4th June 2026

To,
Shri Akhilesh Kumar Trivedi
Advisor (Networks, Spectrum and Licensing)
Telecom Regulatory Authority of India (TRAI)
New Delhi.

Subject: Response to the Consultation Paper on the Authorisation for Vehicle-to-Infrastructure (V2I) Communication Service (Consultation Paper No. 08/2026 dated 30 April 2026)

Respected Sir

We write on behalf of The Quantum Hub (TQH), an independent public policy firm based in New Delhi. We work extensively on technology policy issues, including telecommunications regulation, spectrum and licensing policy, data protection and the governance of emerging technologies. We write in response to the Consultation Paper on the introduction of an authorisation for Vehicle-to-Infrastructure (V2I) communication service under Section 3(1)(a) of the Telecommunications Act, 2023.

We thank the Authority for the opportunity to comment, and we welcome the decision to consult at this early, pre-deployment stage. The choices made now, on who may deploy roadside infrastructure, on what terms, and under what interoperability conditions, will shape the cost, reach and safety value of Vehicle-to-Everything (V2X) in India for years to come. We offer the following comments and recommendations on the questions where we have a considered view, namely the need for and design of a V2I authorisation (Question 1) and other suggestions relevant to the framework (Question 3).

A. Need for a V2I authorisation, and its eligibility, validity, service area, scope and conditions (Q1)

1. A V2I authorisation is warranted, but it should be the lightest the framework permits

A V2I authorisation should be introduced under Section 3(1)(a). In our view, an individual authorisation is justified where a service either uses a scarce or coordinated spectrum resource, or raises a genuine public-safety consideration. Where neither is present, lighter registration approaches and even exemptions are more appropriate. V2I engages both grounds. It operates in the reserved 5875–5905 MHz band, which requires coordinated interference management, and its core functions are safety-of-life. An authorisation is therefore warranted.

The question is therefore not whether to authorise V2I, but how heavily. On that question, proportionality points towards the lightest authorisation available. The spectrum is assigned administratively rather than through auction, and safety-critical V2I generates no direct revenue, so there is limited justification for heavy financial conditions even though the case for an authorisation itself holds. Comparable jurisdictions bear this out. The European Union and the United Kingdom operate their V2X frameworks on a class-authorisation basis, under which operators may deploy on pre-set technical conditions without seeking an individual, case-by-case authorisation, and the United States permits both governmental and non-governmental operators to run Cellular-V2X (C-V2X) roadside units under a single set of FCC rules.

2. The vehicle-facing interface is the critical control point, and interoperability and open standards should be built into the authorisation

The principal risk in V2I lies not in who owns the roadside hardware, but in who controls the vehicle-facing interface, that is, the message format and protocol through which every passing vehicle communicates with the infrastructure. That interface tends towards a single dominant standard, and whoever controls it controls the connected-vehicle ecosystem on the network, regardless of how many roadside units exist or who has deployed them. In this specific sense, the interface has the characteristics of a natural monopoly.

The consequences of leaving this undesigned are significant. If roadside units are permitted to operate on proprietary interfaces, a single large operator, whether a dominant concessionaire, an original equipment manufacturer or a technology vendor, may establish a de facto standard and then control access to it. Vehicles would effectively be tied to the infrastructure of whichever operator their manufacturer had contracted with. A vehicle that receives a collision warning on one highway network could fall silent on another. Since the value of safety messaging depends on every vehicle receiving every relevant warning, such fragmentation along commercial lines would represent both a competition failure and a safety failure, which is precisely the outcome an authorisation regime exists to prevent.

