

Comments of Zero-Sum ITS Solutions India Pvt. Ltd.

on TRAI Consultation Paper No. 08/2026

[Reference Consolidated Version]

Comments in Q-and-A Form

On: Regulatory Framework for V2X Communication, dated 30.04.2026

Submitted to: Shri Akhilesh Kumar Trivedi, Advisor (Networks, Spectrum and Licensing), Telecom Regulatory Authority of India (advmn@traai.gov.in)

Submitted by: Mr. Mallesh Boggarapu, Director, Zero-Sum ITS Solutions India Pvt. Ltd., No. 254, 1st Floor, 6th Cross Road, Indira Nagar 1st Stage, Stage 1, Indiranagar, Bengaluru, Karnataka 560 038, (mallesh@zero-sum.co.in)

Date: 29 May 2026

Scope of these comments: This consolidated submission addresses Questions Q1(c), Q1(e), Q4, Q5, Q6, Q8(d), Q8(e), Q11, Q12 and Q15 of the Consultation Paper. Other questions raised in Chapter V are not pressed in this submission, and ZSITS does not thereby take any position on them.

1. Executive Summary

Zero-Sum ITS Solutions India Pvt. Ltd. ("ZSITS") is a Co-opted Member of the Department of Telecommunications' Committee on V2X/ITS Policy Formulation (January 2023, Annexure-II to the Consultation Paper) and a participant in ongoing C-V2X field trials in Bengaluru. ZSITS submits these comments in the spirit of constructive engagement with the regulatory process.

The overall positions advanced in these comments may be summarised as follows.

(i) Harmonised technology stack and national interoperability testing (Q4, Q6). LTE-V2X (Release 14) should be adopted as the harmonised access-layer technology across India, with eventual migration to NR-V2X (Release 16) for Day-2 use cases. The ETSI TC ITS stack should be adopted for the upper layers, and a PKI Trust Framework based on ETSI TS 102 941 for the security layer. A National V2X Interoperability Test Facility should be established, hosted by an independent agency such as TEC, ARAI, ICAT, GARC or NATRAX, with testing know-how and procedures developed by C-DAC.

(ii) MTCTE inclusion of OBUs and RSUs, with software update and supply chain transparency requirements (Q1(e), Q5, Q11). OBUs and RSUs should be brought within the MTCTE regime consistently with paragraph 8.8 of Annexure-III. Within the Essential Requirements, (a) secure software update functionality should be expressly required, in a form consistent with AIS 189 and AIS 190, and (b) supply chain transparency requirements (BOM disclosure, country-of-origin disclosure for critical components, and Trusted Source linkage via the National Cyber Security Coordinator and the Trusted Telecom Portal) should be incorporated, as a direct exercise of the power conferred by Section 19(c) of the Telecommunications Act 2023.

(iii) Site management of RSUs (Q1(c), Q8(d), Q8(e)). The service area of the V2I

communication service authorisation should be defined on a site-based approach, linked to a National RSU Registry. A prior-approval mechanism for the establishment of RSUs, analogous to SACFA clearance and administered by the Wireless Planning and Coordination Wing of the Department of Telecommunications, should be put in place. Minimum directionality, inter-RSU protection distance, and maximum antenna height should be prescribed by TEC in the next revision of TEC 31218:2023.

(iv) Pricing of the V2I communication service authorisation (Q12, Q15). Authorisation should be restricted to Central Government, State Governments, and agencies authorised by them (including public-private partnership concessionaires and Smart City Special Purpose Vehicles), consistently with MoRTH letter dated 20.11.2025 (Annexure-IV) and paragraph 3.14(b) of the Consultation Paper. No spectrum charge and no authorisation fee should be levied in respect of safety-related V2X services, consistently with paragraphs 4.30 and 4.34 of the Consultation Paper and with the precedent set by the DoT Machine-to-Machine Service Authorisation (Gazette notification dated 09.09.2025).

(v) Additions to the Day-0 and Day-1 use-case taxonomy (Q11). Three use cases should be added to the C-V2X use-case taxonomy adopted by the MoRTH Task Force on Intelligent Transportation System: §5.2(vi) Emergency Vehicle Approach Notification (V2V) at Day-0; §5.2(vii) Hazardous Location Notifications — Mobile Safety Vehicle (V2V) at Day-0; and §5.3(v) Hazardous Location Notifications — Fixed Roadside (I2V) at Day-1. Each is commercially deployed in Japan (ITS Connect) or Europe (ETSI ITS-G5 / C-Roads), each has been demonstrated by ZSITS in India, and each is consistent with the infrastructure requirements set out for Day-0 and Day-1 in Sections 5.2 and 5.3 of Annexure-III respectively.

2. Responses to Specific Questions

Q1(c) — Service area of the V2I communication service authorisation

ZSITS submits that the service area of the V2I communication service authorisation should be defined by reference to the specific geographic locations at which RSUs are installed (a site-based approach), linked to the registration entries in the National RSU Registry proposed in response to Q8(e) below.

Q1(e) — Technical, operating and security conditions of the V2I communication service authorisation

ZSITS submits that the technical and security conditions should include, as a minimum:

- adoption of the ETSI TC ITS stack (consistently with paragraph 8.5 of Annexure-III);
- PKI-based security services based on ETSI TS 102 941 (consistently with paragraph 8.6 of Annexure-III); and
- inclusion of secure software update functionality within the MTCTE Essential Requirements, in the form proposed in response to Q5 below.

