CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT

Comments on

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

Executive Summary :

As India stands at the threshold of a mobility revolution, the emergence of Vehicle-to-Everything (V2X) communication represents far more than a technological upgrade. It marks the beginning of a new era in which our roads, vehicles, infrastructure, and citizens are connected through a seamless digital fabric designed to save lives, reduce accidents, and create safer, smarter, and more efficient transportation systems. In this context, TRAI's consultation paper arrives at a pivotal moment. It provides the nation with an opportunity to craft a regulatory framework that is not only technologically sound but also deeply rooted in public welfare, consumer protection, and long-term national interest.

Across the world, countries that have embraced V2X early—such as the European Union, the United States, China, Korea, and Japan—have done so with a clear understanding that V2X is not merely a commercial service. It is a **public-safety infrastructure**, a **digital public good**, and a **national strategic asset**. Their regulatory models consistently prioritise safety,

interoperability, cybersecurity, and affordability. India, with its unique mobility patterns, dense traffic environments, and high road-fatality rates, has even greater reason to adopt a **Consumer-First, Safety-First** approach.

In shaping India's V2X ecosystem, the foremost consideration must be the citizen. Every regulatory decision—whether related to spectrum assignment, licensing, PKI, interoperability, testing, power limits, or AGR—must be guided by the principle that **no Indian citizen should be denied life-saving V2X services due to cost, geography, or OEM differences**. Safety messages must be universal, reliable, and free from commercial barriers. This is not merely a policy preference; it is a moral imperative.

The consultation paper rightly highlights the need for a robust spectrum framework. International experience shows that the 5.9 GHz ITS band is treated as a public-interest resource, assigned administratively and protected from harmful interference. India must follow a similar path, ensuring that spectrum for safety-critical V2X remains affordable, interference-free, and future-ready. Radiated power limits, OOBE thresholds, and coexistence conditions must be aligned with global standards such as ETSI EN 302 571 and China's C-V2X norms, while being adapted to India's unique propagation and density conditions.

Equally important is the establishment of a **National V2X Security and PKI Framework**. Trust is the foundation of V2X. Without strong authentication, pseudonymity, certificate management, and misbehaviour detection, the system cannot function safely. India must adopt a PKI architecture aligned with ETSI TS 103 097, ETSI TS 102 941, and IEEE 1609.2, anchored under CCA/MeitY with sectoral sub-CAs. Privacy must be protected through

pseudonym certificates and strict data-minimisation principles. Cybersecurity must be embedded at every layer—from hardware to firmware to application.

Interoperability is another cornerstone. India cannot afford a fragmented V2X ecosystem where devices from different OEMs or states fail to communicate. The higher-layer ITS stack must be standardised, ideally adopting the ETSI ITS model with India-specific adaptations. RSUs and OBUs must undergo mandatory testing and certification under MTCTE to ensure EMI/EMC compliance, cybersecurity robustness, and cross-vendor compatibility. A national interoperability profile—an "India ITS Profile"—should be developed to ensure uniformity across deployments.

On the economic and licensing front, the regulatory framework must recognise the **public-good nature of safety-related V2X services**. Revenue from safety applications should be excluded from AGR calculations. Spectrum charges, if any, should be nominal or waived entirely for safety-critical use. GR, ApGR, and AGR definitions must clearly distinguish between safety-related, operational, and commercial V2X revenue streams. This ensures that safety services remain affordable and universally accessible while maintaining transparency and accountability for commercial offerings.

India must also seize the opportunity to become a global leader in V2X manufacturing and innovation. With the right incentives—such as PLI schemes, standardised procurement, open APIs, and national testbeds—India can emerge as a major producer of RSUs, OBUs, chipsets, security modules, and edge-computing infrastructure. This aligns with the national

vision of **ATMANIRBHAR** Bharat and strengthens India's position in global supply chains.

The deployment of V2X infrastructure must be integrated with national and state-level initiatives. Smart Cities, NHAI highways, MoRTH road-safety programs, and public-transport systems must adopt V2X as a core component of their digital transformation. Priority should be given to high-risk intersections, school zones, industrial corridors, and accident-prone stretches. A coordinated governance structure involving DoT, TRAI, MoRTH, MeitY, BIS, state governments, and industry stakeholders is essential to ensure smooth implementation.

Ultimately, V2X is not just a technological upgrade—it is a nation-building initiative. With the right regulatory foundation, India can reduce road fatalities by 30–40% over the next decade, enable AI-driven traffic management, improve logistics efficiency, and create a trusted, secure, and privacy-preserving mobility ecosystem. The decisions we make today will shape the safety and mobility of future generations.

As the President of a Consumer Protection Association, I strongly support TRAI's initiative and urge that the final regulatory framework be **consumer-centric, safety-oriented, globally benchmarked, and future-ready**. India must adopt a model that accelerates deployment, ensures universal access, protects citizens, and fosters innovation. This consultation is not merely a regulatory exercise—it is an opportunity to redefine the future of mobility in India.

Precautions Needed to Protect Consumer Interest in the V2X Regulatory Framework

As India prepares to introduce V2X communication at a national scale, the most important responsibility of the regulatory framework is to **safeguard the consumer**—the driver, the pedestrian, the cyclist, the school-going child, the elderly citizen, and every road user who depends on safe mobility. V2X is not just a telecom service; it is a **life-saving public-safety infrastructure**, and therefore the regulatory design must incorporate strong, non-negotiable precautions to ensure that consumer rights, safety, privacy, and affordability are fully protected.

The first and most fundamental precaution is to ensure that **safety messages remain universal, reliable, and free from commercial barriers**. No citizen should ever be denied collision warnings, emergency braking alerts, or pedestrian safety notifications because of subscription fees, OEM restrictions, or device incompatibility. Safety-related V2X must be treated as a **public good**, not a premium feature. This requires clear separation between **safety services** and **commercial V2X services**, both in licensing and in revenue treatment.

A second precaution relates to **interoperability**. Consumers must not suffer because different manufacturers or states deploy incompatible systems. India must adopt a **single, harmonised ITS stack**, aligned with ETSI and 3GPP standards, ensuring that every RSU and OBU—regardless of brand—can communicate seamlessly. Interoperability failures can directly translate into safety failures, and therefore strict conformance testing, certification, and interoperability audits must be mandatory.

The third precaution concerns **cybersecurity and privacy**. V2X devices continuously broadcast information about vehicle position, speed,

direction, and events. Without strong safeguards, this data could be misused for surveillance, profiling, or malicious attacks. India must establish a **National V2X PKI**, with pseudonym certificates, misbehaviour detection, and strict data-minimisation rules. Consumers must be protected from cyber-attacks that could manipulate safety messages or compromise personal privacy.

Another essential precaution is **quality assurance through mandatory testing and certification**. RSUs and OBUs must undergo rigorous EMI/EMC, RF, safety, and cybersecurity testing under MTCTE. Sub-standard or uncertified devices can cause harmful interference, message loss, or system failure—directly endangering consumers. India must not allow low-quality imports or uncertified devices to enter the V2X ecosystem.

Affordability is also a critical consumer-protection concern. Spectrum charges, licence fees, and AGR treatment must be designed in a way that **does not increase the cost of V2X devices or services**. Safety-related V2X revenue should be excluded from AGR, and spectrum for safety applications should be assigned at **zero or nominal cost**. If the regulatory framework imposes heavy financial burdens on OEMs or RSU operators, those costs will ultimately be passed on to consumers, limiting adoption and undermining public safety.

A further precaution is the need for **transparent governance and accountability**. Consumers must know who is responsible for safety message integrity, PKI management, device certification, and system reliability. A multi-agency governance structure—DoT, TRAI, MoRTH, MeitY, BIS, and state governments—must work in coordination, with clear roles

and accountability mechanisms. Without this, consumers may face fragmented, inconsistent, or unsafe deployments.

Finally, the regulatory framework must include **grievance redressal and consumer-awareness mechanisms**. Consumers must have access to clear information about V2X features, safety benefits, device compatibility, and privacy protections. A national awareness campaign is essential to ensure that citizens understand how V2X works and how it protects them. A dedicated grievance mechanism must be established for reporting device failures, safety-message issues, or privacy concerns.

In summary, protecting consumer interest in V2X requires a **holistic set of precautions**—universal access to safety messages, strict interoperability, strong cybersecurity, mandatory certification, affordability safeguards, transparent governance, and consumer awareness. If these precautions are embedded into the regulatory framework from the beginning, India can build a V2X ecosystem that is not only technologically advanced but also **safe, equitable, and deeply aligned with the public interest**.

ISSUES FOR CONSULTATION :

Q1. Whether there is a need to introduce an authorisation for vehicle to-infrastructure (V2I) communication service under Section 3(1)(a) of the Telecommunications Act, 2023? If yes, please provide input with respect to the following aspects:

(a) Eligibility conditions for the authorisation;

(b) Period of validity of the authorisation and conditions for its renewal;

(c) Service area of the authorisation;

(d) Scope of service of the authorisation;

(e) Technical, operating, security related conditions etc. of the authorisation;

(f) Any other related aspect. Kindly provide a detailed response with justification.

Q2. In case your reply to Q1 is no, what should be the mechanism for enabling, facilitating and regulating vehicle-to-infrastructure (V2I) communication service in India? Kindly provide a detailed response with justification.

Q3. Any other suggestions relevant to the authorisation for vehicle to-infrastructure (V2I) communication service may be submitted with proper explanation and justification.

