TRAI Consultation Paper No. 08/2026

on the Regulatory Framework for Vehicle-to-Everything (V2X) Communication

Submitted by:

[Sumit Chouhan]

[SVP – Automotive / UAV Cybersecurity]

+91-9868275577

c.sumit@trojanhuntindia.com

To,
Shri Akhilesh Kumar Trivedi
Advisor (Networks, Spectrum and Licensing)
Telecom Regulatory Authority of India
Tower F, NBCC World Trade Centre
Nauroji Nagar, New Delhi - 110029
Email: advmn@trai.gov.in

Subject: Comments on TRAI Consultation Paper No. 08/2026 on the Regulatory Framework for Vehicle-to-Everything (V2X) Communication, dated 30 April 2026.

Dear Sir,

Jai Hind!

This submission is filed in response to the Consultation Paper No. 08/2026 on the Regulatory Framework for V2X Communication. The comments below address questions Q1 through Q26 with a primary focus on the cybersecurity dimensions of V2X deployment in India, drawing on ongoing technical engagement with C-V2X cooperative safety systems and automotive cybersecurity practice.

The comments are organised by question number for ease of reference, with extended treatment of Q7 (security framework) and Q11 (other regulatory framework issues), where India-specific considerations and cybersecurity architecture decisions warrant additional analysis.

A summary of positions is provided in the Executive Summary that follows. Detailed responses begin with Part A.

Yours sincerely,

Sumit Chouhan
5th May 2025
New Delhi

Table of Contents

Executive Summary

The Telecom Regulatory Authority of India released Consultation Paper No. 08/2026 on the Regulatory Framework for Vehicle-to-Everything (V2X) Communication on 30 April 2026, with comments invited by 28 May 2026 and counter-comments by 11 June 2026. This submission engages with the consultation across all twenty-six questions, with extended technical analysis on the cybersecurity dimensions in Q7 and on India-specific considerations in Q11.

Three core positions are advanced in this submission:

First, the consultation should formally endorse the security framework recommended by the MoRTH Task Force on Intelligent Transportation System (paragraph 8.6 of the Task Force final report), based on ETSI TS 102 941 derived from IEEE 1609.2. However, the consultation paper's Q7(c) on coexistence with the legacy X.509 PKI infrastructure operated by the Controller of Certifying Authorities requires architectural specificity rather than preserving optionality. This submission recommends Option A (a separate national ITS root Certificate Authority) over Option C (X.509 countersigning of ITS certificates), with a formal acknowledgement bridge between CCA and a National V2X Root CA established at the policy and audit level rather than the certificate format level. The technical reasoning for this recommendation is presented in detail under Part E.

Second, crypto-agility and post-quantum readiness should be built into the V2X public key infrastructure framework from inception. With the United States National Institute of Standards and Technology having finalised FIPS 203 (Module-Lattice-Based Key-Encapsulation Mechanism, ML-KEM) and FIPS 204 (Module-Lattice-Based Digital Signature Standard, ML-DSA) in 2024, the cryptographic primitives that will secure V2X communications today should include explicit migration pathways. Vehicles deployed in 2026 will operate through 2040 and beyond. The "Store Now, Decrypt Later" risk applies materially to long-lived V2X telemetry, pseudonym credentials, and any persistent identifier that vehicles broadcast over their operational lifetimes.

Third, multi-authority coordination across TRAI, the Department of Telecommunications, the Ministry of Road Transport and Highways, the Controller of Certifying Authorities, the Ministry of Electronics and Information Technology, the Automotive Research Association of India, the International Centre for Automotive Technology, the National Highways Authority of India, and State Governments should be formalised through a permanent V2X Cybersecurity Coordination Forum. The current bilateral arrangements between authorities create jurisdictional gaps in incident response, misbehaviour detection authority, and cross-track coordination with AIS-189 and AIS-190 implementation. The MoRTH Task Force's continuity recommendation (paragraph 8.12 of the Task Force final report) provides an institutional starting point for this Forum.

The submission also addresses Indian-road specific threat modelling considerations under Part G. The cybersecurity assumptions embedded in IEEE 1609.2 and ETSI TS 102 941 were largely calibrated against traffic environments characterised by lane discipline, homogeneous vehicle classes, and predictable trajectory patterns. Indian roads exhibit none of these characteristics, with high two-wheeler density, mixed-mode driving behaviour, and atypical vehicle classes that fall outside the standard SAE and ETSI taxonomies. Specific implications for misbehaviour detection thresholds, pseudonym certificate scaling, and Vulnerable Road User protection are analysed.

On the financial conditions in Q12 through Q26, this submission supports minimal or no spectrum charges for safety-related V2X spectrum, consistent with international precedent and the public welfare nature of cooperative safety services. The treatment of these questions in the present submission is brief, with detailed financial analysis deferred to industry stakeholders better positioned to engage with revenue and pricing models.

Part A: Responses on V2I Authorisation (Q1 to Q3)

Q1: Need for V2I Authorisation

Position: Yes, V2I communication service should require authorisation under Section 3(1)(a) of the Telecommunications Act, 2023.

Roadside Unit (RSU) operations involve the establishment of fixed wireless infrastructure that interfaces with vehicles operating safety-critical decisions in real time. Without a formal authorisation framework, there is no enforceable mechanism for technical compliance, security baseline adherence, or interference management. This position aligns with international precedent, including the Federal Communications Commission Part 90 framework in the United States, the Innovation, Science and Economic Development Canada licensed RSU framework, the Ministry of Industry and Information Technology licensing approach in China, and the Ministry of Science and ICT licensing framework in South Korea.

