MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER



One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

May 21, 2025

VIA ELECTRONIC TRANSMISSION

Ms. Stella Li
Chief Executive Officer
BYD North America LLC
888 E. Walnut St.
Pasadena, CA 91101

Mr. Patrick Duan
Co-Chief Executive Officer
RIDE Mobility LLC
888 E. Walnut St., Suite 200B
Pasadena, CA 91101

Dear Ms. Li and Mr. Duan:

We write to request documents and information related to the corporate structure, data security practices, and operational footprint of BYD North America LLC ("BYD") and RIDE Mobility LLC ("RIDE") as part of an ongoing investigation into the national security risks posed by foreign-affiliated transportation manufacturers operating in the United States. Your companies' growing roles in the electric bus market, and the deployment of your vehicles across American transit systems, raise serious concerns about potential foreign influence, data exposure, and systemic vulnerabilities that may directly impact the security and integrity of U.S. transportation networks.

While BYD is incorporated in the United States,[1] it is a wholly owned subsidiary of BYD Company Ltd., which is headquartered in the People's Republic of China (PRC).[2] Under the PRC's expansive national security laws, PRC-based companies, and, in many cases, their subsidiaries and affiliates abroad, are required to cooperate with state intelligence and security services.[3] These legal provisions are broadly written and extraterritorial in scope, raising important considerations about whether sensitive data or technologies connected to your vehicles could be subject to PRC legal obligations or potentially accessible to the PRC's intelligence and security services.[4]

---

[1] State of California, Secretary of State, *Registration of Out-of-State Limited Liability Company*, File No. 202251913517, Filed August 9, 2022, https://static.bizprofile.net/4/8/8/5/1/3/4885138.pdf.
[2] BYD Co. LTD., *About the Company*, (last accessed May 15, 2025), Financial Times, https://markets.ft.com/data/equities/tearsheet/profile?s=1211:HKG.
[3] U.S. Senate, Committee on Homeland Security and Governmental Affairs, *Safeguarding the Homeland: Examining Conflicts of Interest in Federal Contracting to Protect America's Future*, September 24, 2024, 118th Cong., 2nd Session, https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Doshi-2024-09-24.pdf.
[4] *Id.*

Electric buses and other vehicles produced, manufactured, or assembled by your companies are equipped with a wide range of embedded technologies, including real-time geolocation systems, cellular modems, telematics control units, video surveillance platforms, diagnostic sensors, and cloud-based fleet management software.[5] When integrated into U.S. transportation networks, these vehicles can generate continuous streams of data concerning routing patterns, passenger movements, and location tracking, sometimes in proximity to sensitive sites such as military installations, government facilities, schools, or mass transit hubs.[6] If that data is handled or processed through foreign-controlled components, supply chains, or cloud infrastructure, it could be subject to exploitation in ways that compromise operational security and public safety.[7]

Recent public reports underscore how these risks are neither speculative nor isolated. A *Reuters* investigation published on May 14, 2025, revealed that U.S. energy officials discovered "rogue communication devices" embedded in PRC-manufactured solar inverters and batteries.[8] If this report is correct, these devices may have allowed for unauthorized communication channels that could bypass established cybersecurity safeguards, including firewalls, creating the potential for U.S. grid destabilization or coordinated disruption.[9] This alarming precedent illustrates the potential for similar covert capabilities to be embedded in other PRC-affiliated technologies, including those deployed in electric vehicles or public transit platforms. It also reinforces a broader pattern of the Chinese Communist Party (CCP) leveraging seemingly benign infrastructure, whether in energy,[10] maritime,[11] telecommunications,[12] or transportation, as strategic entry points for surveillance, disruption, or foreign influence operations.

We are also concerned by your companies' recent efforts to rebrand operations under the RIDE Mobility banner, a move that appears designed to portray your business as a U.S.-based domestic manufacturer. While rebranding is not itself improper, public representations made by RIDE fail to account for ongoing corporate and operational entanglements with PRC-based entities. This creates the appearance that your companies are seeking to circumvent procurement restrictions or avoid scrutiny applied to PRC-affiliated firms seeking access to the U.S. electric

---

[5] *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, 89 Fed. Reg. 79088 (proposed Sept. 26, 2024) (to be codified at 15 C.F.R. pt. 791).
[6] Jim Tankersley, "*Biden Calls Chinese Electric Vehicles a Security Threat*," Feb. 29, 2024, The New York Times, https://www.nytimes.com/2024/02/29/us/politics/biden-chinese-electric-vehicles.html.
[7] *Id.*
[8] Sarah McFarlane, "*Rogue communication devices found in Chinese solar power inverters*," May 14, 2025, Reuters, https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/.
[9] *Id.*
[10] *Id.*
[11] H. Comm. on Homeland Sec. & H. Select Comm. on the Strategic Competition Between the U.S. & the Chinese Communist Party, Majority Staff Report, *Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry* (Sept. 2024).
[12] Chris Jaikaran, Cong. R. Serv., IF12798, *Volt Typhoon Hacks of Telecommunications Companies and Federal Response Implications* (Jan. 23, 2025), https://crsreports.congress.gov/product/pdf/IF/IF12798.

vehicle market. This concern is magnified by your companies' extensive lobbying[13] and public relations efforts aimed at U.S. government officials,[14] labor unions, and local communities, often framed around themes of economic revitalization, domestic job creation, and "climate-friendly" innovation,[15] while omitting relevant ownership, data privacy, and implications for national security.

