United States Senate
WASHINGTON, DC 20510

February 3, 2026

Tekedra Mawakana
Dmitri Dolgov
Co-Chief Executive Officers
Waymo
1600 Amphitheatre Parkway
Mountain View, California

Dear Ms. Mawakana and Mr. Dolgov,

As automakers deploy autonomous vehicles (AVs) on public roads, the industry's practices around remote assistance operators (RAOs) — the individuals who intervene when an AV finds itself in an uncertain situation — are becoming increasingly important. Yet, AV companies, including Waymo, have provided little public information about their policies around RAOs — including if they are located in the United States. Without proper safeguards, the AV industry's reliance on RAOs could create serious safety, national security, and privacy risks. As Waymo continues to expand its operations, Congress and the public deserve assurance that its remote assistance operations will not endanger passengers, other road and vulnerable road users, or national security.

Despite the limited public knowledge about RAOs, every AV manufacturer and operator relies on them to help their autonomous driving systems (ADS) — the technology that operates the vehicle autonomously — drive safely. Although the exact role and performance for RAOs vary by manufacturer, RAOs intervene when an AV confronts a driving condition or situation in which the system either cannot or is unsure how to proceed. Notably, RAOs do not directly control the steering, braking, or acceleration of the vehicle. Instead, they provide guidance, approvals, or clarifications for how the ADS should handle a situation or road condition.[1] In practice, however, the difference between directly operating a vehicle and issuing specific directives to the ADS can be difficult to discern. RAOs are similar to aircraft dispatchers — a regulated profession — who, in joint agreement with the airline captain, decide flight planning, route and altitude selection, and aircraft legal compliance during flights and carry out these duties from a remote location.[2] In essence, RAOs are intended to serve as a critical backup, keeping the public safe when an AV cannot determine the correct driving decision. Information about these RAOs is therefore critical to understanding their potential safety and security risks.

Unfortunately, manufacturers have not disclosed several key details about their remote operations procedures. For example, except as required under a few state laws, AV companies

[1] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[2] Aircraft dispatchers, 14 C.F.R. Part 65, Subpart C.

have provided little information about how often an RAO must intervene and provide guidance to a vehicle or whether an RAO can take over full control of the vehicle and tele-drive.[3] Moreover, many manufacturers have not disclosed the number of RAOs that they employ, the location of these RAOs, and the number of AVs that a single RAO is responsible for at any given time. Companies have also provided little information about their fallback procedures if an RAO is unable to communicate with a vehicle's ADS. Although the AV industry trade association published a document on RAOs, it offers limited information on these issues, including failing to identify safety risks that remote assistance could introduce.[4] Given the growth in the AV industry, this information gap is unacceptable.

The location of RAOs is especially important for vehicle safety. As with all networks, the physical distance between the remote assistance operator and the ADS can have a significant impact on the timing of their communications.[5] Weather, natural disasters, and other factors can harm the reliability, speed, and latency of the network connection between an RAO and a vehicle's ADS. When latency interrupts a zoom call or streaming service, it may frustrate the user. When it slows down an RAO's ability to direct an AV, it could have much more serious consequences. For example, as operators help steer an ADS through difficult scenarios, the visual and audio information the operator receives may already be out of date, rendering any guidance potentially unsafe. In fact, researchers have found that latency as small as 300 milliseconds can reduce driving performance.[6] Yet, AV manufacturers face no minimum latency standards for transmission of driving data from the vehicle to the RAO.[7] Moreover, most RAOs are not required to be located in the same state or even *country* that the driving system operates in; only Florida requires remote operators to be located in the United States.[8] In other words, AV manufacturers may be relying on overseas RAOs — located thousands of miles from the operating domain of their autonomous vehicles — and expecting they can quickly intervene if an AV gets into an uncertain, and potentially dangerous, situation. The safety risks with such an approach are obvious.

---

[3] Even where a company has released data on RAOs, it's unclear if it's accurate. For example, in 2021, an anonymous former Waymo remote operator reportedly stated he had to "disengage" the driving system and intervene around 30 times per day, but Waymo publicly reported only 21 disengagements over more than 600,000 miles driven in 2020. The explanation for this substantial discrepancy is unclear. Hyunjoo Jim, *Insight: A secret weapon for self-driving car startups: Humans,* Reuters (Aug. 23, 2021), https://www.reuters.com/business/autos-transportation/secret-weapon-self-driving-car-startups-humans-2021-08-23/.

[4] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[5] Volico, *Network Latency: Root Causes and Solutions* (Apr. 8, 2025), https://www.volico.com/network-latency-root-causes-and-solutions/.

[6] Stephanie Neumeier et al, *Teleoperation: the holy grail to solve problems of automated driving? Sure, sure but latency matters,* 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (Sept. 2019), https://www.researchgate.net/publication/335941077_Teleoperation_The_Holy_Grail_to_Solve_Problems_of_Automated_Driving_Sure_but_Latency_Matters.

[7] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[8] Id.

Locating remote assistance operations in different states or countries from the operating vehicle creates additional security risks. For example, overseas remote assistance operations may be more susceptible to physical takeover by hostile actors, potentially granting them driver-like control of thousands of vehicles transporting passengers on American roads. Heavy and fast-moving vehicles could quickly become the weapons of foreign actors seeking to harm innocent Americans. Overseas RAOs also creates cybersecurity risks.[9] While any form of remote connectivity introduces cyber risk, locating remote assistance centers overseas significantly amplifies these vulnerabilities. Remote assistance personnel operating outside the United States may be subject to foreign laws and standards rather than U.S. cybersecurity and data-protection requirements. For these reasons, it is critical that autonomous vehicle operators ensure all remote assistance operations are located in the United States.

Many RAOs are also not required to hold a driver's license, raising significant concerns about their qualifications to influence the operation of a motor vehicle.[10] A driver's license is a foundational safety regulation that ensures anyone legally operating a vehicle on public roads has met a minimum standard of competence. Although RAOs are supposedly not tele-driving the vehicle, their responsibilities involve guiding autonomous systems through complex situations that demand substantial knowledge of driving laws, maneuvers, and real-world contexts. Although states such as Florida require these operators to hold a driver's license, other states where AVs are operating do not.[11] As a result, riders in these states, and in any future states with similar gaps in regulation, may find themselves in vehicles influenced by individuals who lack even a basic driver's license.

AV manufacturers are also not subject to any federal standard ensuring that their RAOs are sober while on duty or free from a history of impaired driving. Currently, no federal or state law explicitly requires remote operators to be sober while performing their duties.[12] Without such laws, an intoxicated RAO could provide unsafe guidance or fail to provide timely guidance altogether to a vehicle's ADS. Moreover, if an RAO is intoxicated and an AV is involved in a crash, questions of liability and accountability remain unresolved — an outcome that further undermines public safety.[13] Manufacturers frequently tout eliminating drunk driving as a key benefit of autonomous driving, yet they offer no assurances that their own remote assistance operators are held to any standards regarding past or current alcohol use while driving or providing remote assistance.

---

[9] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024) (to be codified at 15 C.F.R Part 7).

[10] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[11] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[12] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[13] Jesse L. Keeffe, Designated Driver-Less Cars? *Why Current Georgia Law Supports Liability for Intoxicated Drivers of Autonomous Vehicles*, 57 Ga. L. Rev. 1387-1412 (2023).

Finally, remote assistance raises serious privacy concerns. Conventional vehicles already collect vast amounts of sensitive personal information about drivers and passengers, which manufacturers often leverage for financial gain.[14] With numerous cameras and other sensors installed to enable an ADS to operate, AVs significantly enhance these privacy risks. RAOs further increase these risks by requiring the transfer of continuous video, sensor, and audio feeds — potentially capturing interior views, the vehicle's surroundings, and communications with passengers or nearby road users — from the AV to an RAO. Transmitting and processing these feeds introduces additional questions about data collection, retention, access controls, and passenger knowledge when an RAO is engaged. The public deserves clear, transparent answers about how these data are used, how long they are stored, who has access to them, and whether they are ever shared with outside organizations for any purpose.

Given the increasing deployment of driverless vehicles on U.S. roads, the public deserves a detailed overview of Waymo's remote-assistance operations, policies, metrics, and safeguards. Accordingly, I ask that you provide the following written information by February 17, 2026:

1. A complete description of Waymo's remote assistance operations, including:

    a) The roles and responsibilities of the remote assistance operator, such as whether the operator is limited to providing advice or instruction or is permitted to change's the vehicles trajectory or driving path;

    b) Whether your company ever allows RAOs to tele-drive a vehicle, beyond providing guidance to the AV;

    c) The frequency with which remote assistance sessions are invoked (for example, number of sessions per vehicle-mile or per trip), and the proportion of sessions that result in human input that alters the vehicle's driving plan;

    d) The number and location (city/state/country) of remote assistance centers or teams and number of RAOs at each location;

    e) Whether any remote assistance operators are located outside the United States, and if so, the countries and jurisdictions involved, and how your company conducts oversight, supervision and qualification of such overseas operators;

    f) The average and worst-case latency (broken down by location of each RAO center) between the vehicle and remote assistance operator from the time a request is generated by the vehicle until a human begins interaction and the time from human intervention to vehicle execution of any instruction;

    g) Whether all remote assistance operators are required to obtain and maintain a valid driver's license while serving as an operator;

[14] Press Release, Senator Edward Markey, *Senator Markey Urges FTC to Investigate Invasive Data Privacy Practices of Automakers* (Feb. 28, 2024).

h) The background screening process for remote assistance operator applicants, including past experience with alcohol impaired driving;

i) Procedures and protocols in place to prevent remote assistance operators from being intoxicated while performing their duties as operators;

j) A summary of the cybersecurity architecture protecting the link between vehicle and remote assistance infrastructure, including network encryption protocols, authentication of operators, redundancy and resilience measures, and data retention and access policies; and

k) The procedures by which remote assistance involvement is logged, audited, and reviewed for safety analysis, particularly during crashes or other safety incidents.