Q1(a): Eligibility conditions for the authorisation

Authorisation should be available to the following categories of entities:

- Central Government, State Governments, and their authorised agencies, consistent with the position expressed in the MoRTH letter dated 20 November 2025 referenced as Annexure-IV of the consultation paper
- National Highways Authority of India and equivalent road-owning agencies at State and municipal levels
- Public Sector Undertakings designated by Central or State Governments for ITS deployment
- Private entities authorised by Central or State Governments for specific V2I services in defined geographic areas, with restrictions for safety-critical applications
- Academic and research institutions for time-bounded pilot deployments under controlled conditions, with explicit sunset provisions

The eligibility framework should explicitly recognise that the authorisation entitles the holder to deploy infrastructure that exchanges safety-critical messages with vehicles. The eligibility threshold should reflect this responsibility through demonstrated technical and operational capability, including the ability to maintain continuous operations, respond to security incidents within defined timelines, and participate in misbehaviour detection processes at scale.

Q1(b): Period of validity and conditions for renewal

Initial authorisation period: ten years from the date of grant, matching the FCC precedent established under 47 CFR Section 90.149(b). Renewable for further ten-year periods subject to

compliance review. The ten-year horizon balances investment certainty for infrastructure deployment with the need for periodic review as the technology and threat landscape evolve.

Q1(c): Service area of the authorisation

State-level service areas as the default unit, with provisions for:

- National authorisations for entities operating across multiple states, such as the National Highways Authority of India and Central Government agencies
- District-level authorisations for municipal and urban local body deployments
- Geographic boundaries explicitly tied to road network jurisdiction rather than administrative boundaries alone, to avoid coverage gaps at jurisdictional boundaries

Q1(d): Scope of service of the authorisation

The authorisation framework should distinguish between three service categories, each with potentially different technical, operational, and financial conditions:

- Safety-related V2I services, including collision warnings, emergency vehicle priority, hazard alerts, and Vulnerable Road User protection
- Operational V2I services, including electronic toll collection, traffic management, parking management, and pollution monitoring
- Commercial value-added V2I services, including infotainment delivery, advertising, and third-party data services

The categorisation matters because spectrum charges, AGR computation rules, and authorisation fee structures may reasonably differ across these categories. Safety-related services should attract minimal regulatory friction. Commercial services should be subject to standard commercial regulatory treatment.

Q1(e): Technical, operating, and security related conditions

This sub-question is the formal entry point for the security framework discussion. Detailed technical and security conditions are addressed under Part E (Q7 response) of this submission. A brief summary is provided here for completeness:

Technical conditions:

- Compliance with TEC-specified C-V2X equipment requirements
- Adherence to MoRTH Task Force-recommended power, antenna height, and out-of-band emission limits as set out in paragraph 7.3 of the Task Force Part-1 report
- Mandatory certification under MTCTE for both OBUs and RSUs (see Q5)

Operating conditions:

- Continuous operational availability for safety-related deployments, with defined Service Level Agreements
- Mandatory security incident reporting to the relevant authority within 72 hours of detection
- Annual operational audits by accredited assessors

Security conditions:

- Adherence to ETSI TS 102 941 / IEEE 1609.2 derived security framework as recommended by the MoRTH Task Force
- Mandatory participation in misbehaviour detection processes at the national level
- Crypto-agility provisions to enable algorithm migration over the operational lifetime of deployed equipment
- Compliance with privacy-preserving pseudonym certificate management requirements

Q1(f): Any other related aspect

The authorisation framework should include provisions for infrastructure sharing between authorised entities, analogous to the telecommunications infrastructure sharing framework established under DoT IP-1 authorisation. RSU infrastructure deployment is capital-intensive and benefits from sharing arrangements, particularly in dense urban corridors and along major highway networks where multiple operators may have legitimate deployment interest.

Provisions should also be made for transition mechanisms applicable to any legacy DSRC pilot deployments, although the consultation paper notes that there are no significant legacy V2X implementations in India.

Coordination mechanisms with AIS-189 (Cyber Security Management System) and AIS-190 (Software Update Management System) compliant vehicles should be explicit. The vehicle-side cybersecurity regulation through MoRTH and the infrastructure-side authorisation through TRAI must operate as complementary tracks rather than parallel ones.

Q2: Alternative mechanism if no authorisation

Not applicable, given the affirmative position to Q1.

Q3: Other suggestions on V2I authorisation

Additional suggestions on the authorisation framework, including India-specific threat modelling considerations and governance coordination, are presented in Part G and Part H of this submission. These are formally responses under Q11 (other regulatory framework issues) but cross-reference Q3 where relevant.

Part B: Response on Technology Selection (Q4)

Q4: Specific technology prescription for C-V2X

Position: A phased approach is recommended. LTE-V2X (3GPP Release 14 and Release 15) for Day-0 deployment focused on safety-critical V2V and V2I applications, followed by NR-V2X (Release 16 and onwards) for advanced cooperative driving and platooning use cases, with formal interoperability requirements during the transition period.

The consultation paper acknowledges in paragraph 3.28 that NR-V2X is not backward compatible with LTE-V2X. The two technologies use different radio waveforms, numerologies, and sidelink designs, such that an LTE-V2X device cannot directly decode NR-V2X sidelink transmissions, and vice versa. This non-interoperability is a substantive design challenge that warrants explicit treatment in the regulatory framework rather than deferral to industry consensus.

