



March 15, 2024

The Honorable Giovanni Capriglione  
Texas State Capitol  
1100 Congress Avenue  
Austin TX 78701

Dear Representative Capriglione,

BSA | The Software Alliance appreciates the opportunity to share insights on artificial intelligence (AI) from the enterprise software sector. BSA is the leading advocate for the global software industry.<sup>1</sup> BSA members are at the forefront of developing cutting-edge services, including artificial intelligence (AI), and their products are used by businesses of all sizes across every sector of the economy. AI is much more than robots, self-driving vehicles, or social media; it is used by companies large and small to create and improve the products and services they provide to consumers, to improve their internal operations, and to enhance their capacity to make data-informed decisions. BSA members are on the leading edge of providing businesses-to-business tools that help companies leverage the remarkable benefits of AI.<sup>2</sup>

As leaders in the development of enterprise AI, BSA members have unique insights into the technology's tremendous potential to further spur digital transformation in the private and public sectors and the policies that can best support the responsible use of AI, especially high-risk AI. BSA's views are informed by our recent experience with members developing BSA Framework to Build Trust in AI,<sup>3</sup> a risk management framework for mitigating the potential for unintended bias throughout an AI system's lifecycle. Built on a vast body of research and informed by the experience 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's extensive experience has helped us identify effective policy solutions for addressing AI risks.

When examining AI, we believe policymakers should focus on the priorities outlined below.

---

<sup>1</sup>BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, 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. See BSA | The Software Alliance, Artificial Intelligence in Every Sector, *available at* <https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf>.

<sup>2</sup>See BSA | The Software Alliance, Confronting Bias: BSA's Framework to Build Trust in AI, *available at* <https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai>.

## **I. Focus on High-Risk Use**

BSA recommends you focus on high-risk uses of AI, particularly AI systems that determine an individual's eligibility for housing, employment, credit, education, access to physical places of public accommodation, healthcare, or insurance. These systems have the potential to affect important life opportunities — and are a key area for policymakers to address. In contrast, many everyday uses of AI present few risks to individuals and create significant benefits, like helping organize digital files, auto-populate common forms for later human review, improve a company's ability to forecast supply chain issues, and detect, prevent, and respond to cybersecurity threats.

## **II. Risk Management Programs**

Companies should implement risk management programs that help them identify and mitigate risks. Risk management programs establish repeatable processes for companies to identify and mitigate potential risks that can arise throughout the lifecycle of an AI system. Risk management is particularly important in contexts like AI, privacy, and cybersecurity, where the combination of quickly evolving technologies and highly dynamic threat landscapes can render traditional approaches to compliance ineffective. Risk management programs have two key components: (1) a governance framework of policies, procedures, and personnel that support the company's risk management function, and (2) a scalable process for performing impact assessments that identify and mitigate risks of an AI system.

One way for companies to establish risk management programs is by using the AI Risk Management Framework (AI RMF), which was released last year by the National Institute of Standards and Technology (NIST).<sup>4</sup> The AI RMF builds on NIST's work creating frameworks for managing cybersecurity and privacy risks.<sup>5</sup> The AI RMF helps companies incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products. Ultimately, effective AI risk management programs should support coordination across the company, to promote the identification and mitigation of risks throughout the lifecycle of an AI system.

## **III. Impact Assessments**

BSA recognizes that performing impact assessments of high-risk uses of AI is a key part of creating a meaningful risk management program. Impact assessments have three purposes: (1) identifying potential risks that an AI system may pose, (2) quantifying the degree of potential harms the system could generate, and (3) documenting steps taken to mitigate those risks.<sup>6</sup> Impact assessments are already widely used in a range of other fields, including privacy, as an accountability mechanism that demonstrates a product or system has been designed in a manner that accounts for the potential risks it may pose to the public. Because impact assessments already exist today, they

---

<sup>3</sup> NIST AI Risk Management Framework, available at <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

<sup>4</sup> See NIST, Cybersecurity Framework, Questions and Answers, (discussing federal agency use of the NIST CSF), available at <https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#agency>.