Q4. Whether a specific technology (such as LTE-based C-V2X, NR based C-V2X etc.) should be prescribed for the implementation of 132 C-V2X in India? If yes, which technology should be adopted for the implementation of C-V2X? If no, in what manner, the issues related to inter-operability between different technologies should be addressed? Kindly provide a detailed response with justification.

Comments :

India is facing a severe road safety challenge, with over 1.73 lakh fatalities annually, necessitating urgent deployment of Intelligent Transport Systems (ITS) enabled by Vehicle-to-Everything (V2X) communication. As highlighted

in the consultation paper, V2X enables real-time communication between vehicles, infrastructure, pedestrians, and networks, thereby significantly improving safety, efficiency, and traffic management outcomes.

In this context, while global momentum is shifting toward **Cellular V2X (C-V2X)** technologies, the ecosystem—particularly in India—remains in a transitional phase between LTE-based C-V2X (3GPP Rel-14/15) and NR-based C-V2X (Rel-16+). Prescribing a single technology at this stage would risk **premature lock-in, stranded investments, and reduced innovation flexibility**, especially given evolving standards and heterogeneous deployment conditions.

Accordingly, it is recommended that **TRAI should not prescribe a single specific technology at present**, but instead adopt a **technology-neutral regulatory framework** anchored in:

- Mandatory interoperability standards,
- Defined migration pathways,
- Spectrum harmonisation and coexistence conditions, and
- Strong certification and safety assurance mechanisms.

This approach balances **consumer safety (immediate deployment)** with **long-term technological evolution**, ensuring India avoids fragmentation while preserving flexibility.

Background and Public-Interest Considerations

India's transport ecosystem is at a critical inflection point. Rapid motorisation, urbanisation, and infrastructure expansion have increased both mobility and risk exposure. As noted in the consultation paper:

- Road accidents in India caused **1.73 lakh deaths and 4.63 lakh injuries in 2023**
- Nearly **92% of accidents are linked to human error**, which V2X can directly mitigate through cooperative awareness systems

V2X is not merely a telecom technology—it is a **public safety infrastructure**.

From a consumer protection standpoint, the regulatory objective must be:

1. **Maximising road safety benefits at the earliest**
2. Ensuring **affordable and scalable deployment**
3. Preventing **technology fragmentation**
4. Protecting consumers from **obsolete or incompatible systems**

Given that DoT has indicated **30 MHz in the 5.9 GHz band (5875–5905 MHz)** for initial deployment, with future expansion flexibility , regulatory decisions taken now will shape the ecosystem for decades.

Technology Options and Global Experience

Globally, three primary V2X technologies have evolved:

1. DSRC (IEEE 802.11p)

- Early deployments (USA, Europe, Japan)
- Limitations: scalability, interference, lack of evolution
- Gradually being phased out in favour of C-V2X

2. LTE-based C-V2X (3GPP Rel-14/15)

- Supports direct communication via PC5 interface

- Suitable for **basic safety applications**
- Mature ecosystem (chipsets, OEM integration)

3. NR-based C-V2X (3GPP Rel-16+)

- Designed for:
  - Ultra-low latency
  - High reliability
  - Advanced use cases (platooning, autonomous driving)
- Still evolving in ecosystem readiness

Global trend:

- **China**: LTE C-V2X deployment with migration path to NR
- **EU**: Hybrid and technology-neutral approach emerging
- **USA**: Transition from DSRC to C-V2X

The clear lesson is: **no country has locked itself prematurely into a single long-term technology without migration flexibility**.

Comparative Assessment: LTE-based C-V2X vs NR-based C-V2X

Technical Comparison

Parameter	LTE C-V2X	NR C-V2X
Standard	Rel-14/15	Rel-16+
Latency	Low	Ultra-low
Reliability	High	Very High
Use cases	Basic safety	Advanced/autonomous
Network dependence	Optional	Integrated with 5G

Economic and Ecosystem Considerations

- LTE C-V2X:
    - Mature chipset ecosystem
    - Lower cost of deployment
    - Immediate availability for mass deployment
- NR C-V2X:
    - Higher cost (currently)
    - Limited ecosystem maturity in India
    - Requires deeper 5G penetration

Consumer Impact

- LTE enables **immediate safety benefits**
- NR enables **future advanced safety and automation**

Conclusion:

LTE is **deployment-ready**, NR is **future-ready**

Recommendation on Prescribing a Specific Technology

It is strongly recommended that:

TRAI should NOT prescribe a single specific technology at this stage

Instead, TRAI should adopt a **technology-neutral, standards-driven framework** with the following principles:

1. **Allow both LTE-based and NR-based C-V2X deployments**
2. Mandate **interoperability at application and message layers**
3. Define a **forward-compatible migration roadmap**

4. Ensure **device-level upgradeability**

This approach ensures:

- **No vendor lock-in**
- **No stranded investments**
- **Faster rollout**
- **Future readiness**

Framework for Interoperability

1. Standardisation Framework

- Mandatory adherence to:
    - **3GPP standards (Rel-14 onwards)**
    - **ETSI ITS-G5 / CAM / DENM message sets**
    - Indian adaptation through:
        - **TEC**
        - **BIS ITS standards**
- Adoption of **common message layer interoperability** (CAM, DENM equivalents)

2. Device and RSU Requirements

- OBUs must support:
    - Minimum **LTE C-V2X PC5**
    - Software upgrade capability for NR
- RSUs must:
    - Be **multi-mode capable (LTE + NR ready)**
    - Support **over-the-air upgrades**

3. Conformance and Interoperability Testing

- Establish:
    - **National V2X Testbeds**
    - Mandatory **interoperability certification**
- Testing layers:
    - PHY/MAC layer compliance
    - Application-level message compatibility
    - Multi-vendor interoperability

4. Certification and Lab Ecosystem

- Create:
    - **India V2X Certification Authority**
    - Accredited labs under:
        - TEC
        - ARAI / ICAT collaboration
- Certification must be:
    - **Mandatory before deployment**
    - Periodically updated

5. Spectrum and Coexistence Conditions

Assumptions (India-appropriate):

- 30 MHz initial allocation (5875–5905 MHz)
- Shared ITS ecosystem

Recommendations:

- Define:

    - **Channelisation plan (10 MHz blocks)**
    - Power limits for OBUs/RSUs
    - Interference protection mechanisms
- Ensure coexistence with:
    - Future ITS technologies
    - Other services under NFAP

Consumer Protection and Safety Safeguards

From a consumer rights perspective, the following are critical:

1. Safety First Principle

- Mandatory deployment of **core safety applications**:
    - Collision warning
    - Emergency braking alerts
    - VRU protection

2. Interoperability Mandate

- Vehicles from different OEMs must communicate seamlessly

3. No Obsolescence Risk

- Devices must be:
    - Upgradeable
    - Backward compatible where feasible

4. Data Privacy and Security

- Mandatory:
    - End-to-end encryption

    - Anonymisation of user identity

5. Affordability

- Encourage:
    - Domestic manufacturing
    - Open standards
    - Competitive ecosystem

Implementation Roadmap and Timelines

Phase 1 (0–2 Years): Foundation Deployment

- LTE C-V2X rollout in priority corridors:
    - Highways
    - Urban accident hotspots
- Certification framework operational
- Core safety applications mandatory

Phase 2 (2–5 Years): Expansion and Hybridisation

- Multi-mode (LTE + NR) deployment
- RSU densification
- Integration with Smart Cities

Phase 3 (5–10 Years): Advanced ITS Ecosystem

- NR C-V2X dominance
- Autonomous driving use cases
- AI-driven traffic systems

Conclusion: Policy Outcome Alignment

This recommendation ensures:

Consumer Protection

- Immediate safety benefits
- No fragmentation or incompatibility

Avoidance of Lock-in

- No premature technology commitment
- Flexible evolution path

Make in India

- Open ecosystem encourages domestic manufacturing
- Standardisation enables local innovation

Future-proofing

- Seamless migration from LTE to NR
- Compatibility with evolving 3GPP standards

In essence, India must avoid the mistake of **choosing a technology too early** in a rapidly evolving domain. A **technology-neutral but standards-enforced approach** is the most balanced, consumer-centric, and future-ready regulatory path.

Q5. Whether there is a need to bring road-side units (RSUs) and on board units (OBUs) under the regime of Mandatory Testing Certification of Telecom Equipment (MTCTE)? If no, in what manner, Electromagnetic

Interference (EMI), Electromagnetic Compatibility (EMC), safety, technical and security requirements prescribed by TEC/ DoT may be ensured? Kindly provide a detailed response with justification.

Comments :

The deployment of Vehicle-to-Everything (V2X) communication infrastructure in India represents a critical public-safety intervention, directly impacting road users, pedestrians, and transport systems at large. Roadside Units (RSUs) and On-Board Units (OBUs) form the foundational communication layer of this ecosystem, enabling real-time exchange of safety-critical information. Given their role in collision avoidance, traffic management, and protection of vulnerable road users, any failure, interference, or security compromise in these devices can have immediate and severe consequences for public safety.

In this context, it is recommended that **RSUs and OBUs should be brought under the Mandatory Testing Certification of Telecom Equipment (MTCTE) framework**, with clearly defined, V2X-specific Essential Requirements notified by TEC. However, such inclusion must be implemented through a **phased and calibrated approach**, ensuring that safety and interoperability are not compromised while avoiding excessive compliance burdens on industry stakeholders, particularly domestic manufacturers and start-ups.