The detailed framing of these conditions is best settled by TEC in the next revision of TEC 31218:2023 and of the MTCTE Essential Requirements, in consultation with DoT HQ / NCCS, Bengaluru, ARAI, and the Controller of Certifying Authorities.

Q4 — Harmonisation of C-V2X

ZSITS supports the adoption of LTE-V2X (Release 14) as the harmonised access-layer technology across India, consistently with the DoT Reference dated 01.12.2025 (Annexure-I to the Consultation Paper). It should be deployed for Day-0 and Day-1 use cases, with eventual migration to NR-V2X (Release 16) for Day-2 use cases, as set out in the harmonised technology stack below.

Harmonised technology stack

Layer	Standard to be adopted	Source
Access layer (PHY/MAC)	3GPP C-V2X PC5 sidelink (LTE-V2X (Release 14); future migration to NR-V2X (Release 16))	DoT Reference 01.12.2025 (Annexure-I); Annexure-III, para. 4.1(i)
Upper layers (Facilities / Network / Transport)	ETSI TC ITS stack	Annexure-III, para. 8.5
Security layer	ETSI TS 102 941 (derived from IEEE 1609.2) PKI Trust Framework	Annexure-III, para. 8.6

Each of the three use cases proposed in response to Q11 (§5.2(vi), §5.2(vii) and §5.3(v)) may be implemented on the basis of LTE-V2X (Release 14). They may each be realised by periodic broadcasting of messages over the PC5 interface, and none requires the URLLC or CPM features of NR-V2X (Release 16). The proposals are accordingly consistent with the technology roadmap envisaged by paragraph 4.1(ii) of Annexure-III, which provides that the roadmap shall ensure backward compatibility across Day 0, Day 1 and Day 2 use cases in order to enable phased adoption, ensure interoperability and preserve the associated value proposition.

National V2X Interoperability Test Facility

ZSITS proposes that a National V2X Interoperability Test Facility be established, as part of the MTCTE certification framework, with the following composition:

(a) Competent authority	An independent agency such as the Telecommunications Engineering Centre (TEC), the Automotive Research Association of India (ARAI), the International Centre for Automotive Technology (ICAT), the Global Automotive Research Centre, India (GARC) or the National Automotive Test Tracks (NATRAX)
(b) Testing agency	Centre for Development of Advanced Computing (C-DAC), responsible for developing the testing know-how and procedures
(c) Scope of testing	Interoperability between OBUs and RSUs supplied by different manufacturers, and interoperability of PKI certificates
(d) Frequency of testing	Initial MTCTE certification of equipment, and re-testing at the time of revisions to the principal standards
(e) International	Provision of opportunities for participation in international

coordination	interoperability events such as 5GAA and ETSI Plug-tests
--------------	--

V2X communication presupposes cross-vendor exchange between OBUs supplied by multiple OEMs and equipment manufacturers, and RSUs operated by multiple authorised entities. As paragraph 3.60 of the Consultation Paper makes clear, the assurance of "inter-operability among different RSUs/ OBUs" is a necessary condition for the V2X system to function. Interoperability of this kind cannot be demonstrated by stand-alone testing of equipment at the point of certification: it can be demonstrated only through testing of equipment from multiple manufacturers in combination.

Paragraph 8.4 of Annexure-III recommends the establishment of "a centralized authority for inter-state operations of ITS/ C-V2X, along with a centralized platform to implement ITS/ C-V2X services, ensuring inter-state harmonization and interoperability." The "centralized platform" referred to in that recommendation is properly understood as covering not only the harmonisation of the operational layer but also the interoperability testing of equipment. A division of responsibility under which the host agency prescribes the testing requirements and grants certification, while C-DAC develops and operates the testing procedures, gives operational effect to that recommendation through an appropriate separation between regulator and implementer.

ZSITS would be pleased to support TEC, ARAI, ICAT, GARC, NATRAX, C-DAC, SIAM and Bharat NCAP in the design and operation of the testing arrangement.

Q5 — Whether OBUs and RSUs should be brought within the MTCTE regime

ZSITS supports the bringing of OBUs and RSUs within the MTCTE regime, consistently with paragraph 8.8 of Annexure-III. Within the Essential Requirements, and specifically within the security requirements referred to at paragraph 3.38(g)(iv) of the Consultation Paper, ZSITS proposes that two distinct sets of requirements be expressly included: (a) software update requirements, and (b) supply chain transparency requirements. Both are advanced by ZSITS as the operational means of giving content to the Essential Requirements.

(a) Software update requirements within the Essential Requirements

Requirement	Content
(i) Secure software update mechanism	Updates are received only from authenticated sources; software integrity is verified before and after each update; and a rollback mechanism is provided.
(ii) Cyber security management	Post-deployment vulnerability monitoring, timely distribution of patches, and an incident response capability are maintained.
(iii) Update history traceability	The current software version and update history of every OBU and RSU are tracked, and the records are retained for not less than ten years.