There are broadly two ways to address this. The first is to vest the infrastructure entirely in the state, which carries its own costs in terms of deployment, coverage and the pace of innovation. The second, which we recommend, is to build open standards and interoperability into the authorisation itself. In practice, the authorisation should require every roadside unit on a public road to conform to the common interface and message standards notified for Indian deployment, to expose its services to all compliant vehicles on a non-discriminatory basis, and to operate within a national interoperability architecture overseen by a central authority. This approach is consistent with the concerns the Consultation Paper itself raises. The Committee report reproduced at paragraph 3.2 treats the compatibility and interoperability of vehicles and roadside infrastructure as an important consideration in India's choice of technology, and paragraph 2.28 records the ITU's recommendation that harmonisation delivers cross-border continuity, economies of scale in equipment, and improved spectrum management. **Our submission is that these objectives should be secured not only at the level of technology choice, but as binding conditions of the authorisation, so that they hold regardless of who operates the infrastructure.**

Once interoperability is a condition of the authorisation, the question of who operates the roadside units ceases to be a question of control and becomes a question of efficiency, that is, who can deploy and maintain the network most effectively. This is what makes it possible to open non-safety V2I to private participation. The same approach is reflected in comparable jurisdictions. The European Commission's cooperative-ITS architecture, the United States' C-V2X interoperability requirements, and Japan's ITS Spot architecture all proceed on the basis that the infrastructure is open and standards-based, regardless of who operates it.

This approach has been tested in practice. The US Department of Transportation's Connected Vehicle Pilot Deployment Program is governed centrally by the ITS Joint Program Office, with the Federal Highway Administration overseeing delivery while local transport agencies carry out site-level deployment. Its three pilot sites, in Wyoming, New York City and Tampa, were not permitted to proceed in isolation. The programme required them to share lessons and resolve interoperability challenges collectively, with the stated aim that a connected-vehicle device should operate as designed anywhere in the country, regardless of where it was built. The programme's own assessment found that where common standards were followed, devices from different vendors interoperated successfully, and that the cross-site collaboration enabled by central oversight was itself an important driver of that outcome. The lesson is that interoperability is not automatic. It has to be designed in, through common standards

and a coordinating authority, and where it is, a multi-vendor, multi-operator ecosystem becomes workable. **India's Digital Public Infrastructure approach reflects the same principle.**

3. Eligibility: refine the MoRTH proposal rather than apply it as a blanket rule

The Consultation Paper reproduces the MoRTH letter of 20.11.2025 at paragraph 3.13, which proposes restricting RSU authorisation to central and state governments and the agencies they authorise. We submit that this restriction should be refined rather than applied as a blanket rule. Safety-critical services, such as forward collision warning, red-light violation warning and emergency vehicle pre-emption, are safety-of-life functions, and should be deployed by, or under the supervision of, public authorities: NHAI, state road authorities, city traffic bodies, and the agencies they authorise.

Non-safety and value-added services, such as electronic tolling, traffic-flow optimisation, parking management, in-vehicle infotainment and fleet-management data, stand on a different footing, and should additionally be open to private entities, including highway concessionaires, fleet operators, telecom licensees, smart-city special purpose vehicles, original equipment manufacturers and technology companies, subject to interoperability, technical, security and data-protection conditions. The Consultation Paper itself contemplates this: paragraph 4.47 recognises that private entities could be considered for a V2I authorisation, especially for non-safety-related V2X applications.

4. One authorisation with differentiated conditions, not two

A single V2I authorisation that distinguishes internally between safety and non-safety services is the cleanest design. Splitting V2I into two separate telecom-service authorisations would run into Rule 8(5) of the draft Miscellaneous Telecommunication Service Authorisation Rules, which bars an authorised entity from holding more than one authorisation for the same service in the same service area. If safety and non-safety V2I were treated as two services, a highway concessionaire wishing to provide both a collision warning and electronic tolling on the same stretch of road could not lawfully do so. That outcome would duplicate hardware and serve no commercial purpose, since no operator would wish to install two roadside units at each location. A single authorisation with conditions that vary by use case avoids the problem.