This approach ensures that India establishes a **robust, trusted, and interoperable V2X ecosystem**, aligned with public interest, while simultaneously supporting **innovation, Make in India, and timely deployment** of life-saving technologies.

Background and Regulatory Context

The MTCTE framework, established under the Indian Telegraph (Amendment) Rules, mandates that notified telecom equipment must undergo testing and certification against Essential Requirements (ERs) prescribed by the Telecommunication Engineering Centre (TEC) prior to sale, import, or use in India.

The objectives of MTCTE include:

- Ensuring **network integrity and safety**
- Preventing **harmful electromagnetic interference**
- Enforcing **security and lawful interception capabilities**
- Protecting **end-users and public infrastructure**

RSUs and OBUs, though part of the transport ecosystem, function as **radio communication devices operating in licensed/shared spectrum bands (notably 5.9 GHz)** and directly interface with telecom networks and other connected devices. Therefore, they fall squarely within the broader definition of **telecom equipment impacting public networks and safety systems**.

Given this, regulatory oversight through MTCTE becomes both **legally consistent and functionally necessary**.

Role and Criticality of RSUs and OBUs in V2X/ITS Ecosystem

RSUs and OBUs are not passive devices; they are **active, safety-critical communication nodes**.

- **RSUs (Roadside Units)**:

    - Installed on highways, intersections, and urban corridors
    - Broadcast safety alerts (e.g., red-light violation warnings, accident alerts)
    - Interface with traffic management systems and cloud platforms
- **OBUs (On-Board Units)**:
    - Installed in vehicles
    - Receive and transmit real-time data (speed, position, hazard alerts)
    - Enable collision avoidance and driver assistance systems

Their combined operation enables:

- **Vehicle-to-Vehicle (V2V) safety**
- **Vehicle-to-Infrastructure (V2I) coordination**
- **Vehicle-to-Pedestrian (V2P) protection**
- **Vehicle-to-Network (V2N) integration**

Any malfunction, interference, or inconsistency in these devices can lead to:

- False alerts or missed warnings
- Increased accident risk
- System-wide communication failure

Thus, RSUs and OBUs must be treated as **critical public safety infrastructure**, not merely consumer electronics.

Risk Assessment

1. EMI/EMC Risks

- Interference with:
    - Adjacent ITS channels
    - Wi-Fi (5 GHz band proximity)
    - Other safety-critical communication systems
- Risk of **communication breakdown in dense urban environments**

2. Electrical and RF Safety

- Exposure risks due to continuous RF transmission
- Faulty hardware leading to:
    - Device overheating
    - Electrical hazards

3. Technical Robustness

- Packet loss, latency variation, synchronization issues
- Impact on **real-time safety decisions**

4. Cyber-Security Risks

- Spoofing of safety messages
- Unauthorized access to vehicle systems
- Large-scale coordinated attacks (e.g., traffic disruption)

5. Consumer Impact

- Loss of trust in safety systems
- Financial burden due to faulty devices
- Direct threat to life and property

Analysis of Bringing RSUs/OBUs under MTCTE

Benefits

1. Enhanced Safety Assurance

- Certified compliance with EMI/EMC, RF exposure, and electrical safety norms
- Reduction in risk of device-induced accidents

2. Standardisation and Interoperability

- Uniform Essential Requirements ensure:
    - Multi-vendor compatibility
    - Seamless communication across OEMs

3. Cyber-Security Strengthening

- Mandatory security testing
- Protection against malicious attacks

4. Consumer Protection

- Assurance of minimum quality standards
- Accountability of manufacturers and importers

5. Market Discipline

- Prevention of sub-standard imports
- Promotion of trusted supply chains

Challenges

1. Compliance Cost

- Testing and certification expenses
- Impact on start-ups and MSMEs

2. Time-to-Market Delays

- Certification timelines may slow deployment

3. Lab Capacity Constraints

- Limited availability of V2X-specific testing infrastructure in India

4. Technology Evolution

- Rapid changes in 3GPP standards may outpace rigid certification norms

Recommendation

Adopt a Phased MTCTE Inclusion Framework

RSUs and OBUs should be brought under MTCTE with **graded and phased implementation**, as follows:

1. Scope of Coverage

Phase 1 (Mandatory MTCTE)

- RSUs deployed on:
    - National highways
    - Urban intersections
    - Public transport corridors
- OBUs used in:
    - Commercial vehicles

- Public transport fleets
- Government ITS deployments

Phase 2 (Extended Coverage)

- All OBUs in private vehicles
- Aftermarket devices

2. Essential Requirements (ERs) for V2X Devices

TEC should notify **V2X-specific ERs**, including:

a. EMI/EMC

- Compliance with:
  - ETSI EN standards (adapted for India)
  - Coexistence with adjacent band services

b. RF Performance

- Power limits, spectral masks, channel access mechanisms

c. Electrical Safety

- Protection against overheating, voltage fluctuations

d. Cyber-Security

- Secure boot, encryption, authentication protocols
- Protection against spoofing and replay attacks

e. Interoperability

- Compliance with 3GPP message formats (CAM/DENM equivalent)

3. Phasing and Relaxations

- Initial **self-certification + provisional approval** for 12–18 months
- Transition to **full MTCTE certification**
- Fast-track approvals for:
    - Start-ups
    - Domestic manufacturers

4. Coordination with Other Standards

- Alignment with:
    - **BIS** (safety and quality standards)
    - **MoRTH / AIS** (automotive integration)
    - **ARAI / ICAT** (vehicle-level validation)

Consumer Protection and Public-Safety Safeguards

To ensure public interest:

1. **Mandatory Certification Labelling**
    - Consumers must identify certified devices easily
2. **Recall and Liability Framework**
    - Mandatory recall for defective devices
    - Manufacturer liability for safety failures
3. **Cyber-Security Compliance**
    - Periodic updates and patching requirements
4. **Grievance Redressal Mechanism**
    - Dedicated complaint system for V2X device failures

Implementation Roadmap

0–6 Months

- TEC to:
    - Define V2X ERs
    - Identify testing parameters
- TRAI/DoT to notify regulatory framework

6–18 Months

- Establish:
    - Accredited testing labs
    - Certification processes
- Begin Phase 1 MTCTE compliance

18–36 Months

- Expand to Phase 2 coverage
- Full enforcement with penalties

Beyond 36 Months

- Continuous update of ERs aligned with:
    - 3GPP evolution
    - Emerging ITS use cases

Conclusion

Bringing RSUs and OBUs under MTCTE is not merely a regulatory formality; it is a **public safety imperative**. However, the approach must be **phased, flexible, and innovation-friendly**.

This recommendation:

- **Protects consumers and road users** by ensuring only certified, safe devices are deployed
- **Prevents unsafe and sub-standard equipment** from entering the ecosystem
- **Balances compliance burden with industry growth**, especially for domestic players
- **Supports Make in India** through a predictable and standards-driven framework
- Ensures **long-term interoperability, security, and technological evolution**

A carefully designed MTCTE framework for V2X will ensure that India builds a **safe, resilient, and future-ready intelligent transport ecosystem**.

Q6. To ensure inter-operability among different RSUs/ OBUs, whether there is a need to standardize the layered communication framework (stack) for higher layers (other than the access layer in which C-V2X will be used) of Intelligent Transportation System (ITS)? If yes, which standard for ITS stack and security should be adopted? Specifically, whether the ETSI standard for ITS stack and security, as recommended by the Task Force on Intelligent Transportation System for the use of 5.9 GHz (mentioned at para 3.5 of this consultation paper) should be adopted? If no, in what manner, inter-operability among different RSUs/ OBUs can be ensured? Kindly provide a detailed response with justification.

Comments :

The success of Vehicle-to-Everything (V2X) deployment in India critically depends on **inter-operability across RSUs and OBUs**, particularly at the higher layers of the communication stack where safety messages, applications, and security frameworks operate. While access layer harmonisation through Cellular V2X (C-V2X) provides a common radio interface, lack of standardisation at higher layers can lead to fragmentation, incompatibility, and compromised safety outcomes. In a country facing a significant road safety burden, such risks are unacceptable.

In this context, it is strongly recommended that **India should adopt a standardized higher-layer ITS communication stack**, specifically **ETSI ITS stack with its associated security framework**, while allowing controlled flexibility for non-safety and value-added applications above the facilities layer. This represents a **hybrid approach (Option B)** that balances interoperability, innovation, and long-term scalability.

Adopting ETSI ITS standards for safety-critical communication ensures **global alignment, proven interoperability, and mature security mechanisms**, while flexibility at upper layers supports **Make in India, innovation, and OEM differentiation**. This approach avoids fragmentation and ensures that India builds a **safe, secure, and future-proof ITS ecosystem**.

Background and Importance of Higher-Layer Standardization

V2X communication operates across multiple layers:

- **Access Layer**: Radio communication (e.g., C-V2X via PC5 interface)

- **Network & Transport Layers**
- **Facilities Layer**: Message formats (CAM, DENM)
- **Application Layer**: Safety and mobility services
- **Security Layer**: Authentication, encryption, trust management

While India is converging on **C-V2X at the access layer**, the **higher layers remain undefined**. This creates a critical risk:

- Different OEMs may implement **proprietary message formats**
- RSUs and OBUs may fail to **interpret safety messages correctly**
- Cross-state and cross-vendor deployments may become **non-functional**

Given that V2X is a **life-saving system**, interoperability cannot be optional—it must be **mandated at the protocol level**.