OBUs and RSUs are deployed inside vehicles and on roadside infrastructure for a service life of the order of ten to twenty years. Over that period, continuous response to the various cyber threats

described at paragraphs 3.48–3.52 of the Consultation Paper (spoofing, replay attack, Sybil attack, message tampering, and the like), tracking of revisions to the relevant 3GPP, ETSI and IEEE standards, and renewal of PKI certificates (paragraphs 3.53–3.55) are all required. None of these can be addressed by one-time certification at the point of manufacture alone, and an effective post-deployment software update mechanism is accordingly indispensable.

The Automotive Research Association of India and the Automotive Industry Standards Committee have formulated AIS 189 (Cyber Security Management System, derived from UN R155) and AIS 190 (Software Update Management System, derived from UN R156). Their implementation schedule is as follows: enforcement for new vehicle types from 1 October 2025, and enforcement for all vehicle types from 1 October 2028. AIS 190 requires original equipment manufacturers to implement secure software update mechanisms, to verify each update before deployment to every electronic control unit, and to maintain version traceability for up to ten years. OBUs equipped with V2X functionality are themselves electronic control units of the vehicle, and fall within the scope of AIS 189 and AIS 190. Embedding a software update requirement in the MTCTE Essential Requirements as proposed above would reduce the operational burden that would otherwise arise from having to satisfy MTCTE certification and AIS 189 / AIS 190 conformity through two separate processes, and would in turn improve the predictability of the regulatory framework from the standpoint of OEMs and equipment manufacturers. RSUs are not within the direct scope of AIS 189 or AIS 190 (since they are not vehicle-mounted devices), but it would be appropriate to impose the equivalent requirements on RSUs through the MTCTE Essential Requirements in order to secure the V2X system as a whole.

Paragraph 8.8 of Annexure-III expressly provides that "The certification of radio equipment (OBU and RSU) may be undertaken by competent authority i.e. TEC, DoT to ensure the C-V2X radios comply with emission limits and essential requirements established by the DOT for wireless emissions, EMI/EMC, communication security, etc. in the harmonized band (5.9 GHz)". The placement of communication security within the Essential Requirements list is thus already supported by the Task Force's recommendation.

(b) Supply chain transparency requirements within the Essential Requirements

Requirement	Content
(i) Disclosure of the Bill of Materials	At the time of application for MTCTE certification of an OBU or an RSU, the Bill of Materials (BOM) is to be filed. The BOM is to include, for each component constituting the product (semiconductors, communication modules, PKI modules, cryptographic modules, and the like), the item designation, the manufacturer, and the country of origin.
(ii) Disclosure of country of origin for critical components	For active components performing safety-critical functions (baseband processor, RF transceiver, PKI module, cryptographic module, GNSS receiver, and the like), the country of origin is to be expressly declared.
(iii) Linkage with the Trusted Source mechanism	Where critical components are sourced from a country sharing a land border with India, the applicant is to make a prior reference to the National Cyber Security Coordinator (NCSC) and to

Requirement	Content
	undergo Trusted Source / Trusted Product assessment through the Trusted Telecom Portal.

The operational flow for the supply chain information disclosed at the time of MTCTE certification is proposed to be as follows: (a) TEC is to share the BOM and the country-of-origin information for critical components, disclosed at the time of MTCTE application, with the NCSC through a secure information-sharing mechanism; (b) the NCSC is to assess that information by reference to the Trusted Source / Trusted Product assessment framework of the National Security Directive on Telecommunication Sector (NSDTS) and the Trusted Telecom Portal, and to provide feedback of the result to TEC; (c) TEC is to determine the grant, conditional grant, or refusal of MTCTE certification on the basis of the feedback received from the NCSC; and (d) the supply chain information disclosed and the assessment results are to be retained by TEC for the full lifecycle of the equipment, and in any event for a period of not less than ten years.

Section 19 of the Telecommunications Act 2023, reproduced in full at paragraph 3.35 of the Consultation Paper, confers on the Central Government the power to notify standards and conformity assessment measures in respect of, inter alia, telecommunication equipment (Section 19(a)), the manufacture, import, distribution and sale of telecommunication equipment (Section 19(c)), telecommunication security (Section 19(d)) and cyber security (Section 19(e)). Section 19(c) in particular constitutes the direct legal basis for the supply chain transparency requirements proposed above. V2X equipment is telecommunication equipment falling within the scope of the regulatory measures including certification and testing referred to at paragraph 8.1 of Annexure-III, and the setting of standards in respect of its manufacture, import, distribution and sale is squarely within the proper exercise of the power conferred by Section 19(c).

The Government of India already operates the following frameworks for the purpose of securing supply chain security in respect of telecommunication equipment: (i) the National Security Directive on Telecommunication Sector (NSDTS), approved by the Cabinet Committee on Security on 16 December 2020 and brought into force on 15 June 2021, which introduces the concepts of "Trusted Source" and "Trusted Product"; (ii) the Trusted Telecom Portal (www.trustedtelecom.gov.in), developed by the Centre for Development of Telematics (C-DOT) and operated by the NCSC, through which Trusted Source / Trusted Product assessment is undertaken; and (iii) Rule 144(xi) of the General Financial Rules 2017, as amended on 23 July 2020 and reinforced by Public Procurement Order No. 4 dated 23 February 2023, which requires a bidder from a country sharing a land border with India to be registered with the Competent Authority and to have obtained the requisite political and security clearances in order to participate in public procurement. V2X equipment (OBUs and RSUs) is telecommunication equipment that ought to be brought within these existing national security frameworks in a coherent manner.