<sup>5</sup> See BSA, Impact Assessments: A Key Part of AI Accountability, available at <https://www.bsa.org/files/policyfilings/08012023impactassess.pdf>.

can be readily adapted to help companies identify and mitigate AI-related risks.<sup>7</sup> In our view, 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 risks associated with unintended bias. Companies, both developers and deployers, should use impact assessments as a tool for the responsible development and use of high-risk AI systems.

#### **IV. Distinguishing Between Different Actors in the AI Ecosystem**

Much like privacy and security laws worldwide distinguish between different types of companies that handle consumers' personal data, AI laws should distinguish between different actors involved in developing and deploying an AI system. This can ensure that legal frameworks accurately assign obligations to a company based on its role in the AI ecosystem. These different roles include both the developer and the deployer of an AI system. A developer is the company that designs, codes, or produces an AI system, such as a software company that develops an AI system for speech recognition. A deployer, in contrast, is the company that uses an AI system, such as a bank that uses an AI system either developed internally or by a third party to make loan determinations. Each type of company will have access to different types of information about an AI system and will be positioned to take different actions to mitigate the risks associated with the AI system. AI policies that distinguish between different roles can ensure that the appropriate company within the various real-world AI supply chains can identify and mitigate risks.

Distinguishing between different entities based on of their role in the AI ecosystem can ensure companies are better able to fulfill their obligations and better protect consumers. For example, a developer would be able to describe the features of data used to train an AI system, but it generally would not have insight into how the AI system is used after another company has purchased and implemented the AI system. Instead, the deployer using the system is generally best positioned to understand how the AI system is being used, whether that use aligns with its intended use, whether and how to incorporate human oversight, the outputs from the AI system, any complaints received, and real-world factors affecting the system's performance.

#### **V. Third-Party Audits**

While policymakers have shown interest in understanding the potential role of third-party audits in AI policies, we do not support incorporating third-party audits into AI regulations because the environment for AI auditing is nascent and auditable standards for AI are not mature. There are few existing procedures or best practices for companies to choose a reputable company capable of auditing an AI system, and no central body to certify such auditors. Moreover, there is no consensus around the standards any such auditing company should apply to different AI systems. Indeed, although the International Organization for Standardization has issued several AI-related standards, including guidance on risk management practices, several other standards are still under development, and more broadly there is a lack of sufficient voluntary consensus-

---

<sup>6</sup> For example, thirteen state privacy laws will require companies to conduct impact assessment for specific activities, such as processing sensitive personal data, engaging in targeted advertising, or selling personal data. Colorado, Connecticut, and Virginia already impose these requirements. See Colorado Privacy Act, Colo. Rev. Stat. Tit. 6, Art. 1, Pt. 13 §§ 6-1-1301–6-1-1313; Connecticut Data Privacy Act Conn. Gen. Stat. Tit. 42, Ch. 743jj, Sec. 42-515-525; Virginia Consumer Data Protection Act; Va. Code Tit. 59.1, Ch. 53, § 59.1-575-585. State privacy laws in California, Delaware, Florida, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, and Texas will also require impact assessments for certain activities. Globally, privacy and data protection laws worldwide use impact assessments as a tool for improving accountability.

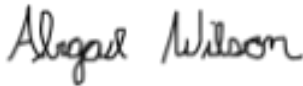
based standards addressing AI systems. Without common standards, the quality of any audits will vary significantly, as companies pick and choose their own auditor and the benchmarks the auditor will apply. This variation undermines the goal of obtaining objective evaluations.

Instead of focusing on third-party audits, we strongly encourage lawmakers to focus on the role of impact assessments in helping companies identify and mitigate potential risks of a high-risk use of AI. As discussed above, impact assessments are an important accountability mechanism that are already widely used in the field of privacy and data protection and can be leveraged to identify and mitigate risks of AI systems.

\* \* \*

Thank you for allowing us to provide the enterprise software sector's perspective. We welcome the opportunity to serve as a resource. BSA would appreciate the opportunity to meet with you and your staff to further engage with you or a member of your staff on these important issues.

Sincerely,



Abigail Wilson  
Manager of State Advocacy