2. A detailed description of any recorded crash or disengagement event (or near-miss) in which remote assistance played a causal or contributory role, whether through advice, instruction, or operator override. For each event, please provide the date, location, description of remote assistance involvement, outcome (damages and injuries, if any), lessons learned, and remedial actions taken.

3. A description of your company's training, qualification, and monitoring practices for remote assistance operators, including how performance is measured, what credentials and oversight apply, how many hours RAOs work per shift, and how your company manages fatigue, distraction, and user-error for remote operators.

4. A copy of any internal policies or standards by which remote assistance operations are governed, such as remote assistance operator to vehicle ratios, escalation procedures, boundaries for remote operator intervention (such as speed limits, zones, vehicle states), and fallback planning when the remote connection fails or is degraded.

Thank you in advance for your cooperation and timely attention to this request. I look forward to your response.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

WASHINGTON, DC 20510

February 3, 2026

Elon Musk
Chief Executive Officer
Tesla
1 Tesla Road
Austin, Texas

Dear Mr. Musk,

As automakers deploy autonomous vehicles (AVs) on public roads, the industry's practices around remote assistance operators (RAOs) — the individuals who intervene when an AV finds itself in an uncertain situation — are becoming increasingly important. Yet, AV companies, including Tesla, have provided little public information about their policies around RAOs — including if they are located in the United States. Without proper safeguards, the AV industry's reliance on RAOs could create serious safety, national security, and privacy risks. As Tesla continues to expand its operations, Congress and the public deserve assurance that its remote assistance operations will not endanger passengers, other road and vulnerable road users, or national security.

Despite the limited public knowledge about RAOs, every AV manufacturer and operator relies on them to help their autonomous driving systems (ADS) — the technology that operates the vehicle autonomously — drive safely. Although the exact role and performance for RAOs vary by manufacturer, RAOs intervene when an AV confronts a driving condition or situation in which the system either cannot or is unsure how to proceed. Notably, RAOs do not directly control the steering, braking, or acceleration of the vehicle. Instead, they provide guidance, approvals, or clarifications for how the ADS should handle a situation or road condition.[1] In practice, however, the difference between directly operating a vehicle and issuing specific directives to the ADS can be difficult to discern. RAOs are similar to aircraft dispatchers — a regulated profession — who, in joint agreement with the airline captain, decide flight planning, route and altitude selection, and aircraft legal compliance during flights and carry out these duties from a remote location.[2] In essence, RAOs are intended to serve as a critical backup, keeping the public safe when an AV cannot determine the correct driving decision. Information about these RAOs is therefore critical to understanding their potential safety and security risks.

Unfortunately, manufacturers have not disclosed several key details about their remote operations procedures. For example, except as required under a few state laws, AV companies have provided little information about how often an RAO must intervene and provide guidance

[1] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[2] Aircraft dispatchers, 14 C.F.R. Part 65, Subpart C.

to a vehicle or whether an RAO can take over full control of the vehicle and tele-drive.[3] Moreover, many manufacturers have not disclosed the number of RAOs that they employ, the location of these RAOs, and the number of AVs that a single RAO is responsible for at any given time. Companies have also provided little information about their fallback procedures if an RAO is unable to communicate with a vehicle's ADS. Although the AV industry trade association published a document on RAOs, it offers limited information on these issues, including failing to identify safety risks that remote assistance could introduce.[4] Given the growth in the AV industry, this information gap is unacceptable.

The location of RAOs is especially important for vehicle safety. As with all networks, the physical distance between the remote assistance operator and the ADS can have a significant impact on the timing of their communications.[5] Weather, natural disasters, and other factors can harm the reliability, speed, and latency of the network connection between an RAO and a vehicle's ADS. When latency interrupts a zoom call or streaming service, it may frustrate the user. When it slows down an RAO's ability to direct an AV, it could have much more serious consequences. For example, as operators help steer an ADS through difficult scenarios, the visual and audio information the operator receives may already be out of date, rendering any guidance potentially unsafe. In fact, researchers have found that latency as small as 300 milliseconds can reduce driving performance.[6] Yet, AV manufacturers face no minimum latency standards for transmission of driving data from the vehicle to the RAO.[7] Moreover, most RAOs are not required to be located in the same state or even *country* that the driving system operates in; only Florida requires remote operators to be located in the United States.[8] In other words, AV manufacturers may be relying on overseas RAOs — located thousands of miles from the operating domain of their autonomous vehicles — and expecting they can quickly intervene if an AV gets into an uncertain, and potentially dangerous, situation. The safety risks with such an approach are obvious.

---

[3] Even where a company has released data on RAOs, it's unclear if it's accurate. For example, in 2021, an anonymous former Waymo remote operator reportedly stated he had to "disengage" the driving system and intervene around 30 times per day, but Waymo publicly reported only 21 disengagements over more than 600,000 miles driven in 2020. The explanation for this substantial discrepancy is unclear. Hyunjoo Jim, *Insight: A secret weapon for self-driving car startups: Humans,* Reuters (Aug. 23, 2021), https://www.reuters.com/business/autos-transportation/secret-weapon-self-driving-car-startups-humans-2021-08-23/.

[4] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[5] Volico, *Network Latency: Root Causes and Solutions* (Apr. 8, 2025), https://www.volico.com/network-latency-root-causes-and-solutions/.

[6] Stephanie Neumeier et al, *Teleoperation: the holy grail to solve problems of automated driving? Sure, sure but latency matters,* 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (Sept. 2019), https://www.researchgate.net/publication/335941077_Teleoperation_The_Holy_Grail_to_Solve_Problems_of_Automated_Driving_Sure_but_Latency_Matters.

[7] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[8] Id.

Locating remote assistance operations in different states or countries from the operating vehicle creates additional security risks. For example, overseas remote assistance operations may be more susceptible to physical takeover by hostile actors, potentially granting them driver-like control of thousands of vehicles transporting passengers on American roads. Heavy and fast-moving vehicles could quickly become the weapons of foreign actors seeking to harm innocent Americans. Overseas RAOs also creates cybersecurity risks.[9] While any form of remote connectivity introduces cyber risk, locating remote assistance centers overseas significantly amplifies these vulnerabilities. Remote assistance personnel operating outside the United States may be subject to foreign laws and standards rather than U.S. cybersecurity and data-protection requirements. For these reasons, it is critical that autonomous vehicle operators ensure all remote assistance operations are located in the United States.

Many RAOs are also not required to hold a driver's license, raising significant concerns about their qualifications to influence the operation of a motor vehicle.[10] A driver's license is a foundational safety regulation that ensures anyone legally operating a vehicle on public roads has met a minimum standard of competence. Although RAOs are supposedly not tele-driving the vehicle, their responsibilities involve guiding autonomous systems through complex situations that demand substantial knowledge of driving laws, maneuvers, and real-world contexts. Although states such as Florida require these operators to hold a driver's license, other states where AVs are operating do not.[11] As a result, riders in these states, and in any future states with similar gaps in regulation, may find themselves in vehicles influenced by individuals who lack even a basic driver's license.

AV manufacturers are also not subject to any federal standard ensuring that their RAOs are sober while on duty or free from a history of impaired driving. Currently, no federal or state law explicitly requires remote operators to be sober while performing their duties.[12] Without such laws, an intoxicated RAO could provide unsafe guidance or fail to provide timely guidance altogether to a vehicle's ADS. Moreover, if an RAO is intoxicated and an AV is involved in a crash, questions of liability and accountability remain unresolved — an outcome that further undermines public safety.[13] Manufacturers frequently tout eliminating drunk driving as a key benefit of autonomous driving, yet they offer no assurances that their own remote assistance operators are held to any standards regarding past or current alcohol use while driving or providing remote assistance.

---

[9] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024) (to be codified at 15 C.F.R Part 7).

[10] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[11] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[12] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[13] Jesse L. Keeffe, Designated Driver-Less Cars? *Why Current Georgia Law Supports Liability for Intoxicated Drivers of Autonomous Vehicles*, 57 Ga. L. Rev. 1387-1412 (2023).

Finally, remote assistance raises serious privacy concerns. Conventional vehicles already collect vast amounts of sensitive personal information about drivers and passengers, which manufacturers often leverage for financial gain.[14] With numerous cameras and other sensors installed to enable an ADS to operate, AVs significantly enhance these privacy risks. RAOs further increase these risks by requiring the transfer of continuous video, sensor, and audio feeds — potentially capturing interior views, the vehicle's surroundings, and communications with passengers or nearby road users — from the AV to an RAO. Transmitting and processing these feeds introduces additional questions about data collection, retention, access controls, and passenger knowledge when an RAO is engaged. The public deserves clear, transparent answers about how these data are used, how long they are stored, who has access to them, and whether they are ever shared with outside organizations for any purpose.

