Business Software Alliance

July 10, 2026

Chairman Ted Cruz
Ranking Member Maria Cantwell
United States Senate Committee on Commerce, Science, and Transportation
Dirksen Senate Office Building 554
Washington, D.C. 20510

Dear Chairman Cruz and Ranking Member Cantwell:

The Business Software Alliance (BSA), a global trade association of the enterprise software industry representing leaders in AI, cybersecurity, cloud computing, and other cutting-edge technologies,[1] appreciates your leadership in shaping Congress's approach on developing policies that can help accelerate AI adoption. BSA works in over 20 markets in the United States, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation. BSA members are leaders in technology privacy, security, and governance, and have unique insights into AI's benefits for every part of the economy.

We understand that the Senate Committee on Commerce, Science, and Transportation continues to consider a range of AI policy issues and, in connection with that effort, we appreciate the opportunity to share BSA's priorities on crafting legislation that enables responsible AI innovation. We provide information below on seven key priorities:

- **Risk-Based Approaches**—Legislation should not sweep in all uses of AI and should be calibrated to the risk the use creates.
- **Role-Based Responsibilities**—Responsibilities should fit the role of the company in the AI ecosystem to ensure they are capable of fulfilling the obligations and that the legislation is effective.
- **Relevant Transparency Disclosures**—Transparency requirements should ensure that the appropriate actor is providing relevant information to the intended audience, which enhances user understanding and protects sensitive information.
- **Content Provenance and Authentication**—Legislation should establish role-based requirements to provide content authentication and provenance information to increase the trustworthiness of AI-generated content.
- **Targeted Frontier Model Safety Protections**—Frontier model safety protections should target material national security risks and avoid overbroad requirements that stifle innovation in less advanced models.
- **National AI Standard**— Federal legislation should establish a national standard on AI, which is the most effective way to set clear rules of the road for businesses and consistent expectations for

[1] *BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.*

consumers, and preempt corresponding state requirements to minimize a patchwork of conflicting obligations and accelerate increased AI adoption.

- **Accelerating AI Development and Adoption**—Congress should pass legislation that includes measures to accelerate AI adoption, including enhancing research and development (R&D), workforce development and labor market analysis, international coordination, and development of standards and best practices that support responsible AI development and use.

Risk-Based Approaches. At the outset, we acknowledge that, because the utility and benefits of AI are so diffuse, it implicates a wide range of issues. We caution, however, against imposing requirements that govern all uses of AI, as many low-risk uses, such as enabling enhanced workflow collaboration or better budget forecasting, do not raise the same level of concerns that might arise in other scenarios, such as the management and operation of critical infrastructure or eligibility determinations for important life opportunities.[2] As a result, we encourage Congress to take a risk-based approach both with respect to its consideration of what areas should be regulated and who should be regulated.

Role-Based Responsibilities. AI legislation should assign role-based responsibilities to ensure that obligations fit the role of the company. The AI supply chain is complex and evolving and includes a variety of companies, including AI developers, integrators, and deployers.[3] In practice, developers have insight into model design and training, integrators into system-level modifications, and deployers into real-world use and user impacts. Creating role-based responsibilities for different AI actors is important for several distinct but related reasons. First, it assigns responsibilities to companies that they can implement based on their access to relevant information and position in the AI supply chain, preventing unworkable obligations for things outside of their control. Second, it ensures that consumers and business customers are better protected because the companies that are best positioned to identify and address risks are the entities designated to take relevant steps to protect them. Third, it creates a policy framework that is workable in practice.

Relevant Transparency Disclosures. Transparency obligations should recognize four key guiding principles: (1) the responsibility should fit the role of the company in the AI value chain; (2) the information an AI actor shares should be relevant to the intended audience; (3) trade secrets and confidential proprietary information should be protected; and (4) companies should maintain flexibility to determine the appropriate mechanisms for communicating relevant information. In some instances, regulators may want access to non-public information to assess a company's legal compliance. In cases where a potential law violation exists, regulators may exercise existing authority to request relevant documentation, subject to protections and safeguards for trade secrets and other proprietary information. Importantly, this information exchange should not be a routine, proactive reporting obligation, as that imposes additional, and frequently burdensome, responsibilities on companies, sweeps too broadly, introduces a risk of inadvertent disclosures because companies' sensitive information is shared more widely, and does not meaningfully address broader transparency goals.