Global ITS Stack Models and Their Relevance to India

1. ETSI ITS-G5 Stack (Europe)

- Widely adopted in Europe
- Layered architecture:
    - Access: IEEE 802.11p / evolving to C-V2X
    - Facilities: CAM (Cooperative Awareness Message), DENM (Decentralized Environmental Notification Message)
    - Security: ETSI TS 103 097
- Mature PKI-based trust model

2. IEEE 1609 WAVE Stack (USA)

- DSRC-based architecture

- Includes:
    - IEEE 1609.2 (security)
    - IEEE 1609.3 (networking)
- Less aligned with C-V2X evolution

3. 3GPP-based Architecture

- Focuses primarily on:
    - Access layer (PC5, Uu)
    - Lower-layer communication
- Does not fully define:
    - Application-layer message sets
    - Complete security trust frameworks

Relevance to India

- India is adopting **C-V2X access layer**
- Requires **higher-layer standardization independent of radio technology**
- ETSI stack is **technology-agnostic at upper layers**, making it ideal

Comparative Analysis

ETSI ITS vs IEEE 1609 vs 3GPP Application Layer

Parameter	ETSI ITS Stack	IEEE 1609	3GPP
Access independence	Yes	Limited	Yes
Message standardization	Strong (CAM, DENM)	Moderate	Limited
Security framework	Mature (TS 103 097)	Mature	Partial
Global adoption	High (EU, hybrid regions)	Declining	Complementary

Parameter	ETSI ITS Stack	IEEE 1609	3GPP
Compatibility with C-V2X	High	Low	Native

Conclusion

- ETSI provides:
    - **Complete higher-layer stack**
    - **Proven interoperability**
    - **Strong security architecture**

Interoperability Challenges Without Standardization

If higher-layer standardization is not mandated:

1. **Vendor Fragmentation**
    - OEM-specific protocols
    - RSU-OBU incompatibility
2. **Safety Risks**
    - Misinterpretation of alerts
    - Delayed or failed warnings
3. **State-Level Silos**
    - Different ITS implementations across states
    - Lack of national interoperability
4. **Stranded Investments**
    - Infrastructure becomes obsolete
    - Retrofitting costs increase
5. **Consumer Harm**
    - Loss of trust in V2X systems
    - Reduced safety benefits

Recommendation

Adopt a Hybrid Standardization Approach (ETSI-based Core Framework)

India should:

1. Mandate ETSI ITS Stack for Safety-Critical Layers

- Facilities Layer:
  - CAM (Cooperative Awareness Messages)
  - DENM (Event Notification Messages)
- Networking & Transport:
  - ETSI GeoNetworking protocols
- Security:
  - ETSI TS 103 097

2. Allow Flexibility Above Facilities Layer

- OEMs may innovate in:
  - Infotainment services
  - Fleet management
  - Advanced analytics
- Provided:
  - They do not interfere with **core safety message interoperability**

3. Ensure Backward and Forward Compatibility

- Support coexistence with:
  - LTE C-V2X (Rel-14/15)
  - NR-V2X (Rel-16+)

4. Define National Interoperability Profile

- India-specific adaptation of ETSI stack
- Standard message dictionary for Indian road conditions

Security Framework Recommendation

Adopt ETSI Security Framework with National PKI

Key Components

1. **ETSI TS 103 097 Compliance**
    - Message signing
    - Certificate-based authentication
2. **National V2X Public Key Infrastructure (PKI)**

- Assumption:
    - Operated under a **trusted government or regulated entity** (e.g., CCA/DoT-authorized body)
- Functions:
    - Certificate issuance
    - Revocation management
    - Trust chain maintenance

3. **Misbehavior Detection System**
    - Identification of malicious or faulty nodes
4. **Privacy Protection**
    - Pseudonym certificates
    - User anonymity safeguards

Consumer Protection and Safety Implications

This recommendation directly benefits consumers:

1. Guaranteed Interoperability

- Vehicles from different manufacturers can communicate seamlessly

2. Enhanced Road Safety

- Reliable, real-time safety alerts
- Reduced accident probability

3. Protection from Vendor Lock-in

- Open standards prevent proprietary ecosystems

4. Trustworthy Ecosystem

- Certified, secure communication framework

5. Long-Term Affordability

- Avoidance of costly upgrades due to incompatible systems

Implementation Roadmap for India

Phase 1 (0–2 Years): Standard Adoption and Pilot

- Notify:
    - ETSI ITS stack as national standard
- Establish:
    - National ITS standards body coordination (TEC, BIS, MoRTH)
- Pilot deployments:
    - Highways and urban corridors

Phase 2 (2–5 Years): Scale and Certification

- Mandatory compliance for:
  - RSUs
  - OBUs
- Establish:
  - Conformance testing labs
  - Certification framework

Phase 3 (5–10 Years): Advanced Integration

- Integration with:
  - NR-V2X
  - Autonomous vehicle systems
- Continuous update of standards

Conclusion

Standardization of the higher-layer ITS stack is not merely a technical choice—it is a **public safety necessity**.

By adopting an **ETSI-based hybrid framework**, India can:

- Ensure **interoperability across vendors and regions**
- Enhance **road safety and consumer protection**
- Avoid **fragmentation and stranded investments**
- Promote **Make in India and innovation**
- Build a **scalable, future-ready ITS ecosystem**

A fragmented approach at this stage would irreversibly compromise the effectiveness of V2X deployment. A **standards-driven, security-first, and**

interoperable framework is therefore the most prudent regulatory path forward.

Q7. Whether there is a need for prescribing a security framework for ITS/ C-V2X in India? If yes, (a) What should be the security framework for ITS/ C-V2X? (b) Which agency [such as Controller of Certifying 133 Authorities (CCA), Ministry of Electronics & Information Technology (MeitY)] should implement the Public Key Infrastructure (PKI) framework for ITS/ C-V2X in India? (c) How to ensure coexistence of V2X PKI certificates with the legacy PKI mechanism in India i.e. based on X.509, operated by Root Certifying Authority of India (RCAI)? Please provide a detailed response with justifications.

Comments :

India should prescribe a **dedicated security and PKI framework for ITS/C-V2X**. V2X is a safety-critical communication system where a spoofed, delayed, modified, or unauthenticated message may directly affect life, limb, public trust, and traffic discipline. Therefore, security cannot be left to voluntary industry practice or proprietary arrangements.

The recommended approach is to adopt a **dedicated Indian V2X Trust Framework**, aligned with **ETSI TS 103 097, ETSI TS 102 941, and IEEE 1609.2 principles**, with suitable adaptation to India's existing PKI ecosystem, data protection requirements, and sectoral governance needs. The framework should provide authentication, integrity, privacy-preserving pseudonymity, certificate lifecycle management, misbehavior detection, revocation, audit, and secure software-update obligations.

For institutional arrangement, the **Controller of Certifying Authorities (CCA)** should be the primary trust and policy authority for the V2X PKI framework, with **MeitY as the nodal policy ministry**, and with sectoral coordination by **DoT, TEC, MoRTH, NIC, NHAI, State Transport Departments, ARAI/ICAT, and BIS**. The preferable model is a **dedicated National ITS/V2X Root of Trust under the regulatory oversight of CCA**, logically separated from ordinary citizen/business X.509 digital signature certificates but capable of coexistence with India's legacy RCAI framework through defined trust-anchor, certificate-policy, audit, and bridging arrangements. The consultation paper itself records that ETSI and IEEE security frameworks are PKI-based, that India's existing CCA framework recognises X.509, and that a harmonised approach based on ETSI TS 102 941 with CCA-led standardisation is recommended by the Task Force.

Background: Why a Security Framework for ITS/C-V2X is Essential

ITS/C-V2X is not merely a connectivity service. It is an operational safety layer for roads, highways, traffic systems, public transport, emergency response, freight corridors, pedestrians, cyclists, and two-wheelers. In V2X, vehicles and roadside infrastructure exchange real-time safety information such as hazard warnings, emergency braking alerts, red-light violation warnings, work-zone alerts, collision risk notifications, and vulnerable road user protection messages.

In such a system, security failure is not limited to data loss. It can result in physical harm. A false emergency braking message, fake congestion alert, spoofed RSU, compromised OBU, replayed certificate, or maliciously injected hazard warning may mislead drivers, automated systems, traffic

controllers, and emergency services. Therefore, the security framework must be prescribed at the national level before large-scale deployment.

A national framework is also necessary because V2X deployments will involve multiple stakeholders: automotive OEMs, telecom service providers, RSU vendors, highway authorities, State transport authorities, smart city agencies, fleet operators, start-ups, and imported device suppliers. Without a common trust model, one State's RSU may not be trusted by another State's vehicles, one OEM's OBU may reject another vendor's safety message, and consumers may face fragmented and unreliable safety services.

Global Reference Models for V2X Security and PKI

Globally, V2X security frameworks converge around the following principles:

1. **PKI-based trust**
2. **Digitally signed safety messages**
3. **Short-lived pseudonym certificates**
4. **Separation of enrolment identity and operational authorization**
5. **Misbehavior detection and revocation**
6. **Privacy protection against vehicle tracking**
7. **Interoperable certificate and message formats**

The major global models are:

ETSI Model

The European framework is primarily based on **ETSI TS 102 941** for trust and privacy management and **ETSI TS 103 097** for secure message formats and certificate structures. It uses a trust model involving enrolment authorities, authorization authorities, trust lists, pseudonym certificates, and lifecycle management. The consultation paper notes that the European Union follows an ETSI-based trust framework with pseudonym-based authorization tickets, certificate lifecycle management, misbehavior detection, and revocation.