To inform our oversight and assess the full scope of these risks, we request that you produce the following documents and information no later than 5:00 p.m. on June 11, 2025:

1. A comprehensive list of all contracts, grants, financing, tax incentives, and subcontracts awarded to BYD and RIDE at the federal, state, and local levels since January 1, 2018. Please include the contracting agencies, project descriptions, contract values, primary points of contact, and any subcontracting or partnership arrangements associated with each contract.

2. A detailed breakdown of BYD and RIDE's ownership structures, including all parent, subsidiary, and affiliated entities, as well as any financial relationships, investments, or partnerships involving PRC state-owned enterprises, investment funds, or government-controlled entities. This should include all relevant investment entities, boards of directors, decision-making hierarchies, and any known PRC government influence or involvement.

3. All internal and external communications, agreements, and strategic plans related to the rebranding or positioning of RIDE as a U.S. company. This includes correspondence with all U.S. or PRC-based public relations firms, lobbying entities, trade associations, financial institutions, and any consultants engaged to influence public perception, regulatory classifications, or eligibility for federal contracts.

4. All documents, policies, and technical reports, whether formal, draft, or final, related to the collection, storage, and transmission of data obtained from BYD and RIDE-manufactured buses operating in the United States. Please specify in a written statement whether this data is or has **EVER** been shared directly with government or corporate officials in the PRC, or been transmitted to servers located in the PRC or those accessible to PRC-based personnel or third-party entities, and outline any safeguards in place to prevent unauthorized foreign access. You are further directed not to withhold responsive documents or materials based on any foreign legal

[13] Jarrett Renshaw and Tina Bellon, "*Electric bus maker BYD shows China complications in Biden climate push*," July 14, 2021, Reuters, https://www.reuters.com/business/sustainable-business/electric-bus-maker-byd-shows-china-complications-biden-climate-push-2021-07-14/.
[14] Rep. Judy Chu. *Southern California Congressmembers Urge NDAA Conferees to Drop Language Targeting BYD.* U.S. House of Representatives, November 13, 2019. https://chu.house.gov/media-center/press-releases/southern-california-congressmembers-urge-ndaa-conferees-drop-language.
[15] Press Release, *BYD and SMART Union Applaud Biden Administration Plan to Build Back Better with Support for Zero Emission Battery Electric Buses.* BYD USA, April 19, 2021. https://en.byd.com/news/byd-and-smart-union-applaud-biden-administration-plan-to-build-back-better-with-support-for-zero-emission-battery-electric-buses/.

requirements without first notifying the Committee in writing, identifying the legal restriction, and providing all supporting documentation for any such claim.

5. All internal and external cybersecurity risk assessments, penetration testing results, and security audits that have been conducted on BYD and RIDE vehicle software and telematics systems, including any assessments related to BYD and RIDE's electric transit and coach buses. This request includes, but is not limited to, any such assessments, tests, or audits conducted pursuant to contracts, agreements, or engagements with third-party vendors, cybersecurity firms, or other external entities acting on behalf of BYD and RIDE. In addition, please identify the third parties that conducted such assessments and provide documents or communications outlining the rationale, selection process, and methodologies used to select them, along with any metrics or frameworks BYD and RIDE use to define, measure, or classify cybersecurity risk.

6. All documentation detailing whether BYD and RIDE has **EVER** been required to comply with the PRC's National Intelligence Law, the Data Security Law, and the Cybersecurity Law, and a written statement confirming whether any PRC intelligence, security, or law enforcement agencies have **EVER** requested access to data collected from BYD and RIDE-manufactured electric vehicles operating in the United States. This should include internal and external legal analyses, communications with PRC government agencies, and any instances where BYD and RIDE has sought or received exemptions from such requirements.

7. A list of all formal partnerships, collective bargaining agreements, and financial transactions between BYD and RIDE and U.S.-based labor unions. Please provide any communications indicating how labor engagements were used to shape public or political narratives or to influence regulatory oversight.

8. All communications between BYD and RIDE and Members of Congress, congressional staff, or U.S. executive branch officials regarding security-related concerns, regulatory issues, or federal procurement policy. This includes lobbying efforts aimed at obtaining exemptions or influencing legislative or administrative determinations.

9. All agreements, memoranda of understanding, or financial relationships between BYD and RIDE and PRC government entities, including state-owned banks, sovereign wealth funds, or regulatory agencies. This includes documentation related to subsidies, tax incentives, export financing, or other PRC-backed programs that support BYD and RIDE's international operations.

10. A detailed list of all electric school buses manufactured by BYD and RIDE that are currently in operation by U.S. school districts or under contract within the United States. Please include geographic deployment, vehicle serial numbers, maintenance

and update responsibilities, data access agreements, and any remote diagnostic or telemetry capabilities utilized by BYD and RIDE personnel.

The security and integrity of America's transportation infrastructure must remain a top priority. We intend to take all necessary steps to ensure that entities with ties to foreign adversaries are not given access to critical U.S. transportation infrastructure. Failure to comply with this request may result in the Committee pursuing further compulsory measures.

Under Rule X of the U.S. House of Representatives, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security."

Thank you for your attention to this important matter and your prompt reply.

Sincerely,



MARK E. GREEN, M.D.
Chairman
Committee on Homeland Security



CARLOS A. GIMENEZ
Chairman
Subcommittee on Transportation
and Maritime Security



ELIJAH CRANE
Member of Congress

Encl.

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

The Honorable LaMonica McIver, Ranking Member
Subcommittee on Transportation and Maritime Security