CHAMBER OF PROGRESS

May 23, 2024

The Honorable Chair John W. Hickenlooper
Chair, Subcommittee on Consumer Protection, Product Safety, and Data Security
Committee of Commerce, Science, and Transportation of the Senate
Russell Senate Office Building 254
Washington, DC, 20510

Re: The "Validation and Evaluation for Trustworthy (VET) Artificial Intelligence Act"

On behalf of Chamber of Progress – a tech industry association supporting public policies to build a more inclusive country in which all people benefit from technological leaps – we appreciate the opportunity to share feedback in response to the VET AI Act version 2.

Artificial intelligence (AI) systems have already proven to have tremendously transformative applications in the education and the creative sector. However, we also acknowledge the potential for harm, particularly when deployed by government actors. Accordingly, there is space for sound AI specifications - and guidance on best practices for assurances is an appropriate place to start.

In scoping assurances for testing and evaluating AI systems, any system should prioritize the design, development, and deployment. This will enable the assessment of technical robustness, legal compliance, and adherence to predefined principles. The assurance should also focus on the *direct* impact of the AI system's outputs on third parties. Assessing for secondary or tertiary impacts is beyond the scope of any initial regime - and stands to stifle beneficial progress.

The specifications for an AI assurance should be tailored to both upstream developers and downstream deployers. Upstream developers should be accountable for the robustness and adequacy of the technology's development processes, while downstream deployers should be responsible for ensuring legal compliance and evaluating the impact of the AI system on users and the

environment. To reiterate: it is essential to delineate responsibility with respect to the role the software plays. Developers should be held accountable for their conduct and end users for theirs. External AI assurances should not require developers or deployers to mitigate proactively against unreasonable or unforeseeable risks, including the misbehavior of end users.

Finally, any vetting regime should not preference incumbent models versus new entrants or vice versa. A differential regime, particularly one that blesses extant models or closed source models with lighter regulatory scrutiny creates a regulatory moat. To that end, we encourage you to clarify the exclusions in Sec. 3.2(B)i to make clear that existing systems do not get special regulatory treatment.

We commend the author for including confidentiality in Section 11 to protect sensitive information obtained during the assurance process.

Thank you for the opportunity to share this feedback, we look forward to discussing your proposed VET AI Act further at your convenience.

Thank you,

Chamber of Progress