Given the increasing deployment of driverless vehicles on U.S. roads, the public deserves a detailed overview of Tesla's remote-assistance operations, policies, metrics, and safeguards. Accordingly, I ask that you provide the following written information by February 17, 2026:

1. A complete description of Tesla's remote assistance operations, including:

    a) The roles and responsibilities of the remote assistance operator, such as whether the operator is limited to providing advice or instruction or is permitted to change's the vehicles trajectory or driving path;

    b) Whether your company ever allows RAOs to tele-drive a vehicle, beyond providing guidance to the AV;

    c) The frequency with which remote assistance sessions are invoked (for example, number of sessions per vehicle-mile or per trip), and the proportion of sessions that result in human input that alters the vehicle's driving plan;

    d) The number and location (city/state/country) of remote assistance centers or teams and number of RAOs at each location;

    e) Whether any remote assistance operators are located outside the United States, and if so, the countries and jurisdictions involved, and how your company conducts oversight, supervision and qualification of such overseas operators;

    f) The average and worst-case latency (broken down by location of each RAO center) between the vehicle and remote assistance operator from the time a request is generated by the vehicle until a human begins interaction and the time from human intervention to vehicle execution of any instruction;

    g) Whether all remote assistance operators are required to obtain and maintain a valid driver's license while serving as an operator;

[14] Press Release, Senator Edward Markey, *Senator Markey Urges FTC to Investigate Invasive Data Privacy Practices of Automakers* (Feb. 28, 2024).

h) The background screening process for remote assistance operator applicants, including past experience with alcohol impaired driving;

i) Procedures and protocols in place to prevent remote assistance operators from being intoxicated while performing their duties as operators;

j) A summary of the cybersecurity architecture protecting the link between vehicle and remote assistance infrastructure, including network encryption protocols, authentication of operators, redundancy and resilience measures, and data retention and access policies; and

k) The procedures by which remote assistance involvement is logged, audited, and reviewed for safety analysis, particularly during crashes or other safety incidents.

2. A detailed description of any recorded crash or disengagement event (or near-miss) in which remote assistance played a causal or contributory role, whether through advice, instruction, or operator override. For each event, please provide the date, location, description of remote assistance involvement, outcome (damages and injuries, if any), lessons learned, and remedial actions taken.

3. A description of your company's training, qualification, and monitoring practices for remote assistance operators, including how performance is measured, what credentials and oversight apply, how many hours RAOs work per shift, and how your company manages fatigue, distraction, and user-error for remote operators.

4. A copy of any internal policies or standards by which remote assistance operations are governed, such as remote assistance operator to vehicle ratios, escalation procedures, boundaries for remote operator intervention (such as speed limits, zones, vehicle states), and fallback planning when the remote connection fails or is degraded.

Thank you in advance for your cooperation and timely attention to this request. I look forward to your response.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

WASHINGTON, DC 20510

February 3, 2026

Aicha Evans
Chief Executive Officer
Zoox Inc.
1149 Chess Drive
Foster City, California

Dear Ms. Evans,

As automakers deploy autonomous vehicles (AVs) on public roads, the industry's practices around remote assistance operators (RAOs) — the individuals who intervene when an AV finds itself in an uncertain situation — are becoming increasingly important. Yet, AV companies, including Zoox, have provided little public information about their policies around RAOs — including if they are located in the United States. Without proper safeguards, the AV industry's reliance on RAOs could create serious safety, national security, and privacy risks. As Zoox continues to expand its operations, Congress and the public deserve assurance that its remote assistance operations will not endanger passengers, other road and vulnerable road users, or national security.

Despite the limited public knowledge about RAOs, every AV manufacturer and operator relies on them to help their autonomous driving systems (ADS) — the technology that operates the vehicle autonomously — drive safely. Although the exact role and performance for RAOs vary by manufacturer, RAOs intervene when an AV confronts a driving condition or situation in which the system either cannot or is unsure how to proceed. Notably, RAOs do not directly control the steering, braking, or acceleration of the vehicle. Instead, they provide guidance, approvals, or clarifications for how the ADS should handle a situation or road condition.[1] In practice, however, the difference between directly operating a vehicle and issuing specific directives to the ADS can be difficult to discern. RAOs are similar to aircraft dispatchers — a regulated profession — who, in joint agreement with the airline captain, decide flight planning, route and altitude selection, and aircraft legal compliance during flights and carry out these duties from a remote location.[2] In essence, RAOs are intended to serve as a critical backup, keeping the public safe when an AV cannot determine the correct driving decision. Information about these RAOs is therefore critical to understanding their potential safety and security risks.

Unfortunately, manufacturers have not disclosed several key details about their remote operations procedures. For example, except as required under a few state laws, AV companies have provided little information about how often an RAO must intervene and provide guidance

[1] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[2] Aircraft dispatchers, 14 C.F.R. Part 65, Subpart C.

to a vehicle or whether an RAO can take over full control of the vehicle and tele-drive.[3] Moreover, many manufacturers have not disclosed the number of RAOs that they employ, the location of these RAOs, and the number of AVs that a single RAO is responsible for at any given time. Companies have also provided little information about their fallback procedures if an RAO is unable to communicate with a vehicle's ADS. Although the AV industry trade association published a document on RAOs, it offers limited information on these issues, including failing to identify safety risks that remote assistance could introduce.[4] Given the growth in the AV industry, this information gap is unacceptable.

The location of RAOs is especially important for vehicle safety. As with all networks, the physical distance between the remote assistance operator and the ADS can have a significant impact on the timing of their communications.[5] Weather, natural disasters, and other factors can harm the reliability, speed, and latency of the network connection between an RAO and a vehicle's ADS. When latency interrupts a zoom call or streaming service, it may frustrate the user. When it slows down an RAO's ability to direct an AV, it could have much more serious consequences. For example, as operators help steer an ADS through difficult scenarios, the visual and audio information the operator receives may already be out of date, rendering any guidance potentially unsafe. In fact, researchers have found that latency as small as 300 milliseconds can reduce driving performance.[6] Yet, AV manufacturers face no minimum latency standards for transmission of driving data from the vehicle to the RAO.[7] Moreover, most RAOs are not required to be located in the same state or even *country* that the driving system operates in; only Florida requires remote operators to be located in the United States.[8] In other words, AV manufacturers may be relying on overseas RAOs — located thousands of miles from the operating domain of their autonomous vehicles — and expecting they can quickly intervene if an AV gets into an uncertain, and potentially dangerous, situation. The safety risks with such an approach are obvious.

---

[3] Even where a company has released data on RAOs, it's unclear if it's accurate. For example, in 2021, an anonymous former Waymo remote operator reportedly stated he had to "disengage" the driving system and intervene around 30 times per day, but Waymo publicly reported only 21 disengagements over more than 600,000 miles driven in 2020. The explanation for this substantial discrepancy is unclear. Hyunjoo Jim, *Insight: A secret weapon for self-driving car startups: Humans,* Reuters (Aug. 23, 2021), https://www.reuters.com/business/autos-transportation/secret-weapon-self-driving-car-startups-humans-2021-08-23/.

[4] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[5] Volico, *Network Latency: Root Causes and Solutions* (Apr. 8, 2025), https://www.volico.com/network-latency-root-causes-and-solutions/.

[6] Stephanie Neumeier et al, *Teleoperation: the holy grail to solve problems of automated driving? Sure, sure but latency matters,* 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (Sept. 2019), https://www.researchgate.net/publication/335941077_Teleoperation_The_Holy_Grail_to_Solve_Problems_of_Automated_Driving_Sure_but_Latency_Matters.

[7] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[8] Id.

Locating remote assistance operations in different states or countries from the operating vehicle creates additional security risks. For example, overseas remote assistance operations may be more susceptible to physical takeover by hostile actors, potentially granting them driver-like control of thousands of vehicles transporting passengers on American roads. Heavy and fast-moving vehicles could quickly become the weapons of foreign actors seeking to harm innocent Americans. Overseas RAOs also creates cybersecurity risks.[9] While any form of remote connectivity introduces cyber risk, locating remote assistance centers overseas significantly amplifies these vulnerabilities. Remote assistance personnel operating outside the United States may be subject to foreign laws and standards rather than U.S. cybersecurity and data-protection requirements. For these reasons, it is critical that autonomous vehicle operators ensure all remote assistance operations are located in the United States.

Many RAOs are also not required to hold a driver's license, raising significant concerns about their qualifications to influence the operation of a motor vehicle.[10] A driver's license is a foundational safety regulation that ensures anyone legally operating a vehicle on public roads has met a minimum standard of competence. Although RAOs are supposedly not tele-driving the vehicle, their responsibilities involve guiding autonomous systems through complex situations that demand substantial knowledge of driving laws, maneuvers, and real-world contexts. Although states such as Florida require these operators to hold a driver's license, other states where AVs are operating do not.[11] As a result, riders in these states, and in any future states with similar gaps in regulation, may find themselves in vehicles influenced by individuals who lack even a basic driver's license.

AV manufacturers are also not subject to any federal standard ensuring that their RAOs are sober while on duty or free from a history of impaired driving. Currently, no federal or state law explicitly requires remote operators to be sober while performing their duties.[12] Without such laws, an intoxicated RAO could provide unsafe guidance or fail to provide timely guidance altogether to a vehicle's ADS. Moreover, if an RAO is intoxicated and an AV is involved in a crash, questions of liability and accountability remain unresolved — an outcome that further undermines public safety.[13] Manufacturers frequently tout eliminating drunk driving as a key benefit of autonomous driving, yet they offer no assurances that their own remote assistance operators are held to any standards regarding past or current alcohol use while driving or providing remote assistance.

---

[9] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024) (to be codified at 15 C.F.R Part 7).

[10] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[11] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[12] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[13] Jesse L. Keeffe, Designated Driver-Less Cars? *Why Current Georgia Law Supports Liability for Intoxicated Drivers of Autonomous Vehicles*, 57 Ga. L. Rev. 1387-1412 (2023).