The dissent note from Shri Sharad Kumar Chauhan, Member from the Wireless Planning and Coordination Wing, recorded in Annexure-III of the consultation paper, correctly observes that the recommendation to lock the entire 50 MHz spectrum allocation to a specific technology like C-V2X conflicts with the technology-neutral principle articulated in the Telecommunications Act, 2023. The dissent from Dr. Santosh Sam Koshy from the Centre for Development of Advanced Computing similarly raises concerns about the LTE-V2X and NR-V2X coexistence question, noting that the FCC chose not to specify any particular 3GPP release in its Second Report and Order while still encouraging industry consensus on technology standards.

This submission proposes a structured phased approach:

1. Phase 1 (Years 1 to 3 of deployment): LTE-V2X (Release 14 / Release 15) prescribed for safety-critical V2V and V2I applications. Mandatory dual-mode capability requirements for OBUs manufactured beyond a defined cutoff date.
2. Phase 2 (Year 3 onwards): NR-V2X (Release 16 and later) authorised for advanced cooperative driving and platooning applications, alongside continued LTE-V2X operation for basic safety services.
3. Throughout both phases: Interoperability gateways at RSUs to support both modes, ensuring that safety-critical messages remain decodable by any compliant vehicle on the road.

This approach matches the FCC's stated preference for objective performance expectations rather than mandated specific standards (FCC Second Report and Order, paragraph 21), while providing greater deployment certainty for the Indian ecosystem during the formative period. It also addresses the legitimate concerns raised in both dissent notes without compromising the safety objective.

Part C: Response on Equipment Certification (Q5)

Q5: MTCTE for RSUs and OBUs

Position: Yes, both RSUs and OBUs should be brought under the Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) regime, with explicit cybersecurity baseline requirements added to the existing Essential Requirements.

The TEC procedure for MTCTE, as referenced in paragraph 3.38 of the consultation paper, already includes security requirements as mandated by DoT Headquarters and the National Centre for Communication Security. For V2X equipment, this baseline should be extended to include the following category-specific requirements:

For On-Board Units

- Secure boot with measured attestation, ensuring that only signed firmware loads on the device
- A Trusted Execution Environment (TEE) or Hardware Security Module (HSM) for cryptographic key storage, isolating long-term enrolment credentials and pseudonym certificate private keys from the application processor
- Secure key provisioning at manufacture, with factory-installed enrolment credentials issued through a controlled provisioning process
- Firmware update authenticity verification, with cryptographic signature checks before any update is applied
- Side-channel attack resistance for key extraction, particularly relevant for OBUs that may be physically accessible to vehicle owners or third parties

For Roadside Units

- All On-Board Unit baseline requirements above
- Tamper detection and reporting, with automatic notification to the misbehaviour authority on physical tampering events
- Network attack resistance against denial-of-service, replay, and message injection attacks
- Physical security baseline appropriate for outdoor installation in publicly accessible locations
- Support for remote attestation by the misbehaviour authority, allowing periodic verification that the RSU is operating its intended firmware

Reference frameworks

The cybersecurity baseline should be defined with reference to the following established frameworks:

- UNECE Regulation No. 155 and Regulation No. 156 for the vehicle-side integration of OBUs
- ISO/SAE 21434 for cybersecurity engineering process maturity
- IEEE 1609.2 for V2X security message processing
- ETSI TS 103 097 for security header and certificate format specifications

The MTCTE certification body designation should include conformity assessment laboratories with V2X-specific test capabilities, including the ability to verify cryptographic operations under realistic vehicular latency budgets.

Part D: Response on ITS Stack Standardisation (Q6)

Q6: Stack standardisation and ETSI adoption

Position: Yes, the Intelligent Transportation System stack should be standardised. Yes, the ETSI TC ITS stack as recommended by the MoRTH Task Force in paragraph 8.5 of the Task Force final report should be adopted, with the corresponding ETSI standards taken up by the Telecommunications Standards Development Society India and the Telecommunication Engineering Centre for adoption as National Standards.

Stack standardisation is essential for interoperability across multiple Original Equipment Manufacturers, RSU operators, and equipment vendors. Without a common stack, cross-vendor message decoding and trust validation become brittle, undermining the cooperative safety value proposition that V2X is intended to deliver.

The recommendation to adopt the ETSI TC ITS stack aligns with the broader ecosystem decision to adopt ETSI TS 102 941 for security (addressed in Part E of this submission). The stack and the security framework should be aligned through a common standards body source, not split between standards bodies in a way that creates integration complexity.

The MoRTH Task Force's recommendation to use TSDSI or TEC for adoption is appropriate. This pathway ensures that the National Standard remains aligned with ETSI standard updates while providing institutional scope for India-specific extensions where required, particularly for vehicle classes specific to Indian traffic environments such as three-wheelers, agricultural vehicles, and the high-density two-wheeler population that constitutes a substantial fraction of the Indian vehicle fleet.

Part E: Response on Security Framework (Q7)

Q7 is the primary section of this submission. The detailed treatment below addresses each of the three sub-questions in turn, with the response to Q7(c) on X.509 coexistence presenting the principal technical contribution.

Q7(a): Security framework architecture

Position: Endorse the MoRTH Task Force baseline of ETSI TS 102 941 (Trust and Privacy Management) derived from IEEE 1609.2 (Security Services for Applications and Management Messages), as recommended in paragraph 8.6 of the Task Force final report. Add four specific extensions: crypto-agility provisions, a misbehaviour detection authority, ITU-T X.1372 threat taxonomy compliance, and explicit pseudonym certificate management specifications.