The international regulatory trend in relation to the supply chain transparency of V2X equipment is illustrated by the Final Rule of the United States Department of Commerce, Bureau of Industry and Security (BIS), entitled "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles" (90 Federal Register 5360, published on 16 January 2025 and effective from 17 March 2025). The MTCTE-stage supply chain transparency

requirements proposed by ZSITS share the same direction of regulatory travel as that international trend, while being organised in a form capable of implementation within the existing Indian regulatory framework (the MTCTE regime). It would, in light of the phased implementation approach adopted in the U.S. BIS Final Rule, be appropriate for TEC, in consultation with the relevant agencies, to settle a comparable phased implementation schedule and exemption arrangements appropriate to the supply chain adaptation period of the Indian automotive original equipment manufacturer industry.

The operational detail of both sets of requirements (software update and supply chain transparency) is best settled through consultation between TEC, DoT HQ / NCCS, Bengaluru, ARAI, the NCSC, and the Controller of Certifying Authorities, and reflected in the next revision of TEC 31218:2023 and of the MTCTE Essential Requirements.

Q6 — Standardisation of the upper-layer ITS stack to secure interoperability among different RSUs / OBUs

ZSITS supports the adoption of the ETSI TC ITS stack, consistently with paragraph 8.5 of Annexure-III, and the adoption of a PKI Trust Framework based on ETSI TS 102 941 for the security layer, consistently with paragraph 8.6 of Annexure-III. The harmonised stack proposed in response to Q4 above (in particular the table headed "Harmonised technology stack") gives effect to that position.

The MoRTH Task Force, at paragraph 8.5 of Annexure-III, expressly recommends that "ETSI TC ITS stack may be adopted for V2X/ITS implementation in the country." Paragraph 3.47 of the Consultation Paper identifies two possible upper-layer options — the ETSI stack (Europe) and the IEEE WAVE / SAE stack (United States) — and the recommendation in Annexure-III is in favour of the ETSI stack. The ETSI stack has a track record of supporting cross-border deployment in Europe through initiatives such as C-Roads, and the interoperability of equipment from multiple manufacturers has been continuously verified at international events including the 5GAA Plug-tests. Consistently with the position taken in response to Q1(e) above (on security and software update), ZSITS supports the adoption of the ETSI TC ITS stack.

Each of the three use cases proposed in response to Q11 may be implemented on the basis of the existing message specifications of the ETSI ITS stack, and may accordingly be deployed in a manner interoperable with the European ITS-G5 Roadworks Warning and Hazardous Location Notification services.

The National V2X Interoperability Test Facility proposed in response to Q4 above is the operational means by which compliance with the ETSI TC ITS stack across multiple manufacturers will in fact be assured.

Q8(d) — Whether a minimum directionality of RSUs, a protection distance between RSUs, or a maximum antenna height should be prescribed

ZSITS supports the prescription of a minimum directionality for RSUs, of a protection distance between RSUs, and of a maximum antenna height. The specific values are best settled by the Telecommunications Engineering Centre at the time of the next revision to TEC 31218:2023, in consultation with the relevant agencies.

Q8(e) — Whether a mechanism for obtaining prior approval (analogous to SACFA clearance) for the establishment of RSUs should be mandated

ZSITS supports the establishment of a prior-approval mechanism for the establishment of RSUs, analogous to SACFA clearance, in the following terms:

Prior-approval mechanism for the establishment of RSUs

(a) Competent authority	Wireless Planning and Coordination Wing (WPC), Department of Telecommunications
(b) Matters subject to review	Installation location of the RSU, antenna height, beam direction, radiated power, and the protection distance from neighbouring RSUs
(c) Inter-agency consultation	Coordination with MoRTH, NHAI, State Public Works Departments, and (where relevant) the Directorate General of Civil Aviation and the Railway authorities
(d) Processing timeline	A standard processing period to be prescribed, so as to provide predictability to authorised entities

The detailed technical parameters (antenna height, radiated power, protection distance, and the like) are best settled by the Telecommunications Engineering Centre at the time of the next revision to TEC 31218:2023, in consultation with the relevant agencies.

National RSU Registry

ZSITS further proposes the establishment of a National RSU Registry, in the following terms:

(a) Maintaining authority	An agency to be designated by the Department of Telecommunications (such as the Telecommunications Engineering Centre)
(b) Information recorded	Installation location, operator (authorised entity), operating channel, date of approval, and operational status of each RSU
(c) Linkage with road-occupation permitting	Upon grant of a road-occupation permit by MoRTH, NHAI or a State Public Works Department, automatic registration in the Registry to be required
(d) Access control	Access to be restricted to authorised entities and to the relevant regulatory authorities; the Registry not to be made public

The DoT Reference dated 01.12.2025 (Annexure-I to the Consultation Paper) expressly contemplates that "authorization may be required for Roadside Units (RSUs) to ensure coordinated deployment and effective interference management". Paragraph 3.14(b) of the Consultation Paper reaffirms that position. To give effect to the twin objectives of coordinated deployment and effective interference management, it is necessary to have a central means of identifying the installation location and the operator of every RSU, and of subjecting proposed installations to prior review.

