



Recommendations from BSA | The Software Alliance on the Skeleton Draft of the New AI Business Operator Guidelines

October 27, 2023

General Comments

BSA | The Software Alliance (**BSA**)¹ appreciates the leadership of the Ministry of Internal Affairs and Communications (**MIC**) and Ministry of Economy, Trade and Industry (**METI**) in drafting the New AI Business Operator Guidelines (**draft Guidelines**) to support artificial intelligence (**AI**) business operators to develop, deploy, and use AI responsibly. We are encouraged to see in the skeleton draft of the Guidelines² (**skeleton draft**) that METI and MIC are taking a risk-based approach that supports industry's voluntary efforts to ensure innovation is not hindered. BSA and its members are eager to work with the Government of Japan to achieve the goal of accelerating AI utilization while providing appropriate safeguards to minimize risks.

BSA is the leading advocate for the global software industry. Our members are at the forefront of software-enabled innovation that is fueling global economic growth, including AI, cloud computing, and data analytics. BSA members help societies harness the benefits of AI in every sector, transforming people's lives in incredible ways, helping them solve complex problems, and driving innovation across the globe.³ As BSA members are leaders in the development of cutting-edge technologies, BSA has unique insights into both their tremendous potential and the government policies that can best support their responsible development and use.

BSA recognizes that the public should be assured that AI systems have been thoroughly vetted to identify and mitigate risks that may emerge during AI life cycle and ensure this is appropriately implemented. We provide the following recommendations, attaching relevant documents which we hope will be useful in further developing the draft Guidelines. 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,⁴ "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

¹BSA'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, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Palo Alto Networks, 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 https://www8.cao.go.jp/cstp/ai/ai_senryaku/5kai/gaidorain.pdf

³ For further details, please refer to "Artificial Intelligence in Every Sector", June 13, 2022, at <https://www.bsa.org/policy-filings/artificial-intelligence-in-every-sector>

⁴ <https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai>

AI marketplace,⁵ and “AI and Cybersecurity” which explains how AI tools can be effectively used to ensure cybersecurity.⁶

These documents elaborate on our recommendations which encourage the Government to consider AI policies:

- apply only to high-risk AI use cases ;
- endorse the use of impact assessments;
- recognize the different roles and responsibilities of AI developers and deployers;
- align with emerging internationally recognized standards;
- incorporate a lifecycle approach to address responsible and secure development and deployment of AI; and
- maintain data and intellectual property policies that promote innovation.

We provide our detailed comments below to MIC and METI relating to the responsibilities of AI business operators based on the released skeleton draft.

Definitions

Given that AI systems are developed and deployed in an international context, definitions, measures, and standards that apply to AI should operate across different jurisdictions to facilitate and promote further widescale adoption and use of AI technologies. We recommend: (1) defining “AI system” in line with internationally supported definitions, and (2) defining a subset of high-risk AI uses cases that are subject to the new Guidelines.

Definition of AI System: BSA proposes that Japan adopts the OECD’s definition of AI system. In its Recommendation of the Council on Artificial Intelligence,⁷ the OECD defines AI system as “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments”, and specifies that AI systems are “designed to operate with varying levels of autonomy”. This definition has been referenced by regulators worldwide, including the European Union.⁸ The US National Institute of Standards and Technology (**NIST**) also adapts the OECD definition for use in its AI Risk Management Framework published in January 2023.⁹ Using an accepted and internationally recognized definition of AI system, such as the OECD’s, will facilitate the international alignment of Japan’s new Guidelines and promote dialogue, adoption, and compliance with those Guidelines.

Definition of High-Risk AI Use Cases: We strongly support a risk-based approach to AI policies that focuses responsibilities on uses of AI that create high risks to individuals. To adopt this risk-based approach, the draft Guidelines should identify a subset of AI use cases

⁵ <https://www.bsa.org/policy-filings/ai-developers-and-deployers-an-important-distinction>

⁶ <https://www.bsa.org/files/policy-filings/20231004aiforcybersecurity.pdf>

⁷ 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.”

⁸ 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”.

