Little Tech Association

July 22, 2026

Michael Kratsios
Director
Office of Science and Technology Policy

The Honorable Howard Lutnick
Secretary of Commerce
U.S. Department of Commerce

cc: The President; The Vice President; Sean Cairncross, National Cyber Director

Re: Principles for American leadership in open-weight AI

Dear Director Kratsios and Secretary Lutnick:

The Little Tech Association represents founders building the next generation of American technology companies. The AI Action Plan supports open-weight models so startups can build without dependence on a closed provider and recognizes their geostrategic value. The June 2 order established a voluntary security framework for cooperation with frontier developers. Three days later, NSPM-11 directed the national-security enterprise to adapt commercial or open-source AI from diverse suppliers and preserve operational control over mission systems. Federal policy should preserve the ability of American developers to release open-weight models while addressing specific security risks through safeguards tied to capability, users, and deployment.

This means a founder can switch to a different host, evaluate a model, run it in a customer's environment, and still serve users even if a platform changes its pricing or direction. Denying American startups access to models available abroad would stifle competition, entrench incumbents, and function as a tax on intelligence, raising their costs and narrowing their choices while foreign competitors retain access to the full global market.

For example, in rural hospitals, factories, government agencies, companies that supply defense equipment, and teams that respond to cyberattacks, models need to be customized to their particular systems and usable within their own secure networks. In a recent survey of Y Combinator founders, nearly half of responding companies run the majority of their production workloads on open-weight models, overwhelmingly on American inference providers or their own hardware. When these organizations host their own models, they can keep sensitive information such as patient records, industrial data, login credentials, and incident logs under their control. This also gives the people responsible for defending these systems a model to examine and use, even when a remote service isn't suitable for their specific mission.

One person can make a model better, another can make it work for a specific area, and another can find a weakness in its security. In the U.S., models can improve faster when the people building them can study, adapt, and use them in their own work.

Recent releases by Chinese companies show that open distribution is now a competitive strategy: Moonshot launched Kimi K3 and scheduled publication of its weights for July 27, while Alibaba previewed Qwen3.8 Max and said open weights would follow. American leadership requires two things: world-leading American open-weight models and continued access for U.S. builders to open models already available worldwide, with proportionate safeguards for hosting, evaluation, and provenance developed alongside allies.

Five principles should govern federal action:

1. American developers should remain free to publish model weights unless the government demonstrates that publication itself creates a material risk distinct from comparable hosted access and that narrower safeguards cannot address it. Any durable threshold should rest on clear statutory authority and published, objective, time-limited criteria.

2. Preserve access to existing open models while applying stronger safeguards to exceptional capabilities, frontier-scale hosted inference, prohibited users, and sensitive deployments. Even when their weights are public, frontier-scale models will ordinarily be accessed through specialized cloud or inference providers, where customer verification, logging, rate limits, and restrictions on prohibited users can reduce risk without restricting publication itself.

3. Federal agencies may apply heightened procurement and security requirements to models developed, controlled, or remotely operated by an entity subject to a foreign adversary's jurisdiction when those models are used in government, national-security, or critical-infrastructure systems. Domestic hosting, fine-tuning, or ordinary commercial deployment of publicly available weights should not, standing alone, trigger heightened requirements absent continuing foreign control, remote access, or data exposure. Those safeguards should remain proportionate to the system and use case and should not become an economy-wide barrier to open-weight development.

4. Remote access to controlled compute and hosted frontier-scale inference can be logged and conditioned on proportionate security requirements. Federal policy should deter model theft, credential fraud, and nonconsensual extraction at scale while preserving authorized training, interoperability, and legitimate research. Once published, model weights can be copied across borders at near-zero marginal cost, making post-release controls difficult to enforce. Therefore, the government should focus on measures it can realistically observe, attribute, and enforce.

5. Each control should clearly state what it aims to achieve, how it will be measured, and when it will be reviewed. Agencies should also compare results against models and services available abroad and to work with allies on common evaluation and security practices.

The Little Tech Association is prepared to collaborate with key government agencies, including the Office of Science and Technology Policy, the Department of Commerce, and the Office of the National Cyber Director, on evaluations, secure deployment, provenance, compute controls, and practical compliance design. By doing so, the United States will take the lead in this significant platform shift, driven by innovative founders who have the freedom to select their tools, own their systems, and transform untested ideas into successful companies that the world relies on.

Respectfully submitted,
The 179 undersigned founders and member companies of the Little Tech Association.

1849 Bio	Adapted Health	Agency	Agency Tool Company
AgentCollect	Agree Ahmed	AI Tech Packs	Aidy
Alphawatch AI	Anakin	Andi	Assembly HOA
Astraea	Atlia	Automax.ai	AutoSitu
Avion	Awesomic Labs	barkbase.app	Bilanc Finance Inc.
Bramante Biologics Corporation	Bucket Robotics	Cabana	Casco
Cheers	chromie.dev	Clara	Clarm
Clearly AI	Convictional, Inc.	Corsair	CTGT
Dart	Decisional	Deferred	DERYA MARITIME INC
Dex	Diode, Inc.	Dispatch	Dots
Edgerun	EffiGov	Ego Live Inc.	Ember AI
Emdash	Empirical Health	Everest	Exla
Fed10	flowscope	Flywheel AI	Forerunner
Forge Robotics	Frizzle	FullSeam	Garage
Gecko Security	Glep Payments	Greypoint Industries	GUILD
Hera	Hermai	Hermes Robotics	Hop Aero
Instacrops	Integuru	Inversion Semiconductor Inc.	JadeIQ Inc
Justinian	Kadro	Kaelio	Khoj
Klime	Koyal AI Inc.	Labdoor	Ligo Biosciences
LunaJoy	Madrone	Magic Hour AI, Inc.	make sunsets
Manufact	Marengo	Meadow	Mem0
Mesmer Labs, Inc.	Metalware, Inc.	Miso	Mithras Industrial
Monarch	Morphik, Inc.	Mytos	NOX METALS
Nua AI	Null Labs	Offbeast	Olam Labs
One Robot	OpenRelay	Opensteer	OpenTrade
Orange Collective	Osmosis	Outpaint	Paces
Palus Finance	Panora	ParadeDB	Parsagon
Parse	Parsewise	Partcl, Inc.	Payna
Pebble	Pennant	Perceptron ML	Pier
Pinnacle Software Development	Pipekit	Poka Labs	Posh Energy
Prescience, Inc.	Proton	Pulse	Reach Power
Reality Defender	Redemption Games	Refresh	Regbase
Reshma Khilnani	Ridecell	Rig	RiskCube
Ritivel	Roundabout Technologies	Rovi Health	Saldor
Sarama	Scheduling Wizard	SchoolMint	Sei AI
Sennu AI	Senri Labs, Inc.	Shiboleth.ai	SID
Slashy	Sol Browser	Soria Analytics	Sourdough Technologies Inc.
Spaceflow Technologies, Inc.	Specific	Spectre Capital	Spice Data
Standard Signal	Stellar Sleep	Sterling Road	Surge
Talkshi	Tavus	TaxGPT Inc.	Terminal Use
The General Aviation Company	The Smart Coop	TinySeed	Tire Swing
Ultrasonium	Understudy Labs	Vantedge AI	VELA AI
Velt	Veria Labs, Inc.	Veryfi, Inc.	Vivaldi
Voker	Vouch, Inc.	Waypoint	Weave
WithAI	Y Combinator	Yuzu Labs AI	