Finally, remote assistance raises serious privacy concerns. Conventional vehicles already collect vast amounts of sensitive personal information about drivers and passengers, which manufacturers often leverage for financial gain.[14] With numerous cameras and other sensors installed to enable an ADS to operate, AVs significantly enhance these privacy risks. RAOs further increase these risks by requiring the transfer of continuous video, sensor, and audio feeds — potentially capturing interior views, the vehicle's surroundings, and communications with passengers or nearby road users — from the AV to an RAO. Transmitting and processing these feeds introduces additional questions about data collection, retention, access controls, and passenger knowledge when an RAO is engaged. The public deserves clear, transparent answers about how these data are used, how long they are stored, who has access to them, and whether they are ever shared with outside organizations for any purpose.

Given the increasing deployment of driverless vehicles on U.S. roads, the public deserves a detailed overview of Zoox's remote-assistance operations, policies, metrics, and safeguards. Accordingly, I ask that you provide the following written information by February 17, 2026:

1. A complete description of Zoox's remote assistance operations, including:

    a) The roles and responsibilities of the remote assistance operator, such as whether the operator is limited to providing advice or instruction or is permitted to change's the vehicles trajectory or driving path;

    b) Whether your company ever allows RAOs to tele-drive a vehicle, beyond providing guidance to the AV;

    c) The frequency with which remote assistance sessions are invoked (for example, number of sessions per vehicle-mile or per trip), and the proportion of sessions that result in human input that alters the vehicle's driving plan;

    d) The number and location (city/state/country) of remote assistance centers or teams and number of RAOs at each location;

    e) Whether any remote assistance operators are located outside the United States, and if so, the countries and jurisdictions involved, and how your company conducts oversight, supervision and qualification of such overseas operators;

    f) The average and worst-case latency (broken down by location of each RAO center) between the vehicle and remote assistance operator from the time a request is generated by the vehicle until a human begins interaction and the time from human intervention to vehicle execution of any instruction;

    g) Whether all remote assistance operators are required to obtain and maintain a valid driver's license while serving as an operator;

[14] Press Release, Senator Edward Markey, *Senator Markey Urges FTC to Investigate Invasive Data Privacy Practices of Automakers* (Feb. 28, 2024).

h) The background screening process for remote assistance operator applicants, including past experience with alcohol impaired driving;

i) Procedures and protocols in place to prevent remote assistance operators from being intoxicated while performing their duties as operators;

j) A summary of the cybersecurity architecture protecting the link between vehicle and remote assistance infrastructure, including network encryption protocols, authentication of operators, redundancy and resilience measures, and data retention and access policies; and

k) The procedures by which remote assistance involvement is logged, audited, and reviewed for safety analysis, particularly during crashes or other safety incidents.

2. A detailed description of any recorded crash or disengagement event (or near-miss) in which remote assistance played a causal or contributory role, whether through advice, instruction, or operator override. For each event, please provide the date, location, description of remote assistance involvement, outcome (damages and injuries, if any), lessons learned, and remedial actions taken.

3. A description of your company's training, qualification, and monitoring practices for remote assistance operators, including how performance is measured, what credentials and oversight apply, how many hours RAOs work per shift, and how your company manages fatigue, distraction, and user-error for remote operators.

4. A copy of any internal policies or standards by which remote assistance operations are governed, such as remote assistance operator to vehicle ratios, escalation procedures, boundaries for remote operator intervention (such as speed limits, zones, vehicle states), and fallback planning when the remote connection fails or is degraded.

Thank you in advance for your cooperation and timely attention to this request. I look forward to your response.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

WASHINGTON, DC 20510

February 3, 2026

Mr. Chris Urmson
Chief Executive Officer and Chairman
Aurora Innovation, Inc.
1654 Smallman Street
Pittsburgh, Pennsylvania

Dear Mr. Urmson,

As automakers deploy autonomous vehicles (AVs) on public roads, the industry's practices around remote assistance operators (RAOs) — the individuals who intervene when an AV finds itself in an uncertain situation — are becoming increasingly important. Yet, AV companies, including Aurora, have provided little public information about their policies around RAOs — including if they are located in the United States. Without proper safeguards, the AV industry's reliance on RAOs could create serious safety, national security, and privacy risks. As Aurora continues to expand its operations, Congress and the public deserve assurance that its remote assistance operations will not endanger passengers, other road and vulnerable road users, or national security.

Despite the limited public knowledge about RAOs, every AV manufacturer and operator relies on them to help their autonomous driving systems (ADS) — the technology that operates the vehicle autonomously — drive safely. Although the exact role and performance for RAOs vary by manufacturer, RAOs intervene when an AV confronts a driving condition or situation in which the system either cannot or is unsure how to proceed. Notably, RAOs do not directly control the steering, braking, or acceleration of the vehicle. Instead, they provide guidance, approvals, or clarifications for how the ADS should handle a situation or road condition.[1] In practice, however, the difference between directly operating a vehicle and issuing specific directives to the ADS can be difficult to discern. RAOs are similar to aircraft dispatchers — a regulated profession — who, in joint agreement with the airline captain, decide flight planning, route and altitude selection, and aircraft legal compliance during flights and carry out these duties from a remote location.[2] In essence, RAOs are intended to serve as a critical backup, keeping the public safe when an AV cannot determine the correct driving decision. Information about these RAOs is therefore critical to understanding their potential safety and security risks.

Unfortunately, manufacturers have not disclosed several key details about their remote operations procedures. For example, except as required under a few state laws, AV companies have provided little information about how often an RAO must intervene and provide guidance

[1] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[2] Aircraft dispatchers, 14 C.F.R. Part 65, Subpart C.

to a vehicle or whether an RAO can take over full control of the vehicle and tele-drive.[3] Moreover, many manufacturers have not disclosed the number of RAOs that they employ, the location of these RAOs, and the number of AVs that a single RAO is responsible for at any given time. Companies have also provided little information about their fallback procedures if an RAO is unable to communicate with a vehicle's ADS. Although the AV industry trade association published a document on RAOs, it offers limited information on these issues, including failing to identify safety risks that remote assistance could introduce.[4] Given the growth in the AV industry, this information gap is unacceptable.

The location of RAOs is especially important for vehicle safety. As with all networks, the physical distance between the remote assistance operator and the ADS can have a significant impact on the timing of their communications.[5] Weather, natural disasters, and other factors can harm the reliability, speed, and latency of the network connection between an RAO and a vehicle's ADS. When latency interrupts a zoom call or streaming service, it may frustrate the user. When it slows down an RAO's ability to direct an AV, it could have much more serious consequences. For example, as operators help steer an ADS through difficult scenarios, the visual and audio information the operator receives may already be out of date, rendering any guidance potentially unsafe. In fact, researchers have found that latency as small as 300 milliseconds can reduce driving performance.[6] Yet, AV manufacturers face no minimum latency standards for transmission of driving data from the vehicle to the RAO.[7] Moreover, most RAOs are not required to be located in the same state or even *country* that the driving system operates in; only Florida requires remote operators to be located in the United States.[8] In other words, AV manufacturers may be relying on overseas RAOs — located thousands of miles from the operating domain of their autonomous vehicles — and expecting they can quickly intervene if an AV gets into an uncertain, and potentially dangerous, situation. The safety risks with such an approach are obvious.

---

[3] Even where a company has released data on RAOs, it's unclear if it's accurate. For example, in 2021, an anonymous former Waymo remote operator reportedly stated he had to "disengage" the driving system and intervene around 30 times per day, but Waymo publicly reported only 21 disengagements over more than 600,000 miles driven in 2020. The explanation for this substantial discrepancy is unclear. Hyunjoo Jim, *Insight: A secret weapon for self-driving car startups: Humans,* Reuters (Aug. 23, 2021), https://www.reuters.com/business/autos-transportation/secret-weapon-self-driving-car-startups-humans-2021-08-23/.

[4] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[5] Volico, *Network Latency: Root Causes and Solutions* (Apr. 8, 2025), https://www.volico.com/network-latency-root-causes-and-solutions/.

[6] Stephanie Neumeier et al, *Teleoperation: the holy grail to solve problems of automated driving? Sure, sure but latency matters,* 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (Sept. 2019), https://www.researchgate.net/publication/335941077_Teleoperation_The_Holy_Grail_to_Solve_Problems_of_Automated_Driving_Sure_but_Latency_Matters.

[7] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[8] Id.

Locating remote assistance operations in different states or countries from the operating vehicle creates additional security risks. For example, overseas remote assistance operations may be more susceptible to physical takeover by hostile actors, potentially granting them driver-like control of thousands of vehicles transporting passengers on American roads. Heavy and fast-moving vehicles could quickly become the weapons of foreign actors seeking to harm innocent Americans. Overseas RAOs also creates cybersecurity risks.[9] While any form of remote connectivity introduces cyber risk, locating remote assistance centers overseas significantly amplifies these vulnerabilities. Remote assistance personnel operating outside the United States may be subject to foreign laws and standards rather than U.S. cybersecurity and data-protection requirements. For these reasons, it is critical that autonomous vehicle operators ensure all remote assistance operations are located in the United States.