Crypto-agility provisions

The PKI framework should explicitly support multiple cryptographic algorithms with versioning at the certificate level. Specific recommendations:

- Current baseline: ECDSA over NIST P-256 or Brainpool P-256r1, consistent with ETSI TS 103 097 version 2.1.1 specifications
- Migration target: hybrid signatures combining ECDSA with ML-DSA (NIST FIPS 204) for post-quantum resistance, anticipating that purely classical signatures may not remain quantum-resistant within the operational lifetime of vehicles deployed today
- Algorithm identifiers carried in certificate extensions, enabling graceful migration where validating parties can negotiate algorithm support with signing parties

The crypto-agility requirement is critical for V2X because vehicles deployed in 2026 will operate through 2040 and beyond. The cryptographic primitives that secure today's certificates may not be quantum-resistant within that operational lifetime. Building crypto-agility now avoids a costly retrofit cycle later, where every deployed vehicle and RSU would need firmware updates to support new algorithms. Equivalent migrations have been historically expensive in other infrastructure domains, including the SHA-1 to SHA-2 migration in TLS and the 3DES to AES migration in payment systems. V2X has the unique characteristic that the population of devices needing migration is not centrally managed and includes safety-critical communications with strict latency budgets, making forward-looking crypto-agility design substantially more important than in those prior cases.

Misbehaviour detection authority

A dedicated Misbehaviour Authority function, operationally separate from the credentialing authority, should be established with the following responsibilities:

- Receive misbehaviour reports from RSUs and, optionally, from OBUs that detect anomalous messages from other vehicles
- Correlate reports across geography and time to identify systematic compromise versus isolated anomalies
- Generate revocation requests for compromised credentials
- Maintain Certificate Revocation Lists (CRLs) and Certificate Trust Lists (CTLs)
- Coordinate with the national Computer Emergency Response Team (CERT-In) on V2X incidents that have broader cybersecurity implications

The technical architecture should follow the IEEE 1609.2 misbehaviour detection model, with adaptations for India's operational context discussed under Part G of this submission.

ITU-T X.1372 threat taxonomy compliance

The security framework should explicitly map controls to the seven threat categories identified in ITU-T X.1372 and reproduced at paragraph 3.51 of the consultation paper:

- Threats to confidentiality, including unauthorised access to V2X messages or related data
- Threats to integrity, including alteration, forgery, or corruption of messages in transit
- Threats to availability, including disruption or denial of safety-critical V2X services
- Threats to non-repudiation, where senders may later deny having sent specific messages
- Threats to authenticity, where receivers cannot verify that a message originated from the claimed sender
- Threats to accountability, where actions or messages cannot be traced to responsible entities
- Threats to authorization, where entities perform actions or access functions without proper permission

Mapping each control in the security framework to one or more of these threat categories provides a structured basis for control adequacy review and gap analysis.

Pseudonym certificate management

Privacy-preserving pseudonym schemes are foundational to V2X. The framework should specify:

- Pseudonym certificate validity period of seven days maximum, balancing privacy protection against operational overhead

- Number of pseudonym certificates held simultaneously by an OBU in the range of twenty to one hundred, balancing privacy protection through frequent rotation against on-board storage and provisioning bandwidth requirements
- Rotation triggers including time-based (at fixed intervals), geography-based (on entering specific zones), and ignition-cycle-based (on each vehicle start)
- Pseudonym-to-true-identity unlinkability requirements, ensuring that the credentialing authority cannot reconstruct vehicle movement patterns from pseudonym usage data

Q7(b): Implementing agency

Position: A multi-agency model with clear functional separation. The Controller of Certifying Authorities serves as the credentialing authority. CERT-In or a new V2X-CERT serves as the misbehaviour authority. Standards adoption is delegated to TEC and TSDSI. Vehicle-side OBU testing is conducted by ARAI and ICAT. Coordination is provided through a permanent V2X Cybersecurity Coordination Forum, addressed under Part H.

Credentialing Authority

The Controller of Certifying Authorities is the appropriate agency for the credentialing function, given its existing statutory role under the Information Technology Act, 2000. CCA already operates the Root Certifying Authority of India and possesses the institutional infrastructure for certificate authority operations, including audit and accreditation processes for subordinate Certifying Authorities.

However, as discussed in detail under Q7(c), the V2X Root CA should be operationally distinct from the existing Root Certifying Authority of India X.509 hierarchy, while remaining under CCA institutional oversight.

Misbehaviour Authority

The misbehaviour authority function should not be placed within CCA. The CCA operating model is designed for long-validity X.509 certificate issuance and audit, not for near-real-time misbehaviour correlation across millions of vehicles producing messages at ten Hertz. The operational characteristics differ fundamentally between traditional PKI operations and V2X misbehaviour detection.

Recommended placement: a new functional unit within CERT-In, or alternatively a new entity operating under MeitY designated as V2X-CERT, with formal liaison arrangements to CCA, MoRTH, and DoT. The placement within or adjacent to the national CERT structure ensures alignment with broader cybersecurity incident response capabilities and provides a natural pathway for V2X-specific incidents that have implications beyond the V2X domain.