SACFA is an existing inter-ministerial body whose function is the review of the physical siting of radio stations and transmission towers. It performs the following functions, each of which is directly applicable to the regulation of V2X RSUs: (a) review of the physical installation location of radio stations; (b) coordination with relevant ministries (aviation, defence, meteorology and the like); and (c) assessment of interference with existing radio services. Rather than constructing an entirely new mechanism, it is operationally preferable to model the RSU prior-approval mechanism on the established practice of SACFA. This is in our submission both the most rapid path to implementation and the one that offers the greatest operational stability.

Paragraph 8.4 of Annexure-III recommends the establishment of "a centralized authority for inter-state operations of ITS/ C-V2X, along with a centralized platform to implement ITS/ C-V2X services, ensuring inter-state harmonization and interoperability". An established international precedent for that recommendation is the C-Roads Platform of the European Union, which functions as a joint initiative of Member States and road operators and which secures the harmonisation and interoperability of RSU deployments across the European Union. The National RSU Registry proposed above is intended to perform an analogous function in the Indian setting, addressing coordination between Central and State Governments and between governmental and government-authorized entities operating across multiple jurisdictions.

Q11 — Other relevant issues

ZSITS submits two matters in response to Q11.

(a) Reflection of proposals in the next revision of TEC 31218:2023

The framework proposed in response to Q4 above (harmonised technology stack and National V2X Interoperability Test Facility), the requirements proposed in response to Q5 above (software update and supply chain transparency), and the framework proposed in response to Q8(e) above (prior-approval mechanism and National RSU Registry) should each be expressly reflected in the next revision of TEC 31218:2023 and, in the case of the MTCTE requirements, in the corresponding revision of the MTCTE Essential Requirements. ZSITS would be pleased to support TEC, DoT HQ / NCCS, Bengaluru, ARAI, the NCSC, the Centre for Development of Advanced Computing and the Controller of Certifying Authorities in the formulation and validation of those requirements.

(b) Proposed additions to the Day-0 and Day-1 use-case taxonomy

ZSITS supports the framework set out in Chapter 5 of Annexure-III to the Consultation Paper, which prioritises C-V2X use cases for India. The categorisation into Day-0, Day-1 and Day-2 stages represents a reasonable roadmap calibrated to India's infrastructure readiness and road-safety challenges. ZSITS proposes three specific additions to that taxonomy:

- §5.2(vi) Emergency Vehicle Approach Notification (V2V) — addition to Day-0: a V2V service by which emergency vehicles (ambulances, fire trucks and the like) broadcast their position to surrounding general traffic, enabling drivers to take timely evacuation action.
- §5.2(vii) Hazardous Location Notifications — Mobile Safety Vehicle (V2V) — addition to Day-0: a V2V service by which information concerning roadworks, accidents, road debris and similar hazards is broadcast directly to approaching vehicles from a roadworks safety vehicle equipped with a movable Variable Message Sign (VMS).

- §5.3(v) Hazardous Location Notifications — Fixed Roadside (I2V) — addition to Day-1: an I2V service by which the same hazard information is broadcast to approaching vehicles from a fixed roadside installation comprising a V2X road-side unit and an LED/VMS display.

Each of these three additions (i) is commercially deployed in either Japan (ITS Connect) or Europe (ETSI ITS-G5 / C-Roads), (ii) has been demonstrated by ZSITS in India, and (iii) is consistent with the infrastructure requirements set out for Day-0 and Day-1 in Sections 5.2 and 5.3 of Annexure-III respectively.

In particular, ZSITS proposes that the hazardous-location notification service be introduced in two stages: the mobile-safety-vehicle form (V2V) at Day-0, and the fixed-roadside form (I2V) at Day-1. This sequencing reflects the fact that the former requires only the installation of a communication unit on the safety vehicle itself and entails no fixed infrastructure, whereas the latter requires the installation of fixed road-side units. Both forms may be implemented using the same message specification, and together they constitute a coherent staged migration from Day-0 to Day-1.

Proposed Use Cases — summary

Proposal	Stage	Use Case	Mode	Infrastructure Dependencies	Global Precedent / ZSITS Demonstration
§5.2(vi)	Day-0	Emergency Vehicle Approach Notification	V2V	OBU on emergency and general vehicles only; no roadside infrastructure required	Japan: ITS Connect "Emergency Vehicle Presence Notification" (Toyota, commercialised 2015). Europe: "Emergency Vehicle Approaching" service based on the ETSI ITS stack (C-Roads catalogue, commercially deployed). ZSITS: Emergency Vehicle Priority trials completed at Ahmedabad, Thiruvananthapuram, Gurgaon and Bengaluru (in collaboration with Tata Motors and Maruti Suzuki).
§5.2(vii)	Day-0	Hazardous Location Notifications — Mobile Safety Vehicle	V2V	V2X communication unit on the mobile-VMS-equipped roadworks safety vehicle only; no fixed roadside	Europe: ASFINAG (Austria) operates a Roadworks Warning service based on roadworks safety trailers. Similar deployments of communication-equipped roadworks safety trailers are progressing in Germany along the URSA

Proposal	Stage	Use Case	Mode	Infrastructure Dependencies	Global Precedent / ZSITS Demonstration
				infrastructure required	MAJOR corridor. ZSITS: Roadworks information trial completed on the Nelamangala–Devihalli Expressway (FY2025-26, in collaboration with Cube Highways, Maruti Suzuki and Nagoya Electric), using a mobile-VMS-equipped vehicle configuration.
§5.3(v)	Day-1	Hazardous Location Notifications — Fixed Roadside	I2V	Fixed roadside installation (V2X RSU + LED/VMS display); no uplink to the traffic management centre required	Europe: ASFINAG (Austria) Roadworks Warning and Hazardous Location Notification services. As at the end of 2024, 471 fixed road-side units had been installed, with a further 54 in 2025 and a final deployment of 525 units. The service has been operational on the Austrian section of the Rotterdam–Vienna C-ITS Corridor since 2023.