IEEE 1609.2 / SCMS Model

The United States has used a Security Credential Management System approach, based on distributed PKI, enrolment certificate authorities, authorization certificate authorities, privacy-preserving pseudonym certificates, and misbehavior detection. The consultation paper notes that the US SCMS model distributes trust across multiple entities so that no single entity can easily link a vehicle's real identity with its communications.

China and Korea Models

China has adopted a sovereign, centralized V2X security architecture aligned with national C-V2X policy, while retaining core elements such as pseudonym certificates and message authentication. South Korea also uses PKI-based V2X security aligned with IEEE 1609.2 principles.

The global lesson is clear: **V2X deployment requires a dedicated trust architecture and cannot rely only on ordinary website-style or enterprise-style PKI.**

Need for a Prescribed Security Framework in India

India should prescribe a security framework for ITS/C-V2X for the following reasons.

First, V2X will operate in a safety-critical environment. Trust, authentication, and message integrity must be assured before vehicles and infrastructure act upon received messages.

Second, India's V2X ecosystem will be multi-vendor and multi-jurisdictional. A vehicle moving from Gujarat to Rajasthan, Maharashtra, Delhi, Tamil Nadu, or Assam must not lose trust in RSUs merely because different agencies or vendors installed them.

Third, consumer privacy must be protected. V2X safety messages may reveal location, speed, direction, vehicle type, and movement patterns. Without pseudonymity and data-minimisation safeguards, V2X can become a mass vehicle-tracking infrastructure.

Fourth, India must avoid fragmented proprietary security systems. Fragmentation will increase costs, create lock-in, reduce Make in India opportunities, and leave consumers dependent on closed vendor ecosystems.

Fifth, existing Indian PKI is primarily X.509-based, whereas V2X PKI frameworks under ETSI/IEEE are based on specific vehicular certificate formats and trust models. The consultation paper specifically notes this incompatibility and the need for a coexistence or bridged framework.

Recommended Security Framework for ITS/C-V2X

India should adopt a **dedicated V2X Security and Trust Framework** based on recognised international V2X security standards, adapted to Indian legal and operational requirements.

Reference Standards

The framework should be based on:

1. **ETSI TS 103 097** for secure message formats, certificate formats, digital signatures, and secured V2X communication.
2. **ETSI TS 102 941** for trust, privacy, certificate lifecycle, enrolment, authorization, and security management.
3. **IEEE 1609.2 principles** for secure vehicular communications, especially where compatibility with global vehicle platforms is required.
4. Indian adoption through **TEC, BIS, TSDSI, CCA, and MoRTH-designated automotive testing agencies**.

This approach is consistent with the Task Force recommendation that security services should follow a harmonised approach based on ETSI TS 102 941, derived from IEEE 1609.2, with CCA as the competent authority for national security framework implementation.

Core Security Services

The Indian framework should mandate the following security services:

Authenticity

Every safety message transmitted by an RSU or OBU should be digitally signed so that the receiver can verify that it originates from a trusted device.

Integrity

Messages must be protected from alteration. Any modified or tampered message should be rejected automatically.

Authorization

Devices should be allowed to transmit only those message types and services for which they are certified and authorized.

Privacy and Pseudonymity

Vehicles should not continuously broadcast permanent identities. Operational communication should use short-lived pseudonym certificates to prevent long-term tracking.

Confidentiality Where Required

Most safety broadcasts may not require encryption because they are meant for nearby receivers. However, confidentiality must be required for backend communication, certificate provisioning, diagnostic interfaces, software updates, user-linked services, and lawfully restricted information.

Non-repudiation with Controlled Disclosure

The framework should protect privacy during ordinary operation but allow identity resolution only through lawful, audited, and proportionate procedures in cases of serious accident investigation, cyberattack, fraud, or national security.

Certificate Types

India should adopt a layered certificate model:

1. **Root Certificate / Trust Anchor**
   This should represent the highest trust authority for the Indian V2X ecosystem.
2. **Enrolment Certificates**
   These should bind a certified device to the V2X ecosystem without exposing its identity in every safety message.
3. **Authorization Certificates / Pseudonym Certificates**
   These should be used for regular V2X safety communication. They should be short-lived and rotated periodically.
4. **RSU Certificates**
   RSUs should have separate certificate profiles because they are fixed infrastructure and may be subject to authorization, location binding, and audit requirements.
5. **Manufacturer / OEM Certificates**
   OEMs and equipment manufacturers should be certified for device provisioning, secure manufacturing, and lifecycle management.
6. **Service Provider Certificates**
   Entities operating V2X backends, traffic platforms, or certificate provisioning services should require separate authorization and audit.

Misbehaviour Detection and Revocation

A security framework without misbehaviour detection is incomplete. India should mandate:

1. Reporting of suspicious or conflicting messages.
2. Automated detection of abnormal patterns.

3. Blacklisting of compromised devices.
4. Certificate revocation lists or equivalent scalable revocation mechanisms.
5. Emergency revocation for compromised RSUs.
6. Periodic audit of misbehaviour reports.
7. Protection against false reporting and malicious blacklisting.

Misbehaviour management should be coordinated nationally because a compromised device may travel across State borders.

Privacy Safeguards and Data Minimisation

The framework should provide that:

1. V2X safety messages shall not contain personally identifiable information unless strictly necessary.
2. Persistent identifiers should not be broadcast in ordinary operation.
3. Pseudonym certificates should be rotated frequently.
4. Linkage between pseudonym certificates and real identity should be held only under legally controlled conditions.
5. Data retention periods should be defined.
6. Access to identity-resolution records should require lawful authorization and audit.
7. Commercial profiling based on V2X safety messages should be prohibited without explicit legal basis and user consent.

Recommended Institutional Arrangement for PKI

Role of CCA

The **Controller of Certifying Authorities** should be the principal trust-policy authority for V2X PKI in India because:

1. CCA already has statutory experience in certifying authorities and trust infrastructure.
2. The question of coexistence with India's existing X.509/RCAI framework directly falls within the domain of national PKI governance.
3. A safety-critical V2X PKI requires national-level trust, audit, licensing, and policy discipline.

Role of MeitY

MeitY should act as the nodal policy ministry for digital trust, cyber security, and alignment with India's digital governance and data protection framework. MeitY should coordinate with CCA, CERT-In, and relevant cyber security bodies.

Role of DoT and TEC

DoT and TEC should prescribe and certify the telecom and radio-related security requirements for RSUs/OBUs, including secure communication interfaces, device identity, secure firmware, lawful technical compliance, and MTCTE-related requirements.

Role of MoRTH and Automotive Agencies

MoRTH, ARAI, ICAT, NHAI, State Transport Departments, and smart-city agencies should define deployment, vehicle integration, road-safety use cases, and operational rules. Vehicle-level approval and safety validation should remain aligned with automotive regulatory systems.

Recommended Model

India should establish a **National V2X Trust Authority** under the oversight of **CCA/MeitY**, with sectoral participation from DoT, TEC, MoRTH, NIC, NHAI, CERT-In, ARAI/ICAT, BIS, TSDSI, State transport authorities, and consumer representatives.

The preferred structure should be:

1. **National ITS/V2X Root of Trust**
   Established or authorised under CCA oversight.
2. **Enrolment Certificate Authorities**
   Licensed or accredited entities issuing enrolment credentials to certified RSUs and OBUs.
3. **Authorization Certificate Authorities**
   Entities issuing pseudonym/authorization certificates for operational V2X messages.
4. **Misbehavior Authority**
   A national or federated authority responsible for detection, reporting, investigation, and revocation.
5. **Policy Authority**
   A multi-stakeholder authority defining certificate policy, privacy policy, revocation policy, audit requirements, and cross-border interoperability.

This model balances sovereign control, technical interoperability, privacy, and scalability.

Coexistence with Legacy X.509 PKI Operated by RCAI

The coexistence challenge is real because India's legacy PKI is X.509-based, while V2X security standards under ETSI/IEEE use vehicular certificate structures derived from IEEE 1609.2. The consultation paper correctly notes that direct incorporation is not straightforward due to incompatibility between certificate formats and trust models.

Therefore, India should adopt **logical coexistence, not forced merger**.

Technical Coexistence

The following approach is recommended:

1. The V2X PKI should maintain its own certificate profiles suitable for vehicular communication.
2. RCAI/CCA should remain the sovereign trust anchor or supervisory anchor.
3. The V2X Root should be either:
    - a dedicated National ITS Root CA under CCA oversight, or
    - an ITS Root whose trust is anchored or countersigned through the existing national PKI framework.
4. Certificate policies should clearly define the relationship between:
    - RCAI/X.509 hierarchy,
    - V2X Root of Trust,
    - enrolment authorities,
    - authorization authorities,
    - and misbehaviour/revocation authorities.
5. Trust lists should be published and updated in machine-readable form for RSUs and OBUs.

Logical Separation

Traditional X.509 identity certificates should not be used directly for routine V2X broadcast safety messages because that would create privacy and tracking risks. V2X pseudonym certificates must be logically separated from ordinary identity certificates.

The framework should ensure that:

1. A vehicle's legal identity is not exposed in ordinary V2X messages.
2. Pseudonym certificates are unlinkable by ordinary receivers.
3. Only authorised authorities can resolve identity under defined legal procedure.
4. RSU certificates may have stronger location and operator binding because RSUs are fixed infrastructure.
5. OEM and backend certificates may use X.509 where appropriate for server-to-server, provisioning, and enterprise interfaces.