Many RAOs are also not required to hold a driver's license, raising significant concerns about their qualifications to influence the operation of a motor vehicle.[10] A driver's license is a foundational safety regulation that ensures anyone legally operating a vehicle on public roads has met a minimum standard of competence. Although RAOs are supposedly not tele-driving the vehicle, their responsibilities involve guiding autonomous systems through complex situations that demand substantial knowledge of driving laws, maneuvers, and real-world contexts. Although states such as Florida require these operators to hold a driver's license, other states where AVs are operating do not.[11] As a result, riders in these states, and in any future states with similar gaps in regulation, may find themselves in vehicles influenced by individuals who lack even a basic driver's license.

AV manufacturers are also not subject to any federal standard ensuring that their RAOs are sober while on duty or free from a history of impaired driving. Currently, no federal or state law explicitly requires remote operators to be sober while performing their duties.[12] Without such laws, an intoxicated RAO could provide unsafe guidance or fail to provide timely guidance altogether to a vehicle's ADS. Moreover, if an RAO is intoxicated and an AV is involved in a crash, questions of liability and accountability remain unresolved — an outcome that further undermines public safety.[13] Manufacturers frequently tout eliminating drunk driving as a key benefit of autonomous driving, yet they offer no assurances that their own remote assistance operators are held to any standards regarding past or current alcohol use while driving or providing remote assistance.

---

[9] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024) (to be codified at 15 C.F.R Part 7).

[10] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[11] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[12] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[13] Jesse L. Keeffe, Designated Driver-Less Cars? *Why Current Georgia Law Supports Liability for Intoxicated Drivers of Autonomous Vehicles*, 57 Ga. L. Rev. 1387-1412 (2023).

Finally, remote assistance raises serious privacy concerns. Conventional vehicles already collect vast amounts of sensitive personal information about drivers and passengers, which manufacturers often leverage for financial gain.[14] With numerous cameras and other sensors installed to enable an ADS to operate, AVs significantly enhance these privacy risks. RAOs further increase these risks by requiring the transfer of continuous video, sensor, and audio feeds — potentially capturing interior views, the vehicle's surroundings, and communications with passengers or nearby road users — from the AV to an RAO. Transmitting and processing these feeds introduces additional questions about data collection, retention, access controls, and passenger knowledge when an RAO is engaged. The public deserves clear, transparent answers about how these data are used, how long they are stored, who has access to them, and whether they are ever shared with outside organizations for any purpose.

Given the increasing deployment of driverless vehicles on U.S. roads, the public deserves a detailed overview of Aurora's remote-assistance operations, policies, metrics, and safeguards. Accordingly, I ask that you provide the following written information by February 17, 2026:

1. A complete description of Aurora's remote assistance operations, including:

    a) The roles and responsibilities of the remote assistance operator, such as whether the operator is limited to providing advice or instruction or is permitted to change's the vehicles trajectory or driving path;

    b) Whether your company ever allows RAOs to tele-drive a vehicle, beyond providing guidance to the AV;

    c) The frequency with which remote assistance sessions are invoked (for example, number of sessions per vehicle-mile or per trip), and the proportion of sessions that result in human input that alters the vehicle's driving plan;

    d) The number and location (city/state/country) of remote assistance centers or teams and number of RAOs at each location;

    e) Whether any remote assistance operators are located outside the United States, and if so, the countries and jurisdictions involved, and how your company conducts oversight, supervision and qualification of such overseas operators;

    f) The average and worst-case latency (broken down by location of each RAO center) between the vehicle and remote assistance operator from the time a request is generated by the vehicle until a human begins interaction and the time from human intervention to vehicle execution of any instruction;

    g) Whether all remote assistance operators are required to obtain and maintain a valid driver's license while serving as an operator;

[14] Press Release, Senator Edward Markey, *Senator Markey Urges FTC to Investigate Invasive Data Privacy Practices of Automakers* (Feb. 28, 2024).

h) The background screening process for remote assistance operator applicants, including past experience with alcohol impaired driving;

i) Procedures and protocols in place to prevent remote assistance operators from being intoxicated while performing their duties as operators;

j) A summary of the cybersecurity architecture protecting the link between vehicle and remote assistance infrastructure, including network encryption protocols, authentication of operators, redundancy and resilience measures, and data retention and access policies; and

k) The procedures by which remote assistance involvement is logged, audited, and reviewed for safety analysis, particularly during crashes or other safety incidents.

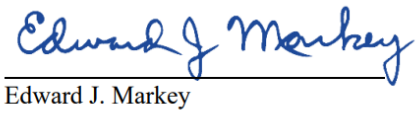
2. A detailed description of any recorded crash or disengagement event (or near-miss) in which remote assistance played a causal or contributory role, whether through advice, instruction, or operator override. For each event, please provide the date, location, description of remote assistance involvement, outcome (damages and injuries, if any), lessons learned, and remedial actions taken.

3. A description of your company's training, qualification, and monitoring practices for remote assistance operators, including how performance is measured, what credentials and oversight apply, how many hours RAOs work per shift, and how your company manages fatigue, distraction, and user-error for remote operators.

4. A copy of any internal policies or standards by which remote assistance operations are governed, such as remote assistance operator to vehicle ratios, escalation procedures, boundaries for remote operator intervention (such as speed limits, zones, vehicle states), and fallback planning when the remote connection fails or is degraded.

Thank you in advance for your cooperation and timely attention to this request. I look forward to your response.

Sincerely,



Edward J. Markey
United States Senator

United States Senate

WASHINGTON, DC 20510

February 3, 2026

Mr. Jiajun Zhu
Dr. Dave Ferguson
Co-Chief Executive Officers
Nuro
1300 Terra Bella Ave, Suite 100
Mountain View, California

Dear Mr. Jiajun and Dr. Ferguson,

As automakers deploy autonomous vehicles (AVs) on public roads, the industry's practices around remote assistance operators (RAOs) — the individuals who intervene when an AV finds itself in an uncertain situation — are becoming increasingly important. Yet, AV companies, including Nuro, have provided little public information about their policies around RAOs — including if they are located in the United States. Without proper safeguards, the AV industry's reliance on RAOs could create serious safety, national security, and privacy risks. As Nuro continues to expand its operations, Congress and the public deserve assurance that its remote assistance operations will not endanger passengers, other road and vulnerable road users, or national security.

Despite the limited public knowledge about RAOs, every AV manufacturer and operator relies on them to help their autonomous driving systems (ADS) — the technology that operates the vehicle autonomously — drive safely. Although the exact role and performance for RAOs vary by manufacturer, RAOs intervene when an AV confronts a driving condition or situation in which the system either cannot or is unsure how to proceed. Notably, RAOs do not directly control the steering, braking, or acceleration of the vehicle. Instead, they provide guidance, approvals, or clarifications for how the ADS should handle a situation or road condition.[1] In practice, however, the difference between directly operating a vehicle and issuing specific directives to the ADS can be difficult to discern. RAOs are similar to aircraft dispatchers — a regulated profession — who, in joint agreement with the airline captain, decide flight planning, route and altitude selection, and aircraft legal compliance during flights and carry out these duties from a remote location.[2] In essence, RAOs are intended to serve as a critical backup, keeping the public safe when an AV cannot determine the correct driving decision. Information about these RAOs is therefore critical to understanding their potential safety and security risks.

Unfortunately, manufacturers have not disclosed several key details about their remote operations procedures. For example, except as required under a few state laws, AV companies

[1] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[2] Aircraft dispatchers, 14 C.F.R. Part 65, Subpart C.

have provided little information about how often an RAO must intervene and provide guidance to a vehicle or whether an RAO can take over full control of the vehicle and tele-drive.[3] Moreover, many manufacturers have not disclosed the number of RAOs that they employ, the location of these RAOs, and the number of AVs that a single RAO is responsible for at any given time. Companies have also provided little information about their fallback procedures if an RAO is unable to communicate with a vehicle's ADS. Although the AV industry trade association published a document on RAOs, it offers limited information on these issues, including failing to identify safety risks that remote assistance could introduce.[4] Given the growth in the AV industry, this information gap is unacceptable.

The location of RAOs is especially important for vehicle safety. As with all networks, the physical distance between the remote assistance operator and the ADS can have a significant impact on the timing of their communications.[5] Weather, natural disasters, and other factors can harm the reliability, speed, and latency of the network connection between an RAO and a vehicle's ADS. When latency interrupts a zoom call or streaming service, it may frustrate the user. When it slows down an RAO's ability to direct an AV, it could have much more serious consequences. For example, as operators help steer an ADS through difficult scenarios, the visual and audio information the operator receives may already be out of date, rendering any guidance potentially unsafe. In fact, researchers have found that latency as small as 300 milliseconds can reduce driving performance.[6] Yet, AV manufacturers face no minimum latency standards for transmission of driving data from the vehicle to the RAO.[7] Moreover, most RAOs are not required to be located in the same state or even *country* that the driving system operates in; only Florida requires remote operators to be located in the United States.[8] In other words, AV manufacturers may be relying on overseas RAOs — located thousands of miles from the operating domain of their autonomous vehicles — and expecting they can quickly intervene if an AV gets into an uncertain, and potentially dangerous, situation. The safety risks with such an approach are obvious.

---

[3] Even where a company has released data on RAOs, it's unclear if it's accurate. For example, in 2021, an anonymous former Waymo remote operator reportedly stated he had to "disengage" the driving system and intervene around 30 times per day, but Waymo publicly reported only 21 disengagements over more than 600,000 miles driven in 2020. The explanation for this substantial discrepancy is unclear. Hyunjoo Jim, *Insight: A secret weapon for self-driving car startups: Humans,* Reuters (Aug. 23, 2021), https://www.reuters.com/business/autos-transportation/secret-weapon-self-driving-car-startups-humans-2021-08-23/.