The framework already provides for this kind of internal differentiation, through three provisions. First, paragraph 4.35 of the Consultation Paper contemplates a differentiated spectrum-charging framework, and asks whether the entire 30 MHz should be assigned for ITS use or a portion earmarked for safety applications, so differentiation by use case within a single V2I service is already in the Authority's contemplation. Second, Rule 30 of the draft Miscellaneous Telecommunication Service Authorisation Rules allows an entity that provides some, but not all, of the services within its authorisation to seek, and the Central Government to grant, exemptions or relaxations from specified rules, so the conditions attaching to a single authorisation can already be applied differentially according to the services an entity actually provides. Third, Rule 10 of the same Rules confirms that the same service may be authorised on the same or different terms and conditions, which means uniform conditions are not a structural requirement. Section 3(2) of the Telecommunications Act, 2023 provides the enabling statutory basis: it permits the Central Government to set different terms and conditions of authorisation for different types of telecommunication service, network or radio equipment. The provision does not, by its terms, compel intra-service differentiation, but it plainly accommodates it.

5. Validity: a twenty-year term

The V2I authorisation should adopt the same twenty-year term (Rule 6 of the draft Miscellaneous Telecommunication Service Authorisation Rules) and renewal mechanism (Rule 16) that those Rules apply uniformly across the other

sub-categories. Roadside infrastructure requires sustained capital deployment over many years, so a long and predictable term is appropriate, and treating V2I differently would create asymmetries with no supporting policy justification.

6. Service area: national

Rule 5 of the draft Miscellaneous Telecommunication Service Authorisation Rules grants six of the seven Miscellaneous sub-categories, namely Enterprise Communication, M2M, PM-WANI, IFMC, Aeronautical Data Communication and International SIM, on a national service-area basis, with only PMRTS granted on a circle or metro basis. **V2I should follow the national pattern. It is, by design, an interoperable national system.** Vehicles routinely cross state and circle boundaries, and a collision warning that operates in Maharashtra but not in Karnataka would serve little purpose. The Task Force's final report, at recommendation 8.4 (reproduced at paragraph 3.5 of the Consultation Paper), proposes a central authority for inter-state ITS operations and a central platform to ensure inter-state harmonisation and interoperability. Comparable jurisdictions adopt the same approach: the European Union's cooperative-ITS framework is built around cross-border continuity, and the United States operates C-V2X on a federal interoperability baseline rather than state by state. A national service area avoids fragmenting the network along administrative boundaries.

7. Scope: cover both safety and non-safety V2I

Paragraph 2.12 of the Consultation Paper identifies three categories of connected-vehicle application: road safety, traffic efficiency, and others including convenience and infotainment. Confining the authorisation to safety applications alone would exclude the other two categories the Consultation Paper itself identifies, and with them much of the commercial basis that makes large-scale RSU deployment financially viable. Non-safety V2I is well established internationally. The examples below are drawn from live deployments, and they illustrate both the range of value a commercially inclusive framework would unlock and the participation of private operators within publicly-set standards.

> **Electronic tolling.** Japan's ETC 2.0 programme, among the first systems to combine tolling with the capture of vehicle driving data, uses roadside ITS spots to receive GPS, distance and braking data from on-board units, supporting dynamic pricing and national infrastructure planning over the same link that carries safety messaging.
>
> **Cooperative parking.** Germany's C-Roads deployments use roadside units to transmit live bay-availability data to vehicles at urban intersections, with private operators such as Cleverciti integrating on-street sensors. San Francisco's SFpark performs a comparable function, reporting available spaces and adjusting meter pricing dynamically. Similar deployments operate in the Netherlands and Austria under the EU C-ITS framework.
>
> **Fleet management and logistics.** The Connected Vehicle Environment in Columbus, Ohio, a flagship of the city's 2016 USDOT Smart City Challenge award, deployed roadside and on-board units on commercial freight and transit vehicles for real-time telemetry, supporting freight mobility and transit efficiency alongside safety. The infrastructure was supplied by a private contractor, Kapsch TrafficCom, across more than 100 intersections, illustrating private participation in the build-out itself.
>
> **Emissions and traffic-flow optimisation.** The EU's C-ITS work treats roadside infrastructure as a means of reducing vehicle emissions through smoother traffic flow and reduced idling. The scale of that benefit is

visible even in adjacent technology: Pittsburgh's adaptive traffic-signal system, which is a signal-control deployment rather than V2I but which optimises the same traffic flows V2I would, reduced intersection wait times by approximately 40 per cent and emissions by approximately 21 per cent. Operators increasingly run roadside units on solar power, so that the infrastructure itself does not add to emissions.