Migration and Interoperability

During pilot phases, India should permit internationally compliant V2X PKI implementations, provided they are onboarded into the Indian trust framework through recognised trust lists and controlled testing. Over time, all public-road deployments should transition to the national V2X trust framework.

Consumer Protection and Public-Interest Considerations

A prescribed security framework is essential for consumer protection.

It protects road users by preventing:

1. **Spoofed emergency warnings**
2. **False accident alerts**
3. **Fake RSUs**
4. **Replay attacks**
5. **Vehicle tracking**
6. **Unauthorized surveillance**
7. **Malicious traffic disruption**
8. **Compromised aftermarket devices**
9. **Non-certified imports**
10. **Fragmented vendor-controlled trust systems**

The framework should also include consumer-facing safeguards:

1. Certified V2X equipment should carry clear compliance marking.
2. Vehicle owners should receive security updates during the supported life of the vehicle.
3. OEMs should disclose minimum security-support periods.
4. Consumers should not be forced into proprietary paid safety services for core road-safety functions.
5. Safety-related V2X functions should continue to operate across brands, States, and operators.
6. Failure of a V2X security update due to manufacturer negligence should attract recall and liability.
7. Data collected through V2X safety systems should not be used for unrelated commercial profiling.

Implementation Roadmap and Phased Adoption

Phase 1: Policy and Standards Notification

Within 6 months:

1. TRAI should recommend a dedicated ITS/C-V2X security framework.
2. MeitY/CCA should initiate the national V2X PKI policy.
3. TEC, BIS, TSDSI, and MoRTH should jointly identify Indian adoption of ETSI TS 103 097, ETSI TS 102 941, and relevant IEEE 1609.2 principles.
4. A national working group should include consumer representatives.

Phase 2: Pilot Trust Infrastructure

Within 6 to 18 months:

1. Establish a pilot National V2X Root of Trust.
2. Issue trial enrolment and authorization certificates.
3. Test RSU/OBU interoperability in controlled environments.
4. Run pilots on selected highways, urban corridors, and accident-prone zones.
5. Test revocation, misbehaviour detection, certificate rotation, and privacy safeguards.

The Task Force itself recommended pilot testing before large-scale rollout and deployment in high-priority zones such as metropolitan cities, highways, and accident-prone areas.

Phase 3: Mandatory Certification for Public-Road Deployment

Within 18 to 36 months:

1. All RSUs deployed on public roads should use certificates issued under the Indian V2X trust framework.

2. OBUs in public transport, commercial vehicles, emergency vehicles, and government fleets should be brought under mandatory compliance first.
3. MTCTE and automotive certification should include V2X security conformance.
4. Misbehaviour reporting and revocation should become operational.

Phase 4: National Scale and Continuous Improvement

Beyond 36 months:

1. Extend compliance to private vehicles and aftermarket OBUs.
2. Periodically update cryptographic algorithms and certificate policies.
3. Integrate with NR-V2X evolution.
4. Maintain cross-border and global interoperability where needed.
5. Conduct annual public security audits and incident transparency reporting.

Conclusion

India should prescribe a **dedicated, legally backed, privacy-preserving, and globally aligned security framework for ITS/C-V2X**. The framework should be based on ETSI TS 103 097, ETSI TS 102 941, and IEEE 1609.2 principles, adapted to Indian law, Indian PKI governance, and Indian road-safety priorities.

The **CCA, under MeitY's policy oversight**, should lead the PKI trust framework, while DoT/TEC should handle telecom equipment security compliance and MoRTH should manage transport-sector operational integration. The best approach is to create a **dedicated National ITS/V2X**

Root of Trust under CCA oversight, with carefully designed coexistence with India's RCAI/X.509 legacy PKI.

This model protects road users from cyber and safety risks, preserves privacy through pseudonym certificates, enables lawful accountability where required, avoids vendor lock-in, supports Make in India, and ensures that India's V2X ecosystem develops as a secure, interoperable, scalable, and consumer-protective national infrastructure.

Q8. What should be the regulatory framework for the assignment of frequency spectrum to the entities holding the proposed V2I communication service authorisation? Specifically,

(a) Whether there is a need for partitioning the 30 MHz spectrum (5,875-5,905 MHz) for specific applications such as "safety applications" and "operational applications (non-safety applications)"?

Comments :

India should adopt a **hybrid spectrum partitioning approach** for the 30 MHz band (5875–5905 MHz), wherein a **minimum guaranteed portion of the band is reserved exclusively for safety-critical V2X applications**, while the remaining spectrum is made available for controlled, priority-aware use by non-safety and value-added applications. This approach ensures that **life-saving safety communications are insulated from congestion and interference**, while still enabling innovation and efficient spectrum utilisation.

The proposed model balances three critical objectives: first, **ultra-reliable, low-latency communication for safety applications**, which must never be compromised; second, **efficient spectrum use and innovation** for non-safety services; and
third, **future scalability toward NR-V2X and advanced ITS use cases**.

From a consumer protection perspective, the hybrid model is the most prudent approach because it **guarantees spectrum availability for safety messaging under all traffic conditions**, prevents misuse of safety channels by commercial applications, and aligns with global best practices while being tailored to India's dense and heterogeneous traffic environment.

Background: Importance of Spectrum for V2I Safety and Reliability

V2I communication relies on **deterministic, low-latency, and highly reliable spectrum access**. Unlike conventional telecom services, V2X safety messages:

- Are **broadcast in real-time**
- Require **latency below 100 ms (often much lower)**
- Must be **received by all relevant nearby vehicles simultaneously**
- Cannot tolerate congestion or packet loss

In India's context—characterised by:

- High traffic density
- Mixed vehicle classes (2-wheelers, heavy vehicles, pedestrians)
- High accident rates

—the spectrum must be treated as **critical public-safety infrastructure**, not merely a shared communications resource.

Global Regulatory Models for 5.9 GHz ITS Spectrum

European Union (ETSI Model)

- Uses **channelised approach within ITS band**
- Dedicated channels for:
    - Safety (CAM/DENM)
    - Service/operational applications
- Strong prioritisation mechanisms

United States (FCC Model)

- Reduced ITS allocation to 30 MHz
- Emphasis on **C-V2X with channel segmentation**
- Coexistence with Wi-Fi in adjacent bands

China

- Fully aligned with **C-V2X**
- Spectrum prioritisation for **safety-critical services**
- Centralised planning and deployment

Korea/Japan

- Hybrid models with:
    - Safety prioritisation
    - Controlled use for non-safety services

Key Global Insight:

All mature ecosystems ensure that **safety communication is either isolated or strictly prioritised** within the ITS spectrum.

Technical Considerations

1. Latency and Reliability

- Safety messages require:
  - Ultra-low latency
  - High reliability (>99.9%)

2. Congestion and Channel Load

- High vehicle density leads to:
  - Channel congestion
  - Message collision risk

3. PC5 Sidelink Behavior (3GPP)

- Uses:
  - Distributed resource allocation
  - Sensing-based semi-persistent scheduling
- Performance degrades under high load without prioritisation

4. Interference Risks

- Cross-channel interference
- Adjacent-band interference (e.g., Wi-Fi)

5. QoS Differentiation

- Safety vs non-safety traffic must be:
    - Differentiated
    - Prioritised

Assessment of Partitioning the 30 MHz Band

Benefits of Partitioning

1. **Guaranteed Spectrum for Safety**
    - No competition from non-safety traffic
    - Predictable performance
2. **Reduced Congestion**
    - Safety messages isolated from infotainment traffic
3. **Simplified QoS Enforcement**
    - Clear separation of traffic types
4. **Enhanced Consumer Safety**
    - Reliable delivery of life-saving messages

Risks of Partitioning

1. **Underutilisation Risk**
    - Safety band may remain underused in low-traffic scenarios
2. **Rigid Allocation**
    - Less flexibility for evolving use cases
3. **Inefficient Spectrum Use (if static)**

Benefits of Unified Band

1. **Maximum Flexibility**
2. **Efficient utilisation**

3. **Simplified spectrum planning**

Risks of Unified Band

1. **Safety Message Degradation**
    - Competing traffic may delay critical alerts
2. **QoS Enforcement Complexity**
3. **Higher Risk of Congestion Collapse**
4. **Potential misuse by commercial applications**

Recommended Regulatory Framework (Hybrid Approach)

Proposed Spectrum Structure (30 MHz)

Assumption: 10 MHz channelisation blocks

1. Dedicated Safety Block

- **20 MHz reserved exclusively for safety-critical V2X communication**
- Use cases:
    - Collision avoidance
    - Emergency braking
    - VRU alerts
    - Hazard warnings

2. Shared/Operational Block

- **10 MHz for non-safety applications**
- Use cases:
    - Traffic efficiency

- Infotainment
- Fleet management
- Software updates (non-critical)

Guard Bands and Technical Rules

- Minimum **guard band of 5 MHz** (logical or physical depending on channelisation)
- Strict **power and emission masks**
- Channel access rules aligned with 3GPP PC5

QoS and Priority Rules

Even within safety band:

- **Priority hierarchy**:
  1. Emergency alerts
  2. Collision warnings
  3. Routine awareness messages
- Mandatory:
  - Congestion control algorithms
  - Message rate adaptation

Dynamic Flexibility Provision

- Under low-load conditions:
  - Controlled, temporary use of unused safety spectrum for non-safety traffic
- Subject to:
  - Automatic pre-emption by safety traffic