These proposals do not displace the use case already listed at Section 5.4(ii) of Annexure-III as a Day-2 item, namely Hazardous Location Notifications dependent on "I2N-V2N + environmental sensors". That Day-2 item is an advanced form integrated with the traffic management centre and environmental sensors. The Day-0 §5.2(vii) and Day-1 §5.3(v) proposals advanced in these comments are, by contrast, simplified forms operating without any uplink to a traffic management centre, and are proposed as separate use cases. The three may co-exist as a staged roadmap: mobile-safety-vehicle form (Day-0) → fixed-roadside form (Day-1) → traffic-management-centre-integrated form (Day-2). Equally, Section 5.3(ii) of Annexure-III ("Traffic Signal Priority for Emergency Vehicles", with dependencies recorded as I2N-V2N / V2I + traffic management) is preserved as a Day-1 use case requiring integration with traffic signal controllers. The Day-0 §5.2(vi) proposal advanced in these comments is a separate, simplified V2V-only form that does not involve any traffic signal control, and the two use cases are functionally independent.

Rationale — consistency with Day-0 / Day-1 infrastructure thresholds

Section 5.2 of Annexure-III defines Day-0 use cases as "focus[ing] on applications that require minimal infrastructure and can be deployed quickly to address India's urgent road safety needs. They rely primarily on the basic functionality of V2X systems in vehicles." Section 5.3 in turn defines Day-1 use cases as ones that "require moderate infrastructure investments and more

advanced communication capabilities."

The proposed §5.2(vi) (Emergency Vehicle Approach Notification, V2V) is constituted solely by OBUs on emergency vehicles and general vehicles, and requires no roadside infrastructure whatsoever. The infrastructure profile is identical to that of EEBL, FCW and Hit-from-Behind Warning, which are already listed as Day-0 use cases in Section 5.2, and the proposal is therefore fully consistent with the Day-0 requirement. The proposed §5.2(vii) (Hazardous Location Notifications — Mobile Safety Vehicle, V2V) is constituted solely by the installation of a V2X communication unit on a mobile-VMS-equipped roadworks safety vehicle, and likewise requires no fixed roadside infrastructure. The infrastructure profile is again equivalent to that of EEBL or FCW, and the form is particularly suited to situations of high urgency in which the hazard position is itself moving (progressive roadworks, sudden appearance of road debris and the like). Because installation of a communication unit on such a vehicle may proceed independently of the rollout of any fixed infrastructure, classification at Day-0 is appropriate. The proposed §5.3(v) (Hazardous Location Notifications — Fixed Roadside, I2V) does require the installation of fixed roadside equipment and accordingly exceeds the strict Day-0 infrastructure threshold. It does not, however, require any uplink to a traffic management centre or to an upper-layer network (I2N-V2N), and is in that respect plainly distinct from the Day-2 use case at Section 5.4(ii). Its level of required infrastructure investment is comparable to that of the existing Day-1 items at Section 5.3(i) (Queue Warning — Traffic Monitoring system) and 5.3(iii) (Cooperative Collision Avoidance), and classification at Day-1 is therefore appropriate.

Rationale — global commercial deployment

Japan — ITS Connect Emergency Vehicle Presence Notification. In Japan, the ITS Connect Promotion Consortium led by Toyota Motor Corporation has, since 2015, commercially deployed V2V and V2I communication services based on ARIB STD-T109 (operating in the 760 MHz band). Among the services in this suite is the "Emergency Vehicle Presence Notification", which is implemented as a V2V service. Field verification undertaken by the Fire and Disaster Management Agency of the Ministry of Internal Affairs and Communications, conducted in Nagoya City and Toyota City, demonstrated that an ITS-Connect-equipped ambulance traversing the 16 intersections of a principal arterial corridor achieved an average reduction of 7.7 per cent in emergency-driving time (Source: Toyota Motor Corporation website, https://www.toyota.co.jp/its/its_connect/). Further, a user survey reported in the same source records that approximately 90 per cent of ITS Connect users responded that the Emergency Vehicle Presence Notification made it easier for them to take evacuation action.