⁹ NIST AI Risk Management Framework, January 26, 2023 at <https://www.nist.gov/itl/ai-risk-management-framework>

as high risk. This includes use of AI that determines an individual's eligibility for housing, employment, credit, education, healthcare, or insurance. AI that does not create high risks to individuals include, for example, cybersecurity use cases where, for example, AI is used to detect the risk level of an IP address during login, AI-enabled video games, or AI inventory management system, among others.

Standards

As MIC and METI examine the responsibilities of entities involved in developing and deploying AI systems, it is important to recognize the role of internationally recognized standards in supporting responsible AI. We recommend the Government of Japan avoid creating Japanese-only standards for AI, and instead leverage the ongoing work of international standards organizations and technical organizations to create harmonized AI standards.

The International Organization of Standardization's (ISO) Standards Committee on AI¹⁰ has completed work on 10 sets of standards, including on bias in AI systems and approaches to enhance trustworthiness in AI.¹¹ Also, ISO 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 and deployment of AI in Japan and impeding efforts to ensure that the technology is developed and deployed responsibly. Misalignment of domestic standards with internationally recognized standards will also reduce the ability of AI systems developed in Japan from being deployed globally. In contrast, alignment with internationally recognized standards will improve international interoperability and promote the ability of organizations in Japan, both AI developers and deployers, to benefit from the most advanced resource, concepts, and options available.

Responsibilities

BSA welcomes the voluntary and risk-based approach proposed in the skeleton draft, recognizing the different roles of entities involved in developing and deploying AI systems.

Risk-based approach: Like many technologies, the risks associated with AI technologies do not exist only in the development of the AI system, but in its application, or how it is used. As the risks associated with AI are context-specific, the responsibilities of businesses should reflect the level of risk posed by the particular use of an AI system. Applying the same responsibilities to all use-cases of AI, without considering whether a particular use creates risk of actual harm may ultimately undermine the objectives of fostering AI uptake and protecting citizens. In fact, such an approach will create significant compliance burdens for companies, especially for SMEs and startups that may be developing or deploying AI systems for low-risk scenarios. We therefore strongly recommend new disciplines and guidelines focus on high-risk uses of AI technologies.

Clear allocation of responsibilities: We support the skeleton draft's recognition that many different companies can be involved in developing and deploying an AI system, which it refers to as "maintaining risk management and governance in AI supply chain". Given the diverse AI value chain, BSA recommends ensuring that responsibilities in the AI value chain are balanced and proportionate, where the obligations are allocated to the entities best placed to comply with them.

¹⁰ See ISO/IEC JTC 1/SC 42 at <https://www.iso.org/committee/6794475.html>

¹¹ 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>

We strongly encourage the Guidelines to distinguish between developers and deployers of AI systems, to ensure any responsibilities identified in the Guidelines reflect a company's role in the AI ecosystem. Developers are the companies that design, code, or produce an AI system, such as a software company that develops an AI system for speech recognition. In contrast, deployers are the companies that use an AI system, such as a bank that uses an AI system to make loan determinations. The developer of an AI system is generally able to describe the features of data used to train that AI system, but a developer generally would not have insight into how the AI system is used after another company has purchased and deployed the AI system. Instead, the deployer using the AI system is generally best positioned to understand how the system is actually being used, the types of data being collected in order to facilitate such use, what type of human oversight is in place, and whether there are complaints about how the system works in practice.

Currently, the skeleton draft refers to a range of different entities, including: (1) algorithm developers, (2) AI training implementers, (3) AI system/service implementers, (4) service implementers using AI, and (5) organizations that use AI in their business operation. We recommend that MIC and METI streamline these categories and provide clearer definitions for these categories with a focus on companies that develop AI systems and companies that deploy AI systems. Clear and focused categories can help companies more readily identify their obligations. If the current categories are maintained, we strongly suggest treating them as subsets of developers (for those entities that develop AI systems) and subsets of deployers (for those entities using AI systems).

Impact assessments: When AI is used in ways that could adversely impact civil rights or access to important life opportunities, the public should be assured that such systems have been thoroughly vetted and will be continuously monitored to account for the associated risks. BSA endorses the use of impact assessments to achieve this objective. Companies that develop or use high-risk AI should establish a comprehensive approach for performing impact assessments. Impact assessments are widely used in a range of other fields — from environmental protection to personal data protection — as an accountability mechanism that promotes trust by demonstrating that a system has been designed in a manner that accounts for the potential risks it may pose. Because companies already use impact assessments, they can be readily adapted to help companies identify and mitigate AI-related risks.