Standards Adoption and Conformity Assessment

- TEC for equipment-level certification under MTCTE, building on the existing MTCTE framework with V2X-specific Essential Requirements as discussed under Q5
- TSDSI for National Standard adoption from ETSI source standards, providing institutional alignment with the broader 3GPP and ETSI standards ecosystem
- ARAI and ICAT for vehicle-integrated OBU testing under the AIS-189 cybersecurity framework, ensuring coherence between vehicle-side and infrastructure-side security requirements

Q7(c): Coexistence of V2X PKI with legacy X.509 PKI

Position: Recommend Option A (a separate national ITS root Certificate Authority) as proposed in MoRTH Task Force paragraph 7.3.5(A), with a formal acknowledgement bridge between CCA and the National V2X Root CA established at the policy and audit level rather than at the certificate format level. Reject Option C (X.509 countersigning of ITS certificates) for the technical reasons set out below.

This is the primary technical recommendation of the present submission. The reasoning is presented in detail because the architectural choice between Option A and Option C will determine the operational characteristics of Indian V2X PKI for decades.

Why Option C (X.509 countersigning) is technically problematic

Option C, as described in Task Force paragraph 7.3.5(C), proposes that the national X.509 root Certificate Authority countersigns the ITS certificates issued under the IEEE 1609.2 / ETSI TS 102 941 framework. This proposal is technically problematic for the following reasons.

First, certificate format incompatibility is irreducible at the technical level. IEEE 1609.2 explicit certificates use ASN.1 OER (Octet Encoding Rules) encoding, distinct from the X.509 DER (Distinguished Encoding Rules) encoding. The certificate field semantics differ substantially, with IEEE 1609.2 certificates including V2X-specific fields such as application identifiers, geographic regions, and short certificate representations optimised for the V2X latency budget of sub-100 millisecond verification at vehicular speeds. A countersigning bridge does not reconcile these structural differences. It adds an additional signature layer that V2X verification logic does not natively process.

The consultation paper acknowledges this difficulty directly in paragraph 3.57: that there are no global standards seeking to resolve the incompatibility, and that any bridging facility would require system-level customisation rendering the resulting solutions globally non-compatible.

Second, international interoperability is foreclosed under Option C. A vehicle whose certificate is countersigned by an Indian X.509 root CA will not be validatable by IEEE 1609.2 verification logic

in vehicles or RSUs deployed in countries that follow the SCMS model in the United States, the CCMS model in the European Union, or the C-SCMS model in China. For cross-border road transport, particularly along corridors connecting India with Nepal, Bhutan, Bangladesh, and (via maritime ports) other regions, this is a significant operational limitation. Foreign-registered vehicles operating temporarily in India would face equivalent difficulties.

Third, cryptographic complexity creates attack surface. A non-standard bridging mechanism requires custom validation logic to be implemented in every OBU and RSU. Custom cryptographic code paths are historically the highest-risk surface for implementation vulnerabilities, with extensive documented history of side-channel attacks, padding oracle attacks, and verification bypass vulnerabilities in non-standard cryptographic glue code. The principle of using standard, well-analysed cryptographic constructions weighs heavily against Option C.

Fourth, the legal recognition motivation can be addressed differently. The apparent motivation for Option C is the Information Technology Act, 2000 recognition of X.509 digital signatures as legally equivalent to handwritten signatures. This legal recognition does not, however, technically require the V2X certificates to be in X.509 format. The same legal effect can be achieved through one of three alternative pathways:

4. Statutory amendment to the Information Technology Act recognising IEEE 1609.2 explicit certificates as valid digital signatures for V2X-specific purposes, alongside the existing X.509 recognition for general purposes
5. Regulatory clarification by MeitY that V2X message authentication is a distinct technical category from general digital signature recognition, with the V2X PKI operating under a sectoral framework
6. Cross-recognition framework where CCA formally recognises a separate National V2X Root CA as a sovereign credentialing entity, with audit and accreditation oversight, but without requiring X.509 format for the operational certificates

The third pathway is the recommended approach in the present submission, as it preserves CCA institutional oversight while avoiding the technical compromises inherent in Option C.

Recommended architecture: Option A with policy bridge

The recommended architecture is structured as follows:

- A National V2X Root Certificate Authority issuing IEEE 1609.2 explicit certificates, operationally distinct from the Root Certifying Authority of India X.509 hierarchy
- A formal Policy Bridge mechanism whereby CCA provides institutional recognition and audit oversight of the National V2X Root CA, but without certificate-format coexistence requirements

- Subordinate Enrolment Authority and Authorization Authority entities operating under the National V2X Root CA, consistent with the IEEE 1609.2 and ETSI TS 102 941 trust hierarchy
- A separate Misbehaviour Authority operating under CERT-In or V2X-CERT, generating revocation requests to the Authorization Authority based on systematic correlation of misbehaviour reports

This architecture provides the following benefits:

- Native compatibility with IEEE 1609.2 and ETSI TS 102 941, avoiding custom validation logic
- Sovereign control through the National V2X Root CA, preserving institutional independence
- Future cross-border interoperability through standard IEEE 1609.2 trust mechanisms, which are already used for cross-border interoperability between SCMS in the United States and CCMS in the European Union under bilateral arrangements
- Legal recognition pathway through the formal CCA acknowledgement, addressing the Information Technology Act concern without architectural compromise
- Operational separation between credentialing and misbehaviour detection, consistent with operational best practice in V2X PKI deployments globally

Part F: Response on Spectrum Framework (Q8 to Q11)

The response to Q8 covers all sub-questions, with detailed treatment focused on those with cybersecurity implications. Q9, Q10, and Q11 are addressed briefly, with Q11 cross-referenced to Parts G and H below.