[4] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[5] Volico, *Network Latency: Root Causes and Solutions* (Apr. 8, 2025), https://www.volico.com/network-latency-root-causes-and-solutions/.

[6] Stephanie Neumeier et al, *Teleoperation: the holy grail to solve problems of automated driving? Sure, sure but latency matters,* 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (Sept. 2019), https://www.researchgate.net/publication/335941077_Teleoperation_The_Holy_Grail_to_Solve_Problems_of_Automated_Driving_Sure_but_Latency_Matters.

[7] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[8] Id.

Locating remote assistance operations in different states or countries from the operating vehicle creates additional security risks. For example, overseas remote assistance operations may be more susceptible to physical takeover by hostile actors, potentially granting them driver-like control of thousands of vehicles transporting passengers on American roads. Heavy and fast-moving vehicles could quickly become the weapons of foreign actors seeking to harm innocent Americans. Overseas RAOs also creates cybersecurity risks.[9] While any form of remote connectivity introduces cyber risk, locating remote assistance centers overseas significantly amplifies these vulnerabilities. Remote assistance personnel operating outside the United States may be subject to foreign laws and standards rather than U.S. cybersecurity and data-protection requirements. For these reasons, it is critical that autonomous vehicle operators ensure all remote assistance operations are located in the United States.

Many RAOs are also not required to hold a driver's license, raising significant concerns about their qualifications to influence the operation of a motor vehicle.[10] A driver's license is a foundational safety regulation that ensures anyone legally operating a vehicle on public roads has met a minimum standard of competence. Although RAOs are supposedly not tele-driving the vehicle, their responsibilities involve guiding autonomous systems through complex situations that demand substantial knowledge of driving laws, maneuvers, and real-world contexts. Although states such as Florida require these operators to hold a driver's license, other states where AVs are operating do not.[11] As a result, riders in these states, and in any future states with similar gaps in regulation, may find themselves in vehicles influenced by individuals who lack even a basic driver's license.

AV manufacturers are also not subject to any federal standard ensuring that their RAOs are sober while on duty or free from a history of impaired driving. Currently, no federal or state law explicitly requires remote operators to be sober while performing their duties.[12] Without such laws, an intoxicated RAO could provide unsafe guidance or fail to provide timely guidance altogether to a vehicle's ADS. Moreover, if an RAO is intoxicated and an AV is involved in a crash, questions of liability and accountability remain unresolved — an outcome that further undermines public safety.[13] Manufacturers frequently tout eliminating drunk driving as a key benefit of autonomous driving, yet they offer no assurances that their own remote assistance operators are held to any standards regarding past or current alcohol use while driving or providing remote assistance.

---

[9] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024) (to be codified at 15 C.F.R Part 7).

[10] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[11] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[12] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[13] Jesse L. Keeffe, Designated Driver-Less Cars? *Why Current Georgia Law Supports Liability for Intoxicated Drivers of Autonomous Vehicles*, 57 Ga. L. Rev. 1387-1412 (2023).

Finally, remote assistance raises serious privacy concerns. Conventional vehicles already collect vast amounts of sensitive personal information about drivers and passengers, which manufacturers often leverage for financial gain.[14] With numerous cameras and other sensors installed to enable an ADS to operate, AVs significantly enhance these privacy risks. RAOs further increase these risks by requiring the transfer of continuous video, sensor, and audio feeds — potentially capturing interior views, the vehicle's surroundings, and communications with passengers or nearby road users — from the AV to an RAO. Transmitting and processing these feeds introduces additional questions about data collection, retention, access controls, and passenger knowledge when an RAO is engaged. The public deserves clear, transparent answers about how these data are used, how long they are stored, who has access to them, and whether they are ever shared with outside organizations for any purpose.

Given the increasing deployment of driverless vehicles on U.S. roads, the public deserves a detailed overview of Nuro's remote-assistance operations, policies, metrics, and safeguards. Accordingly, I ask that you provide the following written information by February 17, 2026:

1. A complete description of Nuro's remote assistance operations, including:

    a) The roles and responsibilities of the remote assistance operator, such as whether the operator is limited to providing advice or instruction or is permitted to change's the vehicles trajectory or driving path;

    b) Whether your company ever allows RAOs to tele-drive a vehicle, beyond providing guidance to the AV;

    c) The frequency with which remote assistance sessions are invoked (for example, number of sessions per vehicle-mile or per trip), and the proportion of sessions that result in human input that alters the vehicle's driving plan;

    d) The number and location (city/state/country) of remote assistance centers or teams and number of RAOs at each location;

    e) Whether any remote assistance operators are located outside the United States, and if so, the countries and jurisdictions involved, and how your company conducts oversight, supervision and qualification of such overseas operators;

    f) The average and worst-case latency (broken down by location of each RAO center) between the vehicle and remote assistance operator from the time a request is generated by the vehicle until a human begins interaction and the time from human intervention to vehicle execution of any instruction;

    g) Whether all remote assistance operators are required to obtain and maintain a valid driver's license while serving as an operator;

[14] Press Release, Senator Edward Markey, *Senator Markey Urges FTC to Investigate Invasive Data Privacy Practices of Automakers* (Feb. 28, 2024).

h) The background screening process for remote assistance operator applicants, including past experience with alcohol impaired driving;

i) Procedures and protocols in place to prevent remote assistance operators from being intoxicated while performing their duties as operators;

j) A summary of the cybersecurity architecture protecting the link between vehicle and remote assistance infrastructure, including network encryption protocols, authentication of operators, redundancy and resilience measures, and data retention and access policies; and

k) The procedures by which remote assistance involvement is logged, audited, and reviewed for safety analysis, particularly during crashes or other safety incidents.

2. A detailed description of any recorded crash or disengagement event (or near-miss) in which remote assistance played a causal or contributory role, whether through advice, instruction, or operator override. For each event, please provide the date, location, description of remote assistance involvement, outcome (damages and injuries, if any), lessons learned, and remedial actions taken.

3. A description of your company's training, qualification, and monitoring practices for remote assistance operators, including how performance is measured, what credentials and oversight apply, how many hours RAOs work per shift, and how your company manages fatigue, distraction, and user-error for remote operators.

4. A copy of any internal policies or standards by which remote assistance operations are governed, such as remote assistance operator to vehicle ratios, escalation procedures, boundaries for remote operator intervention (such as speed limits, zones, vehicle states), and fallback planning when the remote connection fails or is degraded.

Thank you in advance for your cooperation and timely attention to this request. I look forward to your response.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

WASHINGTON, DC 20510

February 3, 2026

Ms. Laura Major
President and Chief Executive Officer
Motional
100 Northern Avenue, Suite 200
Boston, Massachusetts

Dear Ms. Major,

As automakers deploy autonomous vehicles (AVs) on public roads, the industry's practices around remote assistance operators (RAOs) — the individuals who intervene when an AV finds itself in an uncertain situation — are becoming increasingly important. Yet, AV companies, including Motional, have provided little public information about their policies around RAOs — including if they are located in the United States. Without proper safeguards, the AV industry's reliance on RAOs could create serious safety, national security, and privacy risks. As Motional continues to expand its operations, Congress and the public deserve assurance that its remote assistance operations will not endanger passengers, other road and vulnerable road users, or national security.

Despite the limited public knowledge about RAOs, every AV manufacturer and operator relies on them to help their autonomous driving systems (ADS) — the technology that operates the vehicle autonomously — drive safely. Although the exact role and performance for RAOs vary by manufacturer, RAOs intervene when an AV confronts a driving condition or situation in which the system either cannot or is unsure how to proceed. Notably, RAOs do not directly control the steering, braking, or acceleration of the vehicle. Instead, they provide guidance, approvals, or clarifications for how the ADS should handle a situation or road condition.[1] In practice, however, the difference between directly operating a vehicle and issuing specific directives to the ADS can be difficult to discern. RAOs are similar to aircraft dispatchers — a regulated profession — who, in joint agreement with the airline captain, decide flight planning, route and altitude selection, and aircraft legal compliance during flights and carry out these duties from a remote location.[2] In essence, RAOs are intended to serve as a critical backup, keeping the public safe when an AV cannot determine the correct driving decision. Information about these RAOs is therefore critical to understanding their potential safety and security risks.

Unfortunately, manufacturers have not disclosed several key details about their remote operations procedures. For example, except as required under a few state laws, AV companies have provided little information about how often an RAO must intervene and provide guidance

[1] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[2] Aircraft dispatchers, 14 C.F.R. Part 65, Subpart C.

to a vehicle or whether an RAO can take over full control of the vehicle and tele-drive.[3] Moreover, many manufacturers have not disclosed the number of RAOs that they employ, the location of these RAOs, and the number of AVs that a single RAO is responsible for at any given time. Companies have also provided little information about their fallback procedures if an RAO is unable to communicate with a vehicle's ADS. Although the AV industry trade association published a document on RAOs, it offers limited information on these issues, including failing to identify safety risks that remote assistance could introduce.[4] Given the growth in the AV industry, this information gap is unacceptable.

