer rather than the AI developer should be responsible for any risk management related to the high-risk use case. This is in line with requirements under the agreed text of the EU AI Act.

AI and Copyright

The Model Framework raises the issue of the use of copyright material in training datasets. We support the text and data mining exception in Singapore's Copyright Act, which has the purpose of supporting research and innovation. Copyright protected works may be used by commercial and non-commercial organisations if lawfully accessed (e.g., without circumventing paywalls) for computational data analysis, such as sentiment analysis, text and data mining, or training machine learning, without the permission of each copyright owner.[16] As long as lawfully accessed, the use of publicly available copyright protected works should continue to be allowed where appropriate for the training of AI models.

We recognise that Generative AI models may be used to generate creative output which could be highly similar to existing copyrighted content. We support effective protections for copyright owners against the generation and distribution of infringing content. The existing Copyright Act is sufficient to address when a work created with the assistance of AI infringes copyrighted material.

It is important to continue recognising the copyrightability of works created with the assistance of AI. Just as other software applications have long been an important tool of artists and storytellers (e.g., photo enhancements for visual artists, visual effects in media and entertainment, and arranging music for sound recordings), generative AI is a powerful tool to bolster creativity. Copyright protections also play a key role in businesses' ability to protect creative material, including software code. The use of AI should not prevent a work developed in conjunction with human creativity from being eligible for copyright protection. If copyright protection is not available simply because AI was used in the creative process, it will limit the responsible use of AI and the purpose of copyright laws, which is to foster the creation and dissemination of new works for the benefit of society. As a result, AI-assisted human creations or the portions of the work that are influenced by human creativity should continue to be protected by copyright laws. A lack of copyright protection may also cause innovators to seek out jurisdictions with laws and policies that are more protective of intellectual property.

[15] Proposed Model AI Governance Framework for Generative AI, page 6.

[16] Copyright Act of Singapore 2021, Sections 233 and 234 at https://sso.agc.gov.sg/Act/CA2021

Testing and Assurance

BSA encourages measures that incentivise safety and security. Robust testing and evaluation of high-risk AI systems for safety, security, accuracy, and fairness is critical and is prioritised in the NIST AI Risk Management Framework,[17] which BSA supports. Existing technical standards for AI testing are nascent and should be developed consistently with longstanding voluntary, market-driven, and consensus-based approaches to standards development. As such we discourage imposing third-party testing and evaluation requirements. The Model Framework should encourage robust internal testing mechanisms that ensure the quality and safety of AI systems without compromising confidential or proprietary information, avoiding a prescriptive approach that may stifle innovation and impose unnecessary costs on businesses.

We recommend that the fifth dimension of the Model Framework, Testing and Assurance, should also include the use of internal testing and avoid suggesting that external tests or other types of audits should always be conducted. While we agree that companies may see external audits as a useful mechanism to provide transparency and build greater credibility and trust with end-users, we advise against suggesting that organisations should always conduct external testing. Internal testing — which can be performed by a team of employees that is independent from the team tasked with developing an AI system — can identify and mitigate risks without creating concerns about sharing trade secret and other proprietary information that will arise in external testing. As a result, it is likely to be the more powerful tool for identifying, evaluating, and mitigating risks across the AI lifecycle.

Content Provenance

The Model Framework addresses the issue of content provenance and the need to identify solutions such as digital watermarking techniques and cryptographic provenance solutions to identify content created or modified using AI. BSA supports the development and deployment of reliable content authentication and provenance mechanisms (e.g., watermarking) that can help users identify AI-generated content. We support efforts by the Content Authenticity Initiative (**CAI**) to promote the open Coalition for Content Provenance and Authenticity (**C2PA**) standard for content authenticity and provenance. This standard will help consumers decide what content is trustworthy and promote transparency around the use of AI. In conjunction with watermarking, the CAI approach provides secure, indelible provenance. Embracing open standards like that developed by C2PA facilitates interoperability and enhances the integrity of digital content ecosystems. We also note that what constitutes state of the art in ensuring solutions for content provenance will evolve over time, and encourage IMDA to ensure that any governance framework accommodates such developments.

Conclusion

BSA appreciates the opportunity to provide our comments and recommendations on the Draft Model Governance Framework for Generative AI. We hope that our comments will assist in the development of clear and rigorous voluntary guidelines for AI in Singapore and look forward to continuing working with the IMDA, relevant agencies, and the AI Verify Foundation 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

[17] AI Risk Management Framework, 26 January 2023 at https://www.nist.gov/itl/ai-risk-management-framework