United States Senate

WASHINGTON, DC 20510

July 24, 2023

President Joseph R. Biden
1600 Pennsylvania Avenue NW
Washington, DC 20500

Dear President Biden,

I write to applaud the Administration's significant efforts to secure voluntary commitments from leading AI vendors related to promoting greater security, safety, and trust through improved development practices. These commitments – largely applicable to these vendors' most advanced products – can materially reduce a range of security and safety risks identified by researchers and developers in recent years. In April, I wrote to a number of these same companies, urging them to prioritize security and safety in their development, product release, and post-deployment practices. Among other things, I asked them to fully map dependencies and downstream implications of compromise of their systems; focus greater financial, technical and personnel resources on internal security; and improve their transparency practices through greater documentation of system capabilities, system limitations, and training data.

These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, even less capable models are susceptible to misuse, security compromise, and proliferation risks. Moreover, a growing roster of highly-capable open source models have been released to the public – and would benefit from similar pre-deployment commitments contained in a number of the July 21st obligations. As the current commitments stand, leading vendors do not appear inclined to extending these vital development commitments to the wider range of AI products they have released that fall below this threshold or have been released as open source models.

To be sure, responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this burgeoning and highly consequential industry – and in the downstream industries integrating their products. In the interim, the important commitments your Administration has secured can be bolstered in a number of important ways.

First, I strongly encourage your Administration to continue engagement with this industry to extend these all of these commitments more broadly to less capable models that, in part through their wider adoption, can produce the most frequent examples of misuse and compromise.

Second, it is vital to build on these developer- and researcher-facing commitments with a suite of lightweight consumer-facing commitments to prevent the most serious forms of abuse. Most prominent among these should be commitments from leading vendors to adopt development

practices, licensing terms, and post-deployment monitoring practices that prevent non-consensual intimate image generation, social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents.

Lastly, the Administration's successful high-level engagement with the leadership of these companies must be complemented by a deeper engagement strategy to track national security risks associated with these technologies. In June, the Senate Select Committee on Intelligence on a bipartisan basis advanced our annual *Intelligence Authorization Act*, a provision of which directed the President to establish a strategy to better engage vendors, downstream commercial users, and independent researchers on the security risks posed by, or directed at, AI systems.

This provision was spurred by conversations with leading vendors, who confided that they would not know how best to report malicious activity – such as suspected intrusions of their internal networks, observed efforts by foreign actors to generate or refine malware using their tools, or identified activity by foreign malign actors to generate content to mislead or intimidate voters. To be sure, a highly-capable and well-established set of resources, processes, and organizations – including the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Office of the Director of National Intelligence's Foreign Malign Influence Center – exist to engage these communities, including through counter-intelligence education and defensive briefings. Nonetheless, it appears that these entities have not been fully activated to engage the range of key stakeholders in this space. For this reason, I would encourage you to pursue the contours of the strategy outlined in our pending bill.

Thank you for your Administration's important leadership in this area. I look forward to working with you to develop bipartisan legislation in this area.

Sincerely,

Mark R. Warner
United States Senator

Cc:

Jake Sullivan, National Security Advisor
Arati Prabhakar, Director of the Office of Science and Technology Policy
Avril Haines, Director of National Intelligence