The location of RAOs is especially important for vehicle safety. As with all networks, the physical distance between the remote assistance operator and the ADS can have a significant impact on the timing of their communications.[5] Weather, natural disasters, and other factors can harm the reliability, speed, and latency of the network connection between an RAO and a vehicle's ADS. When latency interrupts a zoom call or streaming service, it may frustrate the user. When it slows down an RAO's ability to direct an AV, it could have much more serious consequences. For example, as operators help steer an ADS through difficult scenarios, the visual and audio information the operator receives may already be out of date, rendering any guidance potentially unsafe. In fact, researchers have found that latency as small as 300 milliseconds can reduce driving performance.[6] Yet, AV manufacturers face no minimum latency standards for transmission of driving data from the vehicle to the RAO.[7] Moreover, most RAOs are not required to be located in the same state or even *country* that the driving system operates in; only Florida requires remote operators to be located in the United States.[8] In other words, AV manufacturers may be relying on overseas RAOs — located thousands of miles from the operating domain of their autonomous vehicles — and expecting they can quickly intervene if an AV gets into an uncertain, and potentially dangerous, situation. The safety risks with such an approach are obvious.

---

[3] Even where a company has released data on RAOs, it's unclear if it's accurate. For example, in 2021, an anonymous former Waymo remote operator reportedly stated he had to "disengage" the driving system and intervene around 30 times per day, but Waymo publicly reported only 21 disengagements over more than 600,000 miles driven in 2020. The explanation for this substantial discrepancy is unclear. Hyunjoo Jim, *Insight: A secret weapon for self-driving car startups: Humans,* Reuters (Aug. 23, 2021), https://www.reuters.com/business/autos-transportation/secret-weapon-self-driving-car-startups-humans-2021-08-23/.

[4] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[5] Volico, *Network Latency: Root Causes and Solutions* (Apr. 8, 2025), https://www.volico.com/network-latency-root-causes-and-solutions/.

[6] Stephanie Neumeier et al, *Teleoperation: the holy grail to solve problems of automated driving? Sure, sure but latency matters,* 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (Sept. 2019), https://www.researchgate.net/publication/335941077_Teleoperation_The_Holy_Grail_to_Solve_Problems_of_Automated_Driving_Sure_but_Latency_Matters.

[7] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[8] Id.

Locating remote assistance operations in different states or countries from the operating vehicle creates additional security risks. For example, overseas remote assistance operations may be more susceptible to physical takeover by hostile actors, potentially granting them driver-like control of thousands of vehicles transporting passengers on American roads. Heavy and fast-moving vehicles could quickly become the weapons of foreign actors seeking to harm innocent Americans. Overseas RAOs also creates cybersecurity risks.[9] While any form of remote connectivity introduces cyber risk, locating remote assistance centers overseas significantly amplifies these vulnerabilities. Remote assistance personnel operating outside the United States may be subject to foreign laws and standards rather than U.S. cybersecurity and data-protection requirements. For these reasons, it is critical that autonomous vehicle operators ensure all remote assistance operations are located in the United States.

Many RAOs are also not required to hold a driver's license, raising significant concerns about their qualifications to influence the operation of a motor vehicle.[10] A driver's license is a foundational safety regulation that ensures anyone legally operating a vehicle on public roads has met a minimum standard of competence. Although RAOs are supposedly not tele-driving the vehicle, their responsibilities involve guiding autonomous systems through complex situations that demand substantial knowledge of driving laws, maneuvers, and real-world contexts. Although states such as Florida require these operators to hold a driver's license, other states where AVs are operating do not.[11] As a result, riders in these states, and in any future states with similar gaps in regulation, may find themselves in vehicles influenced by individuals who lack even a basic driver's license.

AV manufacturers are also not subject to any federal standard ensuring that their RAOs are sober while on duty or free from a history of impaired driving. Currently, no federal or state law explicitly requires remote operators to be sober while performing their duties.[12] Without such laws, an intoxicated RAO could provide unsafe guidance or fail to provide timely guidance altogether to a vehicle's ADS. Moreover, if an RAO is intoxicated and an AV is involved in a crash, questions of liability and accountability remain unresolved — an outcome that further undermines public safety.[13] Manufacturers frequently tout eliminating drunk driving as a key benefit of autonomous driving, yet they offer no assurances that their own remote assistance operators are held to any standards regarding past or current alcohol use while driving or providing remote assistance.

---

[9] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024) (to be codified at 15 C.F.R Part 7).

[10] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[11] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[12] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[13] Jesse L. Keeffe, Designated Driver-Less Cars? *Why Current Georgia Law Supports Liability for Intoxicated Drivers of Autonomous Vehicles*, 57 Ga. L. Rev. 1387-1412 (2023).

Finally, remote assistance raises serious privacy concerns. Conventional vehicles already collect vast amounts of sensitive personal information about drivers and passengers, which manufacturers often leverage for financial gain.[14] With numerous cameras and other sensors installed to enable an ADS to operate, AVs significantly enhance these privacy risks. RAOs further increase these risks by requiring the transfer of continuous video, sensor, and audio feeds — potentially capturing interior views, the vehicle's surroundings, and communications with passengers or nearby road users — from the AV to an RAO. Transmitting and processing these feeds introduces additional questions about data collection, retention, access controls, and passenger knowledge when an RAO is engaged. The public deserves clear, transparent answers about how these data are used, how long they are stored, who has access to them, and whether they are ever shared with outside organizations for any purpose.

Given the increasing deployment of driverless vehicles on U.S. roads, the public deserves a detailed overview of Motional's remote-assistance operations, policies, metrics, and safeguards. Accordingly, I ask that you provide the following written information by February 17, 2026:

1. A complete description of Motional's remote assistance operations, including:

    a) The roles and responsibilities of the remote assistance operator, such as whether the operator is limited to providing advice or instruction or is permitted to change's the vehicles trajectory or driving path;

    b) Whether your company ever allows RAOs to tele-drive a vehicle, beyond providing guidance to the AV;

    c) The frequency with which remote assistance sessions are invoked (for example, number of sessions per vehicle-mile or per trip), and the proportion of sessions that result in human input that alters the vehicle's driving plan;

    d) The number and location (city/state/country) of remote assistance centers or teams and number of RAOs at each location;

    e) Whether any remote assistance operators are located outside the United States, and if so, the countries and jurisdictions involved, and how your company conducts oversight, supervision and qualification of such overseas operators;

    f) The average and worst-case latency (broken down by location of each RAO center) between the vehicle and remote assistance operator from the time a request is generated by the vehicle until a human begins interaction and the time from human intervention to vehicle execution of any instruction;

[14] Press Release, Senator Edward Markey, *Senator Markey Urges FTC to Investigate Invasive Data Privacy Practices of Automakers* (Feb. 28, 2024).

g) Whether all remote assistance operators are required to obtain and maintain a valid driver's license while serving as an operator;

h) The background screening process for remote assistance operator applicants, including past experience with alcohol impaired driving;

i) Procedures and protocols in place to prevent remote assistance operators from being intoxicated while performing their duties as operators;

j) A summary of the cybersecurity architecture protecting the link between vehicle and remote assistance infrastructure, including network encryption protocols, authentication of operators, redundancy and resilience measures, and data retention and access policies; and

k) The procedures by which remote assistance involvement is logged, audited, and reviewed for safety analysis, particularly during crashes or other safety incidents.

2. A detailed description of any recorded crash or disengagement event (or near-miss) in which remote assistance played a causal or contributory role, whether through advice, instruction, or operator override. For each event, please provide the date, location, description of remote assistance involvement, outcome (damages and injuries, if any), lessons learned, and remedial actions taken.

3. A description of your company's training, qualification, and monitoring practices for remote assistance operators, including how performance is measured, what credentials and oversight apply, how many hours RAOs work per shift, and how your company manages fatigue, distraction, and user-error for remote operators.

4. A copy of any internal policies or standards by which remote assistance operations are governed, such as remote assistance operator to vehicle ratios, escalation procedures, boundaries for remote operator intervention (such as speed limits, zones, vehicle states), and fallback planning when the remote connection fails or is degraded.

Thank you in advance for your cooperation and timely attention to this request. I look forward to your response.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

WASHINGTON, DC 20510

February 3, 2026

Mr. Edwin Olson
Chief Executive Officer
May Mobility
650 Avis Dr.
Ann Arbor, Michigan

Dear Mr. Olson,

As automakers deploy autonomous vehicles (AVs) on public roads, the industry's practices around remote assistance operators (RAOs) — the individuals who intervene when an AV finds itself in an uncertain situation — are becoming increasingly important. Yet, AV companies, including May Mobility, have provided little public information about their policies around RAOs — including if they are located in the United States. Without proper safeguards, the AV industry's reliance on RAOs could create serious safety, national security, and privacy risks. As May Mobility continues to expand its operations, Congress and the public deserve assurance that its remote assistance operations will not endanger passengers, other road and vulnerable road users, or national security.

Despite the limited public knowledge about RAOs, every AV manufacturer and operator relies on them to help their autonomous driving systems (ADS) — the technology that operates the vehicle autonomously — drive safely. Although the exact role and performance for RAOs vary by manufacturer, RAOs intervene when an AV confronts a driving condition or situation in which the system either cannot or is unsure how to proceed. Notably, RAOs do not directly control the steering, braking, or acceleration of the vehicle. Instead, they provide guidance, approvals, or clarifications for how the ADS should handle a situation or road condition.[1] In practice, however, the difference between directly operating a vehicle and issuing specific directives to the ADS can be difficult to discern. RAOs are similar to aircraft dispatchers — a regulated profession — who, in joint agreement with the airline captain, decide flight planning, route and altitude selection, and aircraft legal compliance during flights and carry out these duties from a remote location.[2] In essence, RAOs are intended to serve as a critical backup, keeping the public safe when an AV cannot determine the correct driving decision. Information about these RAOs is therefore critical to understanding their potential safety and security risks.