Europe — Roadworks Warning and Hazardous Location Notifications under ETSI ITS-G5 (the ASFINAG case). In Europe, Roadworks Warning (RWW) and Hazardous Location Notifications (HLN) have been commercially deployed under the ITS-G5 standards developed by ETSI TC ITS and the service profiles defined by the C-Roads Platform. ASFINAG, the operator of the Austrian motorway network, is among the most advanced deploying entities in Europe, and has implemented the service in two forms. Deployment by mobile safety vehicles (relevant to §5.2(vii)): ASFINAG operates a form of Roadworks Warning in which V2X communication units are installed on safety vehicles or trailers deployed at roadworks sites. This implementation was developed under the ECo-AT project and the successor Austrian national activity within the C-Roads Platform. A joint demonstration was held at Teesdorf, near Vienna, on 24 April 2019,

involving ASFINAG, Volkswagen, ANDATA, Swarco Futurit and others, and the service has since moved into operational deployment. ASFINAG's published materials indicate that 10–15 per cent of roadworks trailers on its motorway network are damaged or destroyed each year, which has been the principal motivation for this service. Deployment by fixed road-side units (relevant to §5.3(v)): In addition to the mobile-safety-vehicle form, ASFINAG had installed 471 fixed road-side units on its motorway network by the end of 2024, with a further 54 units planned for 2025, leading to a final deployment of 525 units (Source: Peter Meckel (ASFINAG), "C-ITS Deployment in Austria," ITS Danmark Annual Meeting 2025). Roadworks Warning has been operational on the Austrian section of the Rotterdam–Vienna C-ITS Corridor (extending from the German border to the Hungarian border) as an operational use case since 2023. Both forms (mobile safety vehicle and fixed roadside) may be implemented under the same message specifications of the ETSI ITS stack. It may further be noted that, in the case of ASFINAG, deployment of both forms is being undertaken in parallel.

Strategic implications: completion of life-safety-related use cases at Day-0

The Day-0 use cases presently set out in Section 5.2 of Annexure-III are directed principally at general vehicle-to-vehicle collision avoidance. The reduction of emergency-vehicle arrival times (directly bearing on survival rates in medical emergencies) and the prevention of accidents in roadworks zones (a leading cause of serious motorway accidents) are, however, equally urgent challenges in the Indian context.

According to the Ministry of Road Transport and Highways report "Road Accidents in India 2023" (referenced at Section 5.2(iii) of Annexure-III), India records approximately 173,000 road-accident fatalities per year. A material proportion of these is attributable to (i) delayed medical intervention owing to slow emergency-vehicle arrival, or (ii) collisions with vehicles or workers in roadworks zones or with stationary vehicles (the precise quantification of which would require separate analysis). The two Day-0 additions proposed in these comments would, without requiring any further infrastructure investment, provide direct V2X-based countermeasures to these challenges. The case for commencing deployment at the Day-0 stage, rather than deferring to Day-1 or Day-2, is accordingly substantial. The further proposal of the fixed-roadside form at Day-1 establishes a natural expansion path and ensures that the hazardous-location notification service is reinforced in stages across the whole of India's V2X deployment roadmap.

Q12 — Whether spectrum charges should be levied in respect of the V2I communication service authorisation, in view of the public-welfare orientation of V2X applications

ZSITS submits that no spectrum charge and no authorisation fee should be levied in respect of safety-related V2X services. Two distinct propositions inform that submission: (i) the class of entity eligible for authorisation should be restricted to governmental and government-authorised entities, and (ii) within that perimeter, neither spectrum charges nor authorisation fees should be levied in respect of safety-related V2X services.

Class of entity eligible for authorisation

ZSITS proposes that authorisation under the V2I communication service framework be restricted to the following classes of entity:

- Central Government agencies (MoRTH, National Highways Authority of India (NHAI), and other related ministries and authorities);
- State Government agencies (State Public Works Departments, State Road Development Corporations, and the like);
- Private entities authorised in writing by an entity falling within the two classes above. This category is intended to cover, in particular, concessionaires of public-private partnership expressways and Special Purpose Vehicles established under the Smart Cities Mission.

This formulation aligns with the policy stated in MoRTH letter dated 20.11.2025 (Annexure-IV to the Consultation Paper, paragraph 3): "The authorization for RSUs will be restricted to Central or State Governments or any other agencies authorized by them."

Fee structure for safety-related V2X services

Spectrum charges	Not to be levied (zero)
Authorisation fee	Not to be levied (zero)
Application processing fee	A minimal amount sufficient to recover administrative costs, consistent with the principles set out in the DoT Notification on Machine-to-Machine Service Authorisation (Gazette notification dated 09.09.2025)

This proposal is confined to safety-related V2X services. Should commercial value-added services (such as advertising distribution, entertainment content delivery, or commercial telematics services) come to be provided in future within the same authorisation framework, the introduction of a separate fee schedule for that commercial component would be a reasonable subject for further consideration at that time.

Rationale

Paragraph 3 of MoRTH letter dated 20.11.2025 (Annexure-IV) expressly states that "The authorization for RSUs will be restricted to Central or State Governments or any other agencies authorized by them." Paragraph 3.14(b) of the Consultation Paper restates and reaffirms that policy. The proposal at the first table above does no more than acknowledge that existing policy, and clarify in operational terms its scope (so as to include concessionaires and Special Purpose Vehicles which are themselves authorised by Central or State Governments).

This staged approach is consistent with the regulatory trajectory followed in Japan in relation to roadside-unit licensing for the ITS Connect system operating in the 760 MHz band. When ITS Connect was introduced in 2015, the radio-station authorisation rules issued under the Radio Act limited the class of licensee for ITS roadside units to the National Police Agency alone. As the requirement for broader rollout of roadside units became apparent in the context of automated-driving implementation, the Ministry of Internal Affairs and Communications amended the relevant rules, as promulgated on 23 December 2025, so as to extend the class of eligible licensees to "the State, local governments, and other operators." The Indian framework set out in MoRTH letter dated 20.11.2025 — restricting authorisation to Central or State Governments and to agencies authorised by them — may be understood as adopting an analogous staged approach:

initial deployment is driven by governmental entities, with extension to authorised non-governmental entities accommodated within the same regulatory perimeter.