- Real-time monitoring

Assignment Mechanism for V2I Service Authorisation Holders

Recommended Model: Administrative Assignment with Controlled Access

1. Nature of Assignment

- **Non-auctioned, administrative assignment**
- Based on:
  - Public safety mandate
  - Infrastructure deployment obligations

2. Eligible Entities

- Government agencies
- Highway authorities (e.g., NHAI)
- Smart city SPVs
- Authorised infrastructure providers

3. Key Obligations

Entities must:

1. **Prioritise safety applications**
2. Ensure **interoperability compliance**
3. Adhere to **security and PKI framework**
4. Maintain **network performance benchmarks**
5. Avoid misuse of safety spectrum

4. Compliance and Monitoring

- Mandatory:
    - Real-time spectrum monitoring
    - Periodic audits
- Enforcement:
    - Penalties for misuse
    - Revocation of authorization

Consumer Protection and Public-Interest Safeguards

The proposed framework ensures:

1. Protection of Road Users

- Guaranteed delivery of safety messages

2. Protection of Vulnerable Groups

- Pedestrians, cyclists, and two-wheelers benefit from reliable alerts

3. Prevention of Spectrum Misuse

- Commercial traffic cannot crowd out safety communication

4. Cross-Vendor Interoperability

- Uniform spectrum usage rules

5. Trust in ITS Systems

- Reliable and predictable system behavior

Implementation Roadmap

Phase 1 (0–2 Years): Pilot and Standardisation

- Define:
  - Spectrum partitioning rules
  - QoS parameters
- Pilot deployment:
  - Highways and metro cities

Phase 2 (2–5 Years): Controlled Expansion

- Mandatory compliance for:
  - RSUs
  - OBUs
- Deployment across:
  - National highways
  - Smart cities

Phase 3 (5–10 Years): Advanced ITS Integration

- Migration toward:
  - NR-V2X
- Dynamic spectrum optimisation
- AI-based congestion management

Conclusion

A **hybrid spectrum partitioning model** is the most balanced and consumer-centric approach for India.

It:

- **Protects road users and vulnerable populations** by guaranteeing safety spectrum
- Ensures **reliable delivery of safety messages under all conditions**
- Prevents **harmful interference and congestion collapse**
- Supports **innovation in non-safety applications**
- Aligns with **global best practices while adapting to Indian realities**

In a country with high traffic density and safety challenges, **spectrum must be treated as a life-saving resource**, and its allocation must reflect that priority.

(b) In case more than one authorised entity has to operate in the same geographical area, what should be the mechanism for simultaneous use of the spectrum? Specifically, whether the spectrum should be divided amongst the authorised entities in an exclusive manner, or should the authorised entities utilize the spectrum in a shared manner?

Comments : No Comments.

(c) If your response to part (b) is "in an exclusive manner", what should be the minimum quantity of spectrum to be assigned to each entity holding the proposed V2I communication service authorisation? If your response to part (b) is "in a shared manner", whether there is a need to prescribe a mechanism for interference management?

Comments : No Comments.

(d) For interference management, whether there is a need to prescribe – (i) minimum directionality of road-side unit (RSU), or (ii) protection

distance between the RSUs, or (iii) maximum antenna height for RSUs? If yes, what should be such parameter(s)?

Comments : No Comments.

(e) Whether there is need to mandate a mechanism for obtaining prior approval (analogous to SACFA clearance) for the establishment of RSUs by the entities holding the proposed V2I communication service authorisation? If no, in what manner, the establishment of RSUs should be regulated?

Comments : No Comments.

(f) For avoiding (i) interference between RSUs, (ii) interference between RSUs and OBUs, and (iii) interference between OBUs, whether the radiated power limits for OBUs and RSUs and OOBE limits, recommended by the Task Force on Intelligent Transportation System for the use of 5.9 GHz (mentioned at para 3.4 of this consultation paper) should be adopted? If no, what should be the radiated power limits for OBUs and RSUs and OOBE limits?

Comments :

India should adopt the Task Force's recommended radiated power and out-of-band emission limits for RSUs and OBUs, but with **carefully calibrated modifications to suit Indian traffic density, urban morphology, and coexistence conditions**. A uniform adoption without contextual adjustment may lead to either underperformance in dense urban environments or excessive interference in high-density traffic scenarios. Therefore, a **modified adoption approach (Option B)** is recommended.

The proposed framework should maintain alignment with global standards such as ETSI EN 302 571 and 3GPP C-V2X guidelines, while introducing **context-sensitive power limits, stricter OOBE controls, and adaptive transmission mechanisms**. This ensures that safety-critical communication achieves **reliable coverage without causing congestion or harmful interference**, particularly in India's mixed and high-density traffic conditions.

From a consumer protection perspective, appropriate power and OOBE limits are essential to ensure that **safety messages are reliably received without degradation**, while preventing spectrum misuse, interference with adjacent services, and system instability. The recommended approach therefore balances **coverage, reliability, and interference mitigation**, which are fundamental to public safety.

Background: Why Power and OOBE Limits Matter for V2X Safety and Reliability

In V2X communication, radiated power and spectral emissions directly influence:

- **Communication range**
- **Packet delivery reliability**
- **Interference levels**
- **Spectrum efficiency**

Unlike traditional telecom systems, V2X operates in a **broadcast, peer-to-peer environment** where:

- Multiple transmitters operate simultaneously

- Messages are exchanged without central coordination (PC5 sidelink)
- Safety messages must reach all nearby receivers instantly

If power levels are too high:

- Interference increases
- Channel congestion worsens
- Message collisions rise

If power levels are too low:

- Safety messages may not reach critical recipients
- Coverage gaps emerge

Similarly, inadequate OOBE limits can:

- Interfere with adjacent channels
- Impact coexistence with other services (e.g., Wi-Fi)
- Degrade overall system performance

Therefore, **power and OOBE limits are fundamental safety parameters**, not merely technical constraints.

Global Benchmarks for RSU/OBU Power and OOBE Limits

ETSI EN 302 571 (Europe)

- OBU EIRP: up to ~23 dBm
- RSU EIRP: up to ~33 dBm
- Strict OOBE masks for adjacent band protection
- Dynamic power control encouraged

United States (FCC legacy ITS)

- RSU higher power for infrastructure coverage
- Emphasis on interference containment

China (C-V2X)

- RSU EIRP: higher than OBUs for extended coverage
- Tight control on spectral emissions

Korea/Japan

- Balanced approach:
  - Moderate power levels
  - Strong coexistence mechanisms

Global Insight:

All jurisdictions maintain **higher power for RSUs than OBUs**, combined with **strict OOBE and interference control mechanisms**.

Technical Analysis of Interference Scenarios

1. RSU-RSU Interference

Occurs in:

- Urban intersections
- Highway corridors with dense RSU deployment

Risks:

- Overlapping coverage zones
- Signal saturation

- Reduced decoding reliability

Mitigation need:

- Controlled RSU power levels
- Directional antennas
- Proper spacing

2. RSU-OBU Interference

Occurs when:

- High-power RSU transmissions overwhelm OBUs
- OBUs experience near-far problem

Risks:

- Receiver desensitization
- Missed safety messages from other OBUs

Mitigation need:

- Balanced RSU power
- Adaptive transmission

3. OBU-OBU Interference

Occurs in:

- Traffic congestion
- Intersections
- Platooning scenarios

Risks:

- Channel congestion
- Packet collisions
- Message loss

Mitigation need:

- Power control
- Congestion control algorithms

Assessment of Task Force Recommendations

Strengths

1. **Alignment with global standards**
2. Provides baseline for:
    - EIRP
    - PSD
    - OOBE limits
3. Ensures initial harmonisation
4. Facilitates early deployment

Limitations

1. May not fully account for:
    - India’s extreme traffic density
    - Mixed mobility patterns (2-wheelers, pedestrians)
2. Uniform limits may:
    - Overpower dense urban environments
    - Underperform in highways

3. OOBE limits may require tightening due to:
    - Adjacent band usage (Wi-Fi, future services)

Alignment with Global Standards

- Broadly consistent with ETSI and 3GPP
- Requires **contextual tuning for India**

Recommended Regulatory Framework (Modified Adoption)

Assumptions

- 10 MHz channelisation
- Mixed urban and highway deployment
- Coexistence with adjacent band services

1. Recommended Radiated Power Limits

OBUs

- **Maximum EIRP: 23 dBm**
- **Adaptive range: 10–23 dBm**
- Mandatory:
    - Dynamic power control
    - Congestion-based adjustment

RSUs

- **Urban deployment: up to 30 dBm EIRP**
- **Highway deployment: up to 33 dBm EIRP**
- Mandatory:
    - Directional antennas

- Site-specific optimisation

2. Power Spectral Density (PSD)

- Defined per MHz basis
- Must ensure:
  - Uniform channel usage
  - Avoidance of spectral spikes

3. OOBE Limits

- Adopt ETSI baseline with **stricter Indian profile**

Recommendations:

- Enhanced attenuation at band edges
- Additional protection for:
  - Adjacent ITS channels
  - Unlicensed bands (Wi-Fi)

4. Antenna Gain Limits

- RSUs:
  - Controlled gain with directional focus
- OBUs:
  - Omnidirectional with capped gain

Additional Interference-Mitigation Measures

1. Congestion Control

- Mandatory algorithms:

    - Message rate control
    - Transmission interval adjustment

2. Sensing-Based Power Adaptation

- Based on:
    - Channel load
    - Vehicle density

3. Channelization and Guard Bands

- Logical separation of channels
- Guard bands to reduce interference

4. RSU Siting Guidelines

- Minimum spacing norms
- Height and orientation specifications
- Avoid overlapping high-power zones

5. Certification and Compliance

- Mandatory testing under:
    - MTCTE / TEC framework
- Periodic field validation

Consumer Protection and Public-Interest Considerations

The recommended framework ensures:

1. Reliable Safety Messaging

- Adequate range without interference

2. Protection from Congestion

- Prevents message loss in dense traffic

3. Fair Spectrum Use

- Prevents misuse by high-power transmissions

4. Protection of Vulnerable Road Users

- Ensures alerts reach all participants

5. Cross-Vendor Interoperability

- Standardised power behavior

6. Long-Term System Stability

- Prevents degradation over time

Implementation Roadmap

Phase 1 (0–2 Years): Baseline Adoption

- Adopt Task Force limits with modifications
- Pilot testing in:
    - Urban areas
    - Highways

Phase 2 (2–5 Years): Optimization

- Refine limits based on field data
- Enforce adaptive power control

Phase 3 (5–10 Years): Advanced Evolution

- Integrate with NR-V2X
- AI-based interference management

Conclusion

India should adopt the Task Force's power and OOBE limits **with calibrated modifications tailored to Indian conditions**.