Unfortunately, manufacturers have not disclosed several key details about their remote operations procedures. For example, except as required under a few state laws, AV companies have provided little information about how often an RAO must intervene and provide guidance

[1] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[2] Aircraft dispatchers, 14 C.F.R. Part 65, Subpart C.

to a vehicle or whether an RAO can take over full control of the vehicle and tele-drive.[3] Moreover, many manufacturers have not disclosed the number of RAOs that they employ, the location of these RAOs, and the number of AVs that a single RAO is responsible for at any given time. Companies have also provided little information about their fallback procedures if an RAO is unable to communicate with a vehicle's ADS. Although the AV industry trade association published a document on RAOs, it offers limited information on these issues, including failing to identify safety risks that remote assistance could introduce.[4] Given the growth in the AV industry, this information gap is unacceptable.

The location of RAOs is especially important for vehicle safety. As with all networks, the physical distance between the remote assistance operator and the ADS can have a significant impact on the timing of their communications.[5] Weather, natural disasters, and other factors can harm the reliability, speed, and latency of the network connection between an RAO and a vehicle's ADS. When latency interrupts a zoom call or streaming service, it may frustrate the user. When it slows down an RAO's ability to direct an AV, it could have much more serious consequences. For example, as operators help steer an ADS through difficult scenarios, the visual and audio information the operator receives may already be out of date, rendering any guidance potentially unsafe. In fact, researchers have found that latency as small as 300 milliseconds can reduce driving performance.[6] Yet, AV manufacturers face no minimum latency standards for transmission of driving data from the vehicle to the RAO.[7] Moreover, most RAOs are not required to be located in the same state or even *country* that the driving system operates in; only Florida requires remote operators to be located in the United States.[8] In other words, AV manufacturers may be relying on overseas RAOs — located thousands of miles from the operating domain of their autonomous vehicles — and expecting they can quickly intervene if an AV gets into an uncertain, and potentially dangerous, situation. The safety risks with such an approach are obvious.

---

[3] Even where a company has released data on RAOs, it's unclear if it's accurate. For example, in 2021, an anonymous former Waymo remote operator reportedly stated he had to "disengage" the driving system and intervene around 30 times per day, but Waymo publicly reported only 21 disengagements over more than 600,000 miles driven in 2020. The explanation for this substantial discrepancy is unclear. Hyunjoo Jim, *Insight: A secret weapon for self-driving car startups: Humans,* Reuters (Aug. 23, 2021), https://www.reuters.com/business/autos-transportation/secret-weapon-self-driving-car-startups-humans-2021-08-23/.

[4] Automated Vehicle Safety Consortium, *ADS Remote Assistance Use Case,* Society of Automative Engineers (Nov. 28, 2023), https://avsc.sae-itc.com/publication/avsc-04-2023.

[5] Volico, *Network Latency: Root Causes and Solutions* (Apr. 8, 2025), https://www.volico.com/network-latency-root-causes-and-solutions/.

[6] Stephanie Neumeier et al, *Teleoperation: the holy grail to solve problems of automated driving? Sure, sure but latency matters,* 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (Sept. 2019), https://www.researchgate.net/publication/335941077_Teleoperation_The_Holy_Grail_to_Solve_Problems_of_Automated_Driving_Sure_but_Latency_Matters.

[7] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[8] Id.

Locating remote assistance operations in different states or countries from the operating vehicle creates additional security risks. For example, overseas remote assistance operations may be more susceptible to physical takeover by hostile actors, potentially granting them driver-like control of thousands of vehicles transporting passengers on American roads. Heavy and fast-moving vehicles could quickly become the weapons of foreign actors seeking to harm innocent Americans. Overseas RAOs also creates cybersecurity risks.[9] While any form of remote connectivity introduces cyber risk, locating remote assistance centers overseas significantly amplifies these vulnerabilities. Remote assistance personnel operating outside the United States may be subject to foreign laws and standards rather than U.S. cybersecurity and data-protection requirements. For these reasons, it is critical that autonomous vehicle operators ensure all remote assistance operations are located in the United States.

Many RAOs are also not required to hold a driver's license, raising significant concerns about their qualifications to influence the operation of a motor vehicle.[10] A driver's license is a foundational safety regulation that ensures anyone legally operating a vehicle on public roads has met a minimum standard of competence. Although RAOs are supposedly not tele-driving the vehicle, their responsibilities involve guiding autonomous systems through complex situations that demand substantial knowledge of driving laws, maneuvers, and real-world contexts. Although states such as Florida require these operators to hold a driver's license, other states where AVs are operating do not.[11] As a result, riders in these states, and in any future states with similar gaps in regulation, may find themselves in vehicles influenced by individuals who lack even a basic driver's license.

AV manufacturers are also not subject to any federal standard ensuring that their RAOs are sober while on duty or free from a history of impaired driving. Currently, no federal or state law explicitly requires remote operators to be sober while performing their duties.[12] Without such laws, an intoxicated RAO could provide unsafe guidance or fail to provide timely guidance altogether to a vehicle's ADS. Moreover, if an RAO is intoxicated and an AV is involved in a crash, questions of liability and accountability remain unresolved — an outcome that further undermines public safety.[13] Manufacturers frequently tout eliminating drunk driving as a key benefit of autonomous driving, yet they offer no assurances that their own remote assistance operators are held to any standards regarding past or current alcohol use while driving or providing remote assistance.

---

[9] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024) (to be codified at 15 C.F.R Part 7).

[10] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[11] Noah Goodall, *Non-technological challenges for the remote operation of automated vehicles,* Transportation Research Part A Policy and Practice (Dec. 2020), https://www.researchgate.net/publication/346415337_Non-technological_challenges_for_the_remote_operation_of_automated_vehicles.

[12] Lauren Schneider, *Robotaxis: Should we be on board?,* Scienceline (Dec. 11, 2024), https://scienceline.org/2024/12/robotaxiexplainer/.

[13] Jesse L. Keeffe, Designated Driver-Less Cars? *Why Current Georgia Law Supports Liability for Intoxicated Drivers of Autonomous Vehicles*, 57 Ga. L. Rev. 1387-1412 (2023).

Finally, remote assistance raises serious privacy concerns. Conventional vehicles already collect vast amounts of sensitive personal information about drivers and passengers, which manufacturers often leverage for financial gain.[14] With numerous cameras and other sensors installed to enable an ADS to operate, AVs significantly enhance these privacy risks. RAOs further increase these risks by requiring the transfer of continuous video, sensor, and audio feeds — potentially capturing interior views, the vehicle's surroundings, and communications with passengers or nearby road users — from the AV to an RAO. Transmitting and processing these feeds introduces additional questions about data collection, retention, access controls, and passenger knowledge when an RAO is engaged. The public deserves clear, transparent answers about how these data are used, how long they are stored, who has access to them, and whether they are ever shared with outside organizations for any purpose.

Given the increasing deployment of driverless vehicles on U.S. roads, the public deserves a detailed overview of May Mobility's remote-assistance operations, policies, metrics, and safeguards. Accordingly, I ask that you provide the following written information by February 17, 2026:

1. A complete description of May Mobility's remote assistance operations, including:

    a) The roles and responsibilities of the remote assistance operator, such as whether the operator is limited to providing advice or instruction or is permitted to change's the vehicles trajectory or driving path;

    b) Whether your company ever allows RAOs to tele-drive a vehicle, beyond providing guidance to the AV;

    c) The frequency with which remote assistance sessions are invoked (for example, number of sessions per vehicle-mile or per trip), and the proportion of sessions that result in human input that alters the vehicle's driving plan;

    d) The number and location (city/state/country) of remote assistance centers or teams and number of RAOs at each location;

    e) Whether any remote assistance operators are located outside the United States, and if so, the countries and jurisdictions involved, and how your company conducts oversight, supervision and qualification of such overseas operators;

    f) The average and worst-case latency (broken down by location of each RAO center) between the vehicle and remote assistance operator from the time a request is generated by the vehicle until a human begins interaction and the time from human intervention to vehicle execution of any instruction;

[14] Press Release, Senator Edward Markey, *Senator Markey Urges FTC to Investigate Invasive Data Privacy Practices of Automakers* (Feb. 28, 2024).

g) Whether all remote assistance operators are required to obtain and maintain a valid driver's license while serving as an operator;

h) The background screening process for remote assistance operator applicants, including past experience with alcohol impaired driving;

i) Procedures and protocols in place to prevent remote assistance operators from being intoxicated while performing their duties as operators;

j) A summary of the cybersecurity architecture protecting the link between vehicle and remote assistance infrastructure, including network encryption protocols, authentication of operators, redundancy and resilience measures, and data retention and access policies; and

k) The procedures by which remote assistance involvement is logged, audited, and reviewed for safety analysis, particularly during crashes or other safety incidents.

2. A detailed description of any recorded crash or disengagement event (or near-miss) in which remote assistance played a causal or contributory role, whether through advice, instruction, or operator override. For each event, please provide the date, location, description of remote assistance involvement, outcome (damages and injuries, if any), lessons learned, and remedial actions taken.

3. A description of your company's training, qualification, and monitoring practices for remote assistance operators, including how performance is measured, what credentials and oversight apply, how many hours RAOs work per shift, and how your company manages fatigue, distraction, and user-error for remote operators.

4. A copy of any internal policies or standards by which remote assistance operations are governed, such as remote assistance operator to vehicle ratios, escalation procedures, boundaries for remote operator intervention (such as speed limits, zones, vehicle states), and fallback planning when the remote connection fails or is degraded.

Thank you in advance for your cooperation and timely attention to this request. I look forward to your response.

Sincerely,

Edward J. Markey
United States Senator