Q8: Regulatory framework for spectrum assignment

Q8(a): Partitioning the 30 MHz spectrum

Yes, partitioning the 30 MHz spectrum (5,875 to 5,905 MHz) for safety applications and operational applications is recommended. The partitioning protects safety-critical communications from contention with operational traffic, particularly under heavy network load conditions. International precedent supports this approach: the FCC Second Report and Order codified a three-tier message priority hierarchy with Safety-of-Life Communications receiving absolute priority.

Q8(b) and Q8(c): Exclusive vs shared assignment

Shared assignment is recommended for the 5,895 to 5,925 MHz band, consistent with the FCC and ISED approaches. Exclusive assignment of safety-critical spectrum to a single operator creates concentration risk and impedes the cooperative coverage that V2X is intended to deliver. Interference management should be addressed through technical conditions including directionality, protection distance, and antenna height limits, rather than through exclusive frequency assignment.

Q8(d): Interference management parameters

Support the MoRTH Task Force-recommended parameters as the baseline. Specifically:

- Maximum effective isotropic radiated power of 4 watts (36 dBm) for both OBUs and RSUs
- Conducted power output of 200 milliwatts (23 dBm) over 20 MHz or higher bandwidth for RSUs
- Out-of-band emission limits as specified in Table 3.1 of the consultation paper

Adding to these parameters, the framework should explicitly include jamming detection capabilities at RSUs, with reporting to the misbehaviour authority. Radio frequency jamming of safety-critical V2X communications should be recognised as a cybersecurity threat, not solely an interference issue. Jamming detection at the infrastructure layer enables timely alerting and coordination with law enforcement when jamming is malicious.

Q8(e): SACFA-equivalent prior approval

Yes, a mechanism analogous to SACFA clearance should be mandatory for RSU establishment. The mechanism should be designed with cybersecurity considerations in mind:

- A public registry of authorised RSU locations and operators, supporting transparency and enabling misbehaviour detection at the infrastructure level
- Attestation records for deployed RSUs, capturing firmware versions, configuration baselines, and security control posture
- Periodic security audit reporting, with audit findings recorded in the registry
- A reporting mechanism for unauthorised RSU sightings, which would indicate either rogue infrastructure or compromised legitimate infrastructure

This balances transparency, which is essential for trust in cooperative safety systems, with operational security considerations.

Q8(f): Power and OOBE limits

Endorse the MoRTH Task Force recommendations on radiated power limits and out-of-band emission limits, as these reflect the international ETSI EN 302 571 baseline appropriate for ITS operations.

Q8(g): Maximum period of spectrum assignment

Ten years from grant, matching the V2I authorisation period proposed in Q1(b), to ensure alignment between authorisation validity and spectrum assignment validity.

Q8(h): Roll-out obligations

Yes, roll-out obligations should be prescribed. The FCC Second Report and Order provides a useful precedent at 47 CFR Section 90.389(b), requiring RSU operations to commence within twelve months of registration. A similar requirement, calibrated to Indian deployment timelines, would prevent spectrum hoarding and ensure that authorised entities deploy infrastructure consistent with their authorisation.

Q8(i): Surrender of spectrum

Yes, provisions for spectrum surrender should be introduced, with appropriate procedural safeguards to prevent operational disruption to vehicles relying on the surrendered RSU coverage.

Q9: Timelines for processing applications

Yes, prescribed timelines should be introduced for application processing, with a target of ninety days from complete application to grant for standard cases. Complex cases requiring inter-agency

coordination may require longer timelines, but these should be the exception with documented reasons.

Q10 and Q11: Other suggestions

Additional suggestions on the regulatory framework, particularly on Indian-road specific threat modelling and governance coordination, are presented in Part G and Part H of this submission.

Part G: Indian-Road Threat Modelling (under Q11)

The need for India-specific threat modelling

The consultation paper acknowledges in paragraph 4.31 that India's traffic environment is heterogeneous and presents context-specific challenges in V2X adoption. The implications for V2X cybersecurity are substantial but undertreated in the current consultation paper.

The cybersecurity assumptions embedded in the IEEE 1609.2 and ETSI TS 102 941 frameworks were largely calibrated against threat models developed in environments characterised by:

- Strong lane discipline
- Homogeneous vehicle classes
- Predictable trajectory patterns
- Low-density Vulnerable Road User presence

Indian roads invert these assumptions in ways that have direct cybersecurity implications.

Misbehaviour detection threshold recalibration

Algorithms for detecting anomalous Basic Safety Messages (BSMs), including sudden trajectory changes, implausible speed claims, and position inconsistencies, are typically tuned against Western traffic data. In Indian traffic, what appears anomalous by Western thresholds may be normal driving behaviour. A vehicle making a sudden lateral movement may be performing a routine lane change in an environment with weak lane discipline. A vehicle reporting an unusual speed may be operating under traffic conditions where speed varies dramatically over short distances.

The implication for misbehaviour detection: thresholds calibrated for Western traffic will produce high false positive rates in Indian traffic, undermining the trustworthiness of misbehaviour reports. Tuning thresholds for Indian conditions requires dedicated test data collection and may require fundamentally different statistical approaches that account for the higher entropy of Indian driving behaviour.

Vulnerable Road User protection in two-wheeler-dense environments

V2P specifications assume relatively low pedestrian and cyclist density. In urban Indian traffic, two-wheeler density frequently exceeds thirty percent of total traffic, with each two-wheeler operator constituting a Vulnerable Road User. This creates a scaling challenge for V2P broadcast volume and pseudonym rotation that exceeds the design assumptions of standard V2X PKI specifications.

