Congress of the United States
House of Representatives
Washington, DC 20515

July 31, 2026

Mr. Tony Xu
Co-Founder and Chief Executive Officer
DoorDash, Inc.
303 2nd Street Suite 800
San Francisco, CA 94107

Dear Mr. Xu:

The House Committee on Homeland Security and the House Select Committee on the Chinese Communist Party (the Committees) are conducting a joint investigation into the national security, cybersecurity, and economic security implications of U.S. companies integrating artificial intelligence (AI) models developed in the People's Republic of China (PRC) into consumer platforms, enterprise software, and systems with access to sensitive commercial or personal information.[1]

Since opening this investigation in April 2026, the Committees have examined the technical, security, and commercial considerations that lead U.S. companies to evaluate and deploy PRC-developed models.[2] The investigation has shown that certain PRC-developed open-weight models may offer competitive performance, lower operating costs, and greater control over customization and deployment than proprietary models whose weights remain controlled by the developer and are generally accessed through a hosted service or managed cloud platform. Because open weights can be obtained and deployed on infrastructure selected by the user, companies may be able to operate these models within computing environments subject to their own security and governance controls.

Those characteristics may mitigate certain data governance and vendor dependency risks, but they do not resolve questions about how a model's capabilities were developed, whether the weights, code, and dependencies were obtained from trustworthy sources, or how the model will behave when given access to proprietary data, source code, development tools, or other sensitive resources. A meaningful evaluation must therefore extend beyond benchmark performance and cost. It should consider reasonably available information concerning the model and developer, the provenance and integrity of any deployed artifacts, the security of the surrounding software supply chain, the model's deployment architecture, permissions, and tool access, the results of security and reliability testing, and the company's ability to replace the model if new

[1] Letter from Chairman Andrew R. Garbarino & Chairman John Moolenaar to Brian Chesky, Chief Exec. Officer, Airbnb, Inc. (Apr. 28, 2026); Letter from Chairman Andrew R. Garbarino & Chairman John Moolenaar to Michael Truell, Co-Founder & Chief Exec. Officer, Anysphere, Inc. (Apr. 28, 2026).
[2] *Id*.

intelligence, legal restrictions, or material changes in the developer's risk profile make continued use unacceptable.

On July 6, 2026, DoorDash co-founder Andy Fang publicly stated that DoorDash had incorporated open-weight models into an internal AI-assisted code review system.[3] According to that statement, DoorDash routed more difficult tasks to a U.S.-developed frontier model and lower level work to Kimi K2.6, an open-weight model developed by Moonshot AI.[4] DoorDash further stated that it evaluated this configuration using DashBench, an internal coding benchmark, and found that it outperformed the configuration using Sonnet 4.6 and Opus 4.8 that it replaced while reducing costs.[5]

On July 22, 2026, the Director of the White House Office of Science and Technology Policy publicly stated that the U.S. Government possesses information indicating that Moonshot operated a covert platform to conduct large scale distillation against American AI models, used Anthropic's Fable model in the development of Kimi K3, and trained models using advanced GB300 systems that it was not authorized to obtain.[6] The Secretary of the Treasury separately indicated that the Administration may consider sanctions or trade restrictions against PRC firms engaged in the industrial scale extraction of American AI capabilities.[7]

These reported findings raise questions about Moonshot's development practices, its compliance with applicable legal and contractual restrictions, and the operational, supply chain, and continuity risks associated with reliance on its models. Evidence that a developer may have obtained capabilities through unauthorized distillation would not, on its own, establish that a particular model contains malicious code, compromised weights, or another technical defect. It would, however, constitute relevant information about the developer's practices and risk profile that a company may need to consider in deciding whether and under what conditions to continue using its technology. Those questions are particularly significant where a company reportedly uses a Moonshot model alongside technology developed by an American company whose models were allegedly targeted by Moonshot.

On June 8, 2026, the Department of War identified Alibaba Group, an investor in Moonshot AI, as a Chinese military company pursuant to Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.[8] Although that designation does not itself establish that Moonshot's models are compromised or prohibit private sector use of those models, it is relevant to an assessment of Moonshot's ownership, financing, affiliations, legal exposure, and potential supply chain dependencies.

---

[3] Andy Fang (@andyfang), *X* (July 6, 2026), https://x.com/andyfang/status/2074252174226493584.
[4] *Id*.
[5] DoorDash AI Research (@AIatDoorDash), *X* (July 6, 2026), https://x.com/AIatDoorDash/status/2074245510450528534.
[6] Director Michael Kratsios (@mkratsios47), *X* (July 22, 2026); *see* Kai Nicol-Schwarz, *Moonshot AI Accessed Nvidia's Chips Despite Chinese Export Ban, White House Official Says*, CNBC (July 23, 2026).
[7] Osmond Chia, *China's Moonshot AI Stole from Anthropic, Trump Tech Adviser Says*, BBC (July 22, 2026).
[8] U.S. Dep't of War., *Entities Identified as Chinese Military Companies Operating in the United States Pursuant to Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* (June 8, 2026).