Question 12 itself is framed in terms of "the public welfare-oriented nature of V2X applications and the need to encourage the deployment of such infrastructure and services". The public-welfare character of V2X services is thus the starting premise of the Consultation Paper, not a matter still in issue. Paragraph 4.30 of the Consultation Paper records the prevailing international practice in the following terms: "The emphasis in international deployment of V2X have generally been on ensuring technical compliance, interoperability, and efficient spectrum use, rather than imposing significant financial burdens. This approach recognizes that the long-term benefits of V2X deployment, in terms of safety and efficiency, outweigh the potential short-term revenue gains from spectrum charges." Paragraph 4.34 of the Consultation Paper develops the point further, noting that the spectrum-charging framework applicable to V2X services must reflect the unique safety-critical character of those services and their broader societal benefits. The tendency of these passages in the Consultation Paper is to favour a treatment under which no spectrum charge is levied in respect of safety-related V2X services. ZSITS, accepting that tendency, proposes that both spectrum charges and authorisation fees be set to zero for such services.

The Department of Telecommunications, by its Gazette notification dated 09.09.2025 (referred to at paragraph 4.55 of the Consultation Paper), has provided in respect of the Machine-to-Machine (M2M) service authorisation that "There shall be no authorisation fee to be paid by the authorised entity." Machine-to-Machine services share with V2I services the characteristics of public-welfare orientation and low commercial margin, and the precedent so set by the Department is in our submission directly applicable to the V2I context.

It may further be observed that, in the case where the authorised entity is itself a governmental body, any authorisation fee or spectrum charge levied operates in substance as an internal transfer of resources within government, generating no net new public revenue. The administrative cost of operating such a charging mechanism (invoicing, reconciliation, and recovery of arrears) is incurred without corresponding benefit. This consideration provides a further, operational basis for setting both fees to zero.

Q15 — In the event that the methodologies referred to in Q13 and Q14 are not adopted, what alternative methodology should be applied for the determination of spectrum charges

ZSITS submits, as set out in response to Q12 above, that neither spectrum charges nor authorisation fees should be levied. V2X services are by their nature infrastructural services that are not provided with a view to commercial profit, and the conventional methodologies for determining spectrum charges contemplated by Questions 13 and 14 are accordingly not suited to them.

Zero-Sum ITS Solutions India Pvt. Ltd. remains available to the Authority for any clarification.

Annex: References to Documents Cited

TRAI Consultation Paper No. 08/2026 and its Annexures

- TRAI Consultation Paper No. 08/2026, paragraphs 3.14(b), 3.35, 3.38(g), 3.47, 3.48–3.55, 3.60, 4.30, 4.34, 4.55, and Chapter V Questions Q1(c), Q1(e), Q4, Q5, Q6, Q8(d), Q8(e), Q11, Q12 and Q15
- Annexure-I to the Consultation Paper (DoT Reference dated 01.12.2025)
- Annexure-II to the Consultation Paper (Report by the DoT Committee on V2X/ITS Policy Formulation, January 2023)
- Annexure-III to the Consultation Paper (Final Report of the MoRTH Task Force on Intelligent Transportation System, January 2026), paragraphs 4.1(i), 4.1(ii), 8.1, 8.4, 8.5, 8.6 and 8.8; Sections 5.2, 5.3 and 5.4
- Annexure-IV to the Consultation Paper (MoRTH letter dated 20.11.2025), paragraph 3

Indian regulatory and legislative instruments

- The Telecommunications Act 2023, Section 19
- Department of Telecommunications, Notification on Machine-to-Machine (M2M) Service Authorisation, Gazette notification dated 09.09.2025
- National Security Directive on Telecommunication Sector (NSDTS), approved by the Cabinet Committee on Security on 16 December 2020 and in force from 15 June 2021
- Trusted Telecom Portal (www.trustedtelecom.gov.in), operated by the Department of Telecommunications and the National Cyber Security Coordinator
- Rule 144(xi) of the General Financial Rules, Department of Expenditure (Ministry of Finance), amended 23 July 2020 (including Public Procurement Order No. 4 dated 23 February 2023)
- AIS 189: Approval of Vehicles with Regard to Cybersecurity and Cybersecurity Management System (ARAI / AISC, derived from UN R155; in force for new vehicle types from 1 October 2025 and for all vehicle types from 1 October 2028)
- AIS 190: Software Update Management System (ARAI / AISC, derived from UN R156; in force for new vehicle types from 1 October 2025 and for all vehicle types from 1 October 2028)

International standards and instruments

- ETSI TS 102 941 (ITS Trust and Privacy Management)
- U.S. Department of Commerce, Bureau of Industry and Security, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles" Final Rule, 90 Federal Register 5360 (published 16 January 2025, effective 17 March 2025)
- European Commission, C-Roads Platform — joint initiative of EU Member States and road operators
- Ministry of Internal Affairs and Communications (Japan), amendment to the rules under the Radio Act concerning licensees for ITS radio stations in the 700 MHz band, promulgated on 23 December 2025

[End of submission]