At a busy intersection in any major Indian city, the cryptographic operations per second required for full V2P pseudonym rotation can exceed the capacity assumptions of current PKI designs. This is not a problem unique to India, but Indian traffic patterns make the scaling challenge particularly acute.

BSM spoofing under heterogeneous traffic

A spoofed BSM claiming a non-existent vehicle in a Western lane-disciplined environment is detectable through trajectory inconsistency. The plausibility envelope is narrow, and a fabricated vehicle outside that envelope is readily identified.

In Indian mixed-mode traffic, the implausible trajectory baseline is much wider, making misbehaviour detection harder. Adversarial use of this widened baseline, where attackers spoof BSMs that fall within the wider plausibility envelope of Indian traffic, requires specific study and mitigation. This is an area where India-specific research could contribute to the global V2X security knowledge base.

Three-wheeler and atypical vehicle classes

Indian traffic includes three-wheelers (auto-rickshaws), multi-axle freight, agricultural vehicles, and tractors that do not fit standard SAE or ETSI vehicle classifications. The OBU certification framework needs explicit treatment of these classes, including:

- Vehicle dynamics models appropriate for three-wheelers, which differ significantly from passenger cars and motorcycles
- Integration approaches for older vehicle architectures that may not have the in-vehicle network sophistication assumed by V2X integration specifications
- Power and connectivity considerations for vehicles operating in remote or rural environments where charging infrastructure and cellular connectivity may be limited

Cross-border corridors

India shares road borders with Nepal, Bhutan, Bangladesh, and (to a limited extent) Myanmar. Vehicle traffic across these borders is regular, particularly along major corridors such as the Indo-Nepal border at Raxaul, the Indo-Bangladesh border at Petrapole, and the Indo-Bhutan border at

Phuentsholing. The PKI architecture should anticipate cross-border credential validation rather than treating it as a future problem.

The Option A architecture recommended in Part E supports cross-border interoperability through standard IEEE 1609.2 trust mechanisms, in contrast to Option C which would require custom bridging at every border crossing.

Recommendation

The TRAI framework, in coordination with MoRTH and ARAI, should commission an India-specific V2X threat modelling study during the Phase 1 deployment period. The study should produce:

- Indian traffic-calibrated misbehaviour detection thresholds, supported by empirical traffic data collection
- Two-wheeler density scaling analysis for PKI infrastructure sizing
- Three-wheeler and atypical vehicle class certification framework
- Cross-border interoperability protocol with neighbouring countries, building on existing diplomatic and transport coordination mechanisms

Part H: Governance Coordination (under Q11)

Multi-authority structure analysis

The current V2X regulatory landscape in India involves multiple authorities, each with clear statutory grounding for their respective domains:

- TRAI for recommendations on the regulatory mechanism, spectrum charges, and authorisation framework
- DoT for spectrum assignment and authorisation under the Telecommunications Act, 2023, and for equipment certification through TEC under MTCTE
- MoRTH for vehicle-side regulation, including AIS-189 (CSMS) and AIS-190 (SUMS) implementation
- CCA for PKI and digital signature recognition under the Information Technology Act, 2000
- MeitY for overall information security policy and CERT-In operations
- ARAI and ICAT for vehicle testing and certification
- NHAI for highway-side RSU deployment and operations
- State Governments for urban and state highway RSU deployment
- NCIIPC for protection of critical information infrastructure

Each authority has clear statutory grounding within its domain. The risk to coherent V2X deployment is in the interfaces between authorities, particularly during incident response and during the routine handshakes required for ongoing operations.

Specific governance gaps

Four specific gaps warrant attention:

Misbehaviour authority placement. The current consultation paper does not designate a misbehaviour authority. Q7(b) of this submission proposes CERT-In or a new V2X-CERT for this role. The placement requires explicit decision rather than emergence by default.

Vehicle-side and infrastructure-side cybersecurity coordination. AIS-189 (CSMS) and AIS-190 (SUMS) regulate vehicle-side cybersecurity under the MoRTH track. The V2X PKI framework regulates infrastructure-side trust under the DoT, TRAI, CCA, and MeitY tracks. The handshake between these tracks is undefined. As an example: when an OEM's CSMS detects a compromised OBU, the OEM needs a defined mechanism to notify the V2X infrastructure-side authority for credential revocation. This mechanism is not currently specified.

Cross-State coordination. RSU operators in different states using shared PKI infrastructure create coordination requirements that are not yet specified. State-level deployments need defined interfaces for cross-state vehicle traffic.

Cross-border coordination. Already addressed under Part G of this submission.

Recommendation: V2X Cybersecurity Coordination Forum

Formalise the MoRTH Task Force's continuity recommendation (paragraph 8.12 of the Task Force final report) into a permanent V2X Cybersecurity Coordination Forum.

Mandate

- Standing coordination across all V2X cybersecurity authorities
- Incident response playbook maintenance and updates
- Annual review of misbehaviour detection effectiveness
- Cross-track coordination with AIS-189 and AIS-190 implementation
- Quarterly threat assessment updates
- Periodic public reporting on V2X cybersecurity posture

Composition

- MeitY representative as Chair, providing institutional separation from operational delivery
- Senior representatives from CCA, DoT, TRAI, MoRTH, ARAI, ICAT, NHAI, and CERT-In

- Two State Government nominees on rotational basis, ensuring State-level perspectives are included
- Two industry representatives nominated through SIAM (OEM perspective) and ITS India Forum (infrastructure operator perspective)
- Two academic and research representatives nominated through TSDSI

Operating model

- Quarterly plenary meetings
- Standing technical sub-committees for incident response, threat assessment, and PKI operations
- Annual public report on V2X cybersecurity posture
- Confidential incident reporting channels for Member entities

This structure provides the coordination capability that current bilateral arrangements between authorities cannot deliver. It also establishes a clear institutional locus for V2X cybersecurity decisions that span multiple statutory domains.