Content Provenance and Authentication. BSA understands that, with the advent of generative AI, innovative AI-powered content creation can also raise questions about whether an image, audio, or video file is authentic, which could undermine trustworthiness in the marketplace. As a result, BSA supports obligations for generative AI application developers to leverage open, technical standards, such as the Coalition for Content Provenance and Authenticity (C2PA) standard, to enable machine-readable, non-visible disclosures for AI-generated images, audio, and video.[4] This approach would help users understand the origin and history of AI-generated content, increasing trust and reliability in the AI ecosystem. BSA does

---

[2] *See* BSA, Everyday AI for Businesses, https://www.bsa.org/policy-filings/everyday-ai-for-businesses.

[3] *See* BSA, Effective Accountability Along the AI Value Chain: Right-Sizing AI Responsibilities for the Role, https://www.bsa.org/policy-filings/effective-accountability-ai-value-chain-right-sizing-ai-responsibilities-role.

[4] *See* BSA, Primer on Content Authenticity, https://www.bsa.org/policy-filings/primer-on-content-authenticity.

not support visible labeling requirements because such labels can be easily removed, spoofed, or separated from content when it is edited or shared across platforms, making visible labels an ineffective and less durable means of communicating provenance than machine-readable metadata. In addition, BSA recognizes related concerns associated with deepfakes and supports legislation that would afford public figures, artists, and other creators with a right to prevent the unauthorized dissemination or use of their name, image, likeness, or voice and the unauthorized impersonation of creators, consistent with First Amendment protections.

Targeted Frontier Model Safety Protections. We understand that it may be appropriate to implement measures to address frontier models with advanced capabilities that pose material national security risks. In those circumstances, it is important that legislation be appropriately scoped, targeting the provision of expert-level assistance in the creation of chemical, biological, radiological, or nuclear threats or advanced frontier cybersecurity attacks. Other important considerations include ensuring that the threshold for covered models is sufficiently robust that it does not capture less advanced and lower-risk models, including by identifying both a high compute threshold and a capabilities-based evaluation that ensures only models posing material national security risks are covered. In addition, to the extent that incident reporting requirements are imposed in this narrow context, which may not be appropriate in other settings, they should be narrowly scoped, such as applying to the unauthorized modification or exfiltration of model weights, allow sufficient time for reporting after discovery, be directed to a single, national entity, and avoid duplication or overlap with existing reporting requirements, such as cybersecurity reporting requirements.

We note that AI is also critical to strengthening cybersecurity and encourage approaches that also advance that goal. Policymakers must understand that LLMs are not, and never will be, a standalone cybersecurity solution. Effective frontier AI defense requires the scaffolding of a comprehensive, defense-in-depth architecture — spanning network, cloud, endpoint, and application layers — because these models alone cannot substitute for the breadth of capabilities that a robust security posture demands.

National AI Standard. We believe that a national standard on AI is the most effective way to set clear rules of the road for businesses and consistent expectations for consumers. To be effective, a national framework should address both AI development and use and preempt corresponding state obligations to minimize a patchwork of competing and/or burdensome obligations and accelerate increased AI adoption.

Accelerating AI Development and Adoption. BSA supports measures that will accelerate AI adoption, including enhancing R&D, workforce development and labor market analysis, international coordination, and development of standards and best practices that support responsible AI development and use. Congressional proposals include a range of initiatives that would help achieve this goal, including codifying the Center for AI Standards and Innovation (CAISI); permanently establishing the National AI Research Resource (NAIRR), which would expand access to AI resources to small businesses, students, and researchers and enhance U.S. AI research capabilities; expanding AI education; investing in workforce preparedness; and modernizing labor statistics to enable better forecasting to predict workforce trends.

***

BSA looks forward to working with you, the other members of the Senate Committee on Commerce, Science, and Transportation, as well as other Members of Congress, to advance AI legislation that achieves these important objectives.

Sincerely,

Shaundra Watson

Shaundra Watson
Senior Director, Policy