Transparency: The skeleton draft addresses how developers of an AI system can create transparency for companies using that system. BSA recognizes the importance of this issue and supports obligations for developers of high-risk AI systems to provide deployers of those systems with key information about the system. This may include, for example, information about the capabilities and limitations of the system, including known or foreseeable risks to individuals. We also recognize that developers of AI systems are creating a range of new resources to provide transparency to their customers about the AI system, such as documentation that provides information on the intended use cases and limitations, responsible AI design choices, and deployment and performance optimization best practices for a particular AI service. The Guidelines should support such efforts to provide the deployer of a high-risk AI system with this type of information, while avoiding requirements for the developer to disclose underlying training data or other information that may jeopardize trade secrets, create privacy concerns, or undermine the security of network and information systems.

Another way of ensuring transparency is to enable users to identify content made with AI. Industry bodies are undertaking efforts to voluntarily reduce the misuse of AI and other tools. For example, the Content Authenticity Initiative (CAI), a multi-stakeholder community, promotes the adoption of an open industry standard for content authenticity and provenance.¹² This enables viewers to know of the origins of an image or video, such as the photographer, the location where the image was generated, and if it was edited using

¹² <https://contentauthenticity.org/>

software. This information assists viewers to determine the content's authenticity. The group, which has over 900 members, is currently developing open-source tools to help prevent misinformation and increase transparency around the use of AI. We encourage the Government of Japan to support such efforts.

External audit: The skeleton draft includes several references to external audits. While we understand that the intention is to present this as an option for companies to demonstrate accountability and transparency, BSA recommends removing references to audits in the Guidelines because the process of developing auditable standards for AI is nascent. There are few existing procedures or best practices for companies to either:

- (1) choose a reputable company capable of auditing an AI system, or
- (2) determine what standards any such auditing company should apply.

Indeed, although the ISO has issued several AI-related standards, including guidance on risk management practices, many other standards are still under development. Currently, there is a lack of sufficient voluntary consensus-based standards addressing AI systems. Without common standards, the quality of any audits will vary significantly because different audits may measure against different benchmarks, undermining the goal of obtaining an evaluation based on an objective benchmark.

Moreover, there is no clear way to ensure audits are conducted by reputable companies that have met specific criteria demonstrating they are qualified to conduct audits of AI systems. The variation among existing auditing companies allows organizations to select auditors based on their own preferred criteria, methods, and scope. This will make the resulting audits less reliable and could unintentionally set back the objective of demonstrating accountability. This concern is exacerbated by the lack of professional bodies governing AI auditors, which is important for ensuring auditors adhere to ethical standards. Additionally, there are concerns over the significant risk of compromising the intellectual property of organizations that have made large investments in developing innovative solutions. Such audits, if required, would need to take place in an environment with strict controls on the access to proprietary information and data to limited personnel (e.g., a “clean room” environment) to protect the intellectual property, and therefore would be a costly endeavor.

Furthermore, while BSA understands the need to promote transparency, we recommend against publishing audit results, as this could disincentivize companies from undertaking a rigorous review of AI systems. For these reasons, external audits are not an appropriate solution to achieving transparency.

Promoting AI Adoption

Accelerating cloud adoption: Enabling the use of cloud computing is critical to harnessing the full potential of AI technologies. Cloud computing is at the forefront of AI development, and many AI-related technologies are specifically developed and tailored for cloud deployments. The Government of Japan should ensure that its policies enable and encourage the public sector and commercial sector to be able to use a variety of state-of-the-art cloud services, including commercial cloud services provided by global cloud service providers. Furthermore, policies related to the use of anonymized and pseudonymized data should avoid being over-prescriptive and requiring regulatory approvals prior to use so that Japanese businesses have access to the latest AI technologies and the broadest range of high-quality data sets to develop and deploy innovative AI solutions.

Conclusion

BSA and our members look forward to working with the MIC and METI to support the goal of developing effective AI policies. In addition to sharing this recommendation, we would appreciate the opportunity for a continued dialogue on how we can further assist in the effort.