At the same time, the Committees recognize that U.S. companies, from large technology firms[9] to startups,[10] may evaluate and deploy PRC-developed open-weight models because they can provide competitive capabilities, lower costs, greater customization, and alternatives to reliance on a small number of proprietary model providers. Those practical considerations do not eliminate the need for risk-based safeguards or diminish the national security concerns associated with growing dependence on models developed by entities subject to PRC jurisdiction. An effective federal approach should therefore scrutinize U.S. companies' reliance on PRC-developed models and strengthen the availability, security, and competitiveness of American open-weight alternatives, while applying appropriately tailored safeguards in sensitive and high-risk applications. This investigation is intended to establish the factual record necessary to inform that approach.

To advance the joint investigation, the Committees request that DoorDash, Inc. produce the following information and documents no later than August 14, 2026:

1. A complete inventory of each AI model developed by a PRC-based or PRC-controlled entity that DoorDash or any subsidiary has evaluated or used in development, testing, staging, or production since January 1, 2025. For each model, identify the developer; model, checkpoint, and version; any quantization or other material modification; the date and purpose of first use; current status; hosting and serving environment; whether DoorDash accessed the model through a hosted service or deployed model artifacts within infrastructure selected by DoorDash; the source from which the model, artifacts, or service were obtained; and, where applicable, the cryptographic hash or other identifier used to verify the deployed artifacts;

2. Documents sufficient to describe DashBench's methodology, test sets, scoring criteria, validation procedures, and results for the configuration incorporating Kimi K2.6, including comparisons with U.S.-developed and other non-PRC models; analyses of possible benchmark contamination, data leakage, or overfitting; and any security, reliability, legal, or operational considerations evaluated separately from coding performance and cost;

3. Documents sufficient to describe all security, assurance, and reliability testing conducted on Kimi K2.6 or any other PRC-developed model identified in response to Request 1. This request includes, as applicable to the manner in which the model was obtained and deployed, testing or analysis concerning artifact integrity; unauthorized modification; anomalous or trigger dependent behavior; insecure code generation; unauthorized disclosure or transmission of data; prompt injection; misuse of tools or permissions; and behavior under adversarial inputs. For each category not evaluated, identify whether DoorDash determined that the category was inapplicable, relied on testing conducted by another entity, accepted the residual risk, or addressed the risk through another control;

---

[9] Katherine Long, *Big Tech Companies Defend Open-Weight AI Models*, POLITICO (July 24, 2026).
[10] Sophia Cai, *Startup Founders Urge Trump Not to Shut Off Chinese Open-Weight AI*, POLITICO (July 22, 2026).

4. Risk assessments, decision memoranda, approval materials, meeting materials, and internal communications concerning the selection, approval, deployment, continued use, suspension, or replacement of Kimi K2.6 or another PRC-developed model identified in response to Request 1. This request includes materials addressing the model's intended use; access to data, code, tools, and systems; the developer's ownership and investors; obligations arising from PRC law; reports concerning unauthorized distillation or acquisition of U.S. model capabilities; potential U.S. sanctions, export controls, or other trade restrictions; and any material reevaluation conducted after July 22, 2026;

5. Documents sufficient to show, by month and business function, the request volume, token volume, computing or service costs, and estimated total operating costs associated with each PRC-developed model identified in response to Request 1. Produce documents explaining the technical, operational, or economic basis for selecting each model and any plan for suspending or replacing it if access becomes restricted, material vulnerabilities are identified, or the company's risk assessment changes;

6. Policies, standards, and procedures governing DoorDash's acquisition, approval, deployment, and continued use of third-party AI models, including any requirements concerning developer due diligence; model and artifact provenance; artifact verification; software dependencies; security and reliability testing; access controls and permissioning; monitoring; incident response; and reevaluation following material changes in a developer's ownership, legal status, affiliations, or risk profile; and

7. Documents sufficient to identify when DoorDash first became aware of allegations or U.S. Government information concerning Moonshot's reported use of unauthorized distillation, restricted computing systems, or other allegedly improper means of acquiring AI capabilities; any assessment DoorDash conducted in response; any changes made to the deployment, permissions, monitoring, or use of Kimi K2.6; and the individual or body responsible for deciding whether DoorDash would continue using the model.

The Committees further request that personnel with responsibility for DoorDash's AI infrastructure, software security, model evaluation, procurement, and legal or compliance review appear for an in-person briefing no later than August 21, 2026. To arrange production, coordinate the briefing, or discuss the scope of these requests, please contact majority staff of the Committee on Homeland Security at (202) 226-8417 and majority staff of the Select Committee on the Chinese Communist Party at (202) 226-1541.

Pursuant to Rules X and XI of the U.S. House of Representatives, the Committee on Homeland Security has jurisdiction over homeland security policy and oversight of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security." House Resolution 5 grants the Select Committee investigative jurisdiction over matters relating to "countering the economic,

technological, security, and ideological threats of the Chinese Communist Party to the United States and allies and partners of the United States." Upon receipt of this letter, please preserve all hard copy and electronic documents and communications related to its subject matter.

Sincerely,

ANDREW R. GARBARINO
Chairman
Committee on Homeland Security

JOHN MOOLENAAR
Chairman
Select Committee on China

cc: The Honorable Bennie Thompson, Ranking Member
Committee on Homeland Security

The Honorable Ro Khanna, Ranking Member
Select Committee on China