Emergency-vehicle priority. Norway, Finland and Sweden have deployed roadside C-ITS corridors under the NordicWay project that give priority to emergency vehicles, public transport and freight. In the Czech Republic, the private operator Yunex Traffic has installed C-ITS units on key highways to create faster and safer paths for emergency vehicles.

Taken together, these non-safety and value-added services generate the economic value capable of supporting large-scale RSU deployment, value that a safety-only scope would forgo.

8. Technical and security conditions: calibrate by use case

V2I sits within the Miscellaneous category for the purpose of fees, but that placement does not limit the rigour of the technical and security conditions that may attach to it. We recommend a layered set of conditions. A baseline would apply to all V2I services: interoperability with the C-V2X standards notified under Section 19 of the Telecommunications Act, 2023, equipment certification, interference management, cyber-security obligations, privacy safeguards, auditability, and conformity with the central interoperability architecture. **Heightened conditions would apply only to safety-critical services**: public-key-infrastructure-based message authentication, message-integrity requirements, conformity with the latency and reliability standards that time-critical safety messaging demands, and safety-message certification. These conditions are essential where a spoofed or delayed warning could cause a collision. They would be disproportionate for an infotainment service or a tolling transaction, which already operate under existing data-protection and payments frameworks.

Where a V2I network is considered sufficiently sensitive from a telecom-security perspective, the Government has independent powers under the Telecommunications Act, 2023, including under Section 22, to impose heightened security obligations through the framework for the protection of telecommunication networks. These powers operate separately from the financial conditions of the authorisation.

9. Fees: split clearly between safety and non-safety V2I

For safety-critical services, held by NHAI, state road authorities, city bodies and other public entities, we recommend a nil authorisation fee, nil entry fee, no bank guarantee, no minimum equity or net-worth requirement, and no AGR-linked charge. This is consistent with the treatment of comparable sub-categories in the draft Miscellaneous Telecommunication Service Authorisation Rules. M2M, PM-WANI and International SIM carry no authorisation fee (Rules 59, 63 and 75). IFMC and Aeronautical Data Communication carry an annual authorisation fee of one rupee (Rules 67 and 71). Schedule A prescribes nil entry fees for Enterprise Communication, M2M, PM-WANI, IFMC and International SIM, and nil initial guarantees for M2M, PM-WANI, IFMC, Aeronautical Data Communication and International SIM. Paragraphs 4.55 to 4.57 of the Consultation Paper observe that a similar nominal or nil-fee approach could be appropriate for V2I, given the public-welfare nature of V2X applications.

For non-safety commercial services, held by private operators, the authorisation fee should be nominal, no higher than the one-rupee Aeronautical Data benchmark, with a nil or nominal entry fee, a minimal compliance-linked bank guarantee, and no minimum equity test. Bank guarantees and equity tests serve a financial-discipline purpose, but where the underlying infrastructure is required to be open and interoperable, that discipline is better achieved

through compliance-linked conditions than through up-front capital barriers, which tend to exclude smaller participants.

This light fee structure follows from the basis on which the authorisation is justified. The V2I spectrum is assigned administratively under Entry 6 of the First Schedule of the Telecommunications Act, 2023 rather than through auction, and safety-critical V2I generates no direct revenue, so there is no scarce resource being allocated whose value needs to be recovered through fees. As the Consultation Paper notes at paragraphs 4.51 and 4.52, where the authorisation is held by public entities, entry barriers and equity tests carry limited relevance.

10. Why private participation in non-safety V2I makes sense

We have argued above that V2I should be open and standards-based regardless of who operates it. Within that framework, the case for permitting private participation in non-safety V2I rests on five considerations.

First, interoperability, not state ownership, is the real safeguard. The concern in V2I is control of the interface, not ownership of the hardware. Once open standards are made a condition of the authorisation, the interface is constrained for every operator equally, and permitting private operators to provide non-safety services introduces no new risk that any one of them captures the network. Interoperability performs the function that a state monopoly would otherwise be relied upon to perform, without the corresponding cost to deployment, coverage and innovation. For that reason, eligibility can be opened to private participation only once the open-standards condition is in place. The two are inseparable.