Part I: Responses on Financial Conditions (Q12 to Q26)

The financial questions Q12 through Q26 are addressed briefly in this submission. The author's primary focus is on the cybersecurity dimensions of V2X deployment. Detailed financial analysis is deferred to industry stakeholders and finance experts better positioned to engage with revenue and pricing models. Brief positions on the principal financial questions are presented below.

Q12: Spectrum charges

Position: minimal or no spectrum charges for safety-related V2X spectrum, supporting rapid deployment and consistent with international precedent.

Several international regulators have adopted minimal or no spectrum charges for V2X safety applications. The FCC operates a non-exclusive geographic area licensing framework. The EU and UK operate under licence-exempt regimes for both OBUs and RSUs. ACMA in Australia operates a class licensing approach with no individual fees. ISED in Canada is in the process of developing a structured but light-touch framework. The Indian framework should align with this international approach for safety-related services.

Minimal or no spectrum charges should not be confused with the absence of operational obligations. Spectrum at zero or minimal cost should come with strong technical, operational, and security obligations as conditions of authorisation, as discussed under Q1(e) and Part E.

Q13 to Q19: Spectrum charging methodology and AGR definitions

These questions are deferred to industry stakeholders. The general position is that any charging framework should be calibrated to recover administrative costs without impeding deployment, and should distinguish between safety-related and commercial V2X services in the manner suggested under Q1(d).

Q20: Excluding safety-related V2X revenue from AGR

Yes, revenue derived from safety-related V2X services should be excluded from AGR computation. This is consistent with the public welfare nature of safety services and avoids creating financial disincentives for deployment of safety-critical infrastructure. Commercial value-added V2X services should be treated separately under standard commercial regulatory frameworks.

Q21 to Q26: Other financial conditions

These questions on entry fees, bank guarantees, minimum equity and net worth requirements, application processing fees, authorisation fee rates, and other financial terms are deferred to industry stakeholders. The general position is that financial conditions should be calibrated to

facilitate participation by appropriate entities (primarily public sector and regulated private entities), without imposing barriers that would slow deployment of public safety infrastructure.

References

Standards

- IEEE Standard 1609.2-2022, "IEEE Standard for Wireless Access in Vehicular Environments -Security Services for Applications and Management Messages"
- IEEE Standard 1609.2.1-2022, "IEEE Standard for Wireless Access in Vehicular Environments -Certificate Management Interfaces for End Entities"
- ETSI TS 102 941 V2.2.1 (2022), "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management"
- ETSI TS 103 097 V2.1.1 (2021), "Intelligent Transport Systems (ITS); Security; Security header and certificate formats"
- ETSI EN 302 571, "Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band"
- ITU-T Recommendation X.1372 (2020), "Security guidelines for vehicle-to-everything (V2X) communications"
- ITU-R Recommendation M.2121-1, "Harmonization of frequency bands for Intelligent Transport Systems in the mobile service"
- ISO/SAE 21434:2021, "Road vehicles -Cybersecurity engineering"
- UNECE Regulation No. 155, "Cyber security and cyber security management system"
- UNECE Regulation No. 156, "Software update and software update management system"

NIST Publications

- FIPS 203 (2024), "Module-Lattice-Based Key-Encapsulation Mechanism Standard" (ML-KEM)
- FIPS 204 (2024), "Module-Lattice-Based Digital Signature Standard" (ML-DSA)

Indian Regulations and Documents

- The Telecommunications Act, 2023
- The Information Technology Act, 2000
- National Frequency Allocation Plan 2025 (NFAP-2025)
- Automotive Industry Standard 189 (AIS-189) on Cyber Security Management Systems
- Automotive Industry Standard 190 (AIS-190) on Software Update Management Systems
- TRAI Consultation Paper No. 08/2026 on the Regulatory Framework for Vehicle-to-Everything (V2X) Communication

- Report by the Committee on V2X/ITS Policy Formulation, dated 20 January 2023
- Report of the Task Force on Intelligent Transportation System for the use of 5.9 GHz, Part-1 (May 2025) and Final Report (January 2026)
- Telecommunication Engineering Centre Technical Report TEC 31218:2023 on Technologies and Standards for Intelligent Transport System

International Regulatory References

- FCC Second Report and Order on Use of the 5.850-5.925 GHz Band (FCC 24-123, November 2024)
- FCC First Report and Order on the 5.9 GHz Band (FCC 20-164, November 2020)
- European Directive 2010/40/EU on Intelligent Transport Systems framework
- European Directive (EU) 2023/2661 on Cooperative, Connected and Automated Mobility
- ISED Canada Decision on Technical and Policy Framework for Radio Local Area Network Devices in the 5850-5895 MHz Band and for Intelligent Transportation Systems in the 5895-5925 MHz Band (December 2022)

Industry Publications

- 5GAA, "A Visionary Roadmap for Advanced Driving Use Cases, Connectivity Technologies, and Radio Spectrum Needs" (September 2020)
- 5GAA, "Road Traffic Operation in a Digital Age: A Holistic Cross-Stakeholder Approach"
- US DOT V2X Deployment Plan (2023)