Second, deployment financing. Paragraph 1.2 of the Consultation Paper records the national highway network at approximately 1.46 lakh km, and equipping it and the wider road network with RSUs is a substantial capital undertaking. Paragraph 4.32 identifies the cost of large-scale RSU deployment as a constraint, and paragraph 4.36 notes that V2X deployment in India is yet to commence. Permitting private capital, from concessionaires, fleet operators and others, to fund non-safety RSU deployment reduces the fiscal burden on government and accelerates coverage.

Third, coverage and safety go together. The safety benefit of V2I warning messages depends on RSU density, and a sparse network delivers limited safety value. A deployment model that relies solely on government funding risks producing exactly that outcome. Where private operators are permitted to deploy non-safety RSUs alongside government safety deployments, the two share the same siting, mounting, power and backhaul, which makes it materially faster and less costly for public authorities to extend safety coverage. The two installations remain distinct, but the underlying infrastructure is shared.

Fourth, the FASTag precedent. FASTag began as an interoperable electronic tolling system, built on common standards, with issuer and acquirer participation, plaza operators and centralised settlement. It has since been extended to adjacent use cases including parking, fuel payments, EV charging and congestion tolling. The relevance for V2I is not that FASTag and RSUs are technically equivalent, but that a government-led interoperable infrastructure layer can support a wide range of public and commercial uses once private entities are permitted to build on it within a common standards framework.

Fifth, the wider DPI lesson. India's experience with Digital Public Infrastructure demonstrates the additional public and commercial value that government-built foundations can unlock once private entities are permitted to build on them through open, standardised interfaces. Aadhaar, an identity layer, enabled private innovation in finance, lending and onboarding through open APIs such as eKYC. UPI, a public payments rail,

now underpins a large private payments ecosystem. If V2I's non-safety layer is opened to private participation under a common standard, it can develop along similar lines.

None of this requires a government monopoly, and international practice confirms that eligibility is a genuine policy choice. The United States permits both governmental and other qualifying entities to hold C-V2X RSU authorisations. The European Union has adopted a largely class-authorisation model, under which operators deploy on pre-set conditions rather than individual licences, with member-state administrations retaining a permitting role. Practice is, however, genuinely split. China's deployment is state-led, though delivered in partnership with telecom operators, and South Korea's C-ITS programme is led by its transport ministry, with a Korea C-ITS Industry Council launched on 9 April 2026 to accelerate rollout through industry partnerships. The surveyed practice spans a spectrum from open to government-centred models, and the eligibility question is therefore a genuine policy choice for India to make.

For these reasons, the single V2I authorisation should be open to private entities for non-safety commercial V2I, alongside government and NHAI eligibility for safety-critical V2I, with interoperability and open-standards conditions binding on both.

B. Other suggestions on the V2I authorisation framework (Q3)

1. Use the Section 27 regulatory sandbox to pilot non-safety V2I

The Consultation Paper, the Task Force and the MoRTH letter all envisage that V2I deployment will follow pilot projects, and the Telecommunications Act, 2023 provides a dedicated instrument for this stage. Section 27 empowers the Central Government to create one or more regulatory sandboxes, defined as live testing environments for new products, services and business models, with specified relaxations from the provisions of the Act, and Entry 19 of the First Schedule provides for administrative spectrum assignment for testing, trial, experimental and demonstration purposes, including for regulatory sandboxes.

Both safety-critical and non-safety commercial V2I applications are well suited to being piloted under a Section 27 regulatory sandbox, with public authorities and private entities as appropriate, before full-scale rollout or in parallel with the development of the permanent authorisation framework. A pilot would allow the technical, interference-management and commercial questions to be tested on a limited scale, and would generate the evidence to inform the final V2I authorisation regime.

We thank the Authority for the opportunity to comment, and would be glad to discuss any of the above further.

Warm regards,

Sumeysh Srivastava
Partner
The Quantum Hub (TQH)