This approach:

- **Ensures reliable safety communication**
- **Prevents harmful interference**
- **Supports dense urban deployments**
- **Protects consumers and road users**
- **Aligns with global best practices while remaining India-specific**

In a high-density and safety-critical environment like India, **precision in power control is essential to save lives**, and regulatory design must reflect that priority.

(g) What should be the maximum period of assignment of spectrum to the entities holding the proposed V2I communication service authorisation?

Comments : No Comments.

(h) Whether there is a need to prescribe roll-out obligations associated with the assignment of spectrum to the entities holding the proposed V2I communication service authorisation?

(i) Whether there is a need to introduce a provision for the surrender of frequency spectrum? Kindly provide a detailed response with justification.

Comments : No Comments.

Q9. Whether there is a need for prescribing timelines for processing the applications for the assignment of spectrum to the entities holding the proposed V2I communication service authorisation? Kindly provide a detailed response with justification.

Q10. Whether there are any other suggestions related to assignment of spectrum to the entities holding the proposed V2I communication service authorisation? Please provide a detailed response with justification.

Q11. Any other issues/ suggestions relevant to the regulatory framework for V2X communication may be submitted with proper explanation and justification.

Comments :

India should treat V2X communication as a **national public-safety digital infrastructure**, not merely as a telecom service or automotive feature. The consultation paper itself recognises that V2X enables vehicles to communicate with other vehicles, infrastructure, vulnerable road users, and networks, and that such communication is central to improving road safety and traffic efficiency in India. It also notes India's severe road-safety burden and the relevance of ITS for safer, smarter transport.

In addition to spectrum assignment, authorization, technology choice, and security standards, TRAI should recommend a **comprehensive national V2X regulatory architecture** covering governance, PKI, cybersecurity operations, certification, spectrum enforcement, data protection, state-level deployment, Make-in-India manufacturing, funding models, and consumer awareness. Without such a broader framework, India may face fragmented deployments, vendor lock-in, unsafe devices, non-interoperable RSUs/OBUs, privacy risks, and weak enforcement.

Therefore, it is respectfully submitted that India should adopt a **nationally coordinated, standards-based, security-first and consumer-centric V2X framework**, jointly implemented by DoT, TRAI, MoRTH, MeitY, TEC, BIS, CCA, NHAI, State Governments, automotive testing agencies, and industry stakeholders.

National V2X Governance Architecture

Problem Statement

V2X lies at the intersection of telecom, transport, cybersecurity, automotive safety, spectrum management, data governance, and urban infrastructure. If each department or State adopts its own model, India may face fragmented deployments.

Proposed Solution

A **National V2X Coordination Council** should be created with representation from:

- DoT

- TRAI
- MoRTH
- MeitY
- TEC
- BIS
- CCA
- NHAI
- State Transport Departments
- Smart City authorities
- ARAI/ICAT
- Consumer organisations

Justification

This will ensure:

- Uniform national policy
- Cross-State interoperability
- Coordinated spectrum use
- Consumer safety
- Accountability of vendors and operators

National PKI and Misbehavior Detection System

Problem Statement

A compromised or fake RSU/OBU can broadcast false safety messages, causing accidents or public panic.

Proposed Solution

India should establish a **National V2X PKI and Misbehavior Detection Framework** with:

- National trust anchor
- Pseudonym certificates
- RSU/OBU authentication
- Certificate revocation
- Misbehavior reporting
- Secure audit trails

Justification

This protects road users from spoofed messages, fake infrastructure, and cyber attacks while preserving privacy through pseudonymous certificates.

National ITS Security Operations Centre

Problem Statement

V2X will be exposed to cyber threats such as spoofing, replay attacks, jamming, malware, and compromised roadside infrastructure.

Proposed Solution

A dedicated **National ITS Security Operations Centre (ITS-SOC)** should monitor:

- V2X cyber incidents
- Compromised RSUs
- Certificate misuse
- Jamming attempts

- Large-scale abnormal message patterns

Justification

Global V2X deployments increasingly recognise that certification alone is insufficient; real-time monitoring is necessary for safety-critical infrastructure.

Certification, Testing and Compliance Ecosystem

Problem Statement

Unsafe or non-compliant devices may enter the market if testing and certification are weak.

Proposed Solution

India should establish accredited V2X testing laboratories for:

- RF testing
- EMI/EMC testing
- Security testing
- Interoperability testing
- Field-performance testing
- Multi-vendor RSU/OBU validation

Justification

This will prevent low-quality imports, support Make in India, and ensure that vehicles from different OEMs communicate reliably.

Spectrum Monitoring and Enforcement

Problem Statement

The 5.9 GHz band will carry safety-critical messages. Interference, unauthorized use, or misuse may directly affect road safety.

Proposed Solution

DoT/WPC should create a dedicated **5.9 GHz ITS spectrum monitoring framework** with:

- Automated monitoring stations
- RSU registration database
- Field inspection powers
- Penalties for harmful interference
- Mandatory shutdown of non-compliant equipment

Justification

Spectrum used for safety must be protected with stronger enforcement than ordinary commercial spectrum.

Interoperability and Standardization Roadmap

Problem Statement

Multiple standards such as ETSI, IEEE, and 3GPP may create confusion if India does not adopt a national interoperability profile.

Proposed Solution

India should notify an **Indian V2X Interoperability Profile** covering:

- C-V2X access layer

- Higher-layer message formats
- Security framework
- PKI rules
- Application priorities
- RSU/OBU certification profiles

Justification

This prevents vendor lock-in and ensures that V2X systems work across States, vehicle brands, highways, and smart cities.

Integration with 5G and Future 6G Networks

Problem Statement

V2X will evolve beyond direct safety messaging into advanced mobility, autonomous transport, edge analytics, and emergency response systems.

Proposed Solution

The regulatory framework should support:

- 5G network slicing for transport safety
- Mobile edge computing near highways and urban corridors
- QoS-based V2N services
- Future migration to NR-V2X and 6G-enabled mobility

Justification

This ensures long-term scalability and avoids repeated infrastructure replacement.

Data Governance, Privacy and Consumer Protection

Problem Statement

V2X data may reveal location, movement, speed, driving behaviour, route history, and vehicle identity.

Proposed Solution

TRAI should recommend strict data-governance safeguards:

- Data minimization
- Pseudonymity
- Purpose limitation
- Consent for non-safety uses
- Prohibition on commercial profiling without lawful basis
- Clear retention limits
- User grievance redressal

Justification

Consumers should not be forced to sacrifice privacy in the name of safety.

Make in India and Domestic Manufacturing

Problem Statement

India may become dependent on imported RSUs, OBUs, chipsets, and security modules if domestic capability is not promoted.

Proposed Solution

The Government should promote:

- Domestic RSU/OBU manufacturing
- Indian V2X chip design
- Trusted supply chains
- PLI-style incentives
- Common testbeds for start-ups
- Open standards-based procurement

Justification

This will reduce cost, improve security, create jobs, and build strategic capability.

State-Level Deployment Models

Problem Statement

India has diverse road environments: highways, city intersections, rural roads, ports, industrial corridors, hill roads, and smart cities.

Proposed Solution

Deployment should be phased as:

1. Accident-prone highway corridors
2. Urban intersections and red-light zones
3. Public transport and emergency vehicles
4. Freight corridors and logistics hubs
5. Two-wheeler and pedestrian-heavy zones

Justification

This ensures that limited public resources are first used where consumer-safety benefits are highest.

Public Awareness and Capacity Building

Problem Statement

Drivers may ignore warnings or misunderstand V2X alerts if they are not educated.

Proposed Solution

A national awareness programme should be launched for:

- Drivers
- Fleet operators
- Traffic police
- State transport officers
- Emergency services
- Vehicle dealers
- OEM service centres

Justification

Technology alone cannot save lives unless users understand and trust it.

Funding and PPP Models

Problem Statement

Large-scale RSU deployment will require significant investment.

Proposed Solution

India should adopt mixed funding models:

- Public funding for safety-critical corridors
- PPP for highways and smart cities
- Viability-gap funding for rural and accident-prone zones
- Mandatory V2X integration in future expressway projects
- CSR support for road-safety pilots

Justification

Safety-critical V2X should not be delayed due to commercial uncertainty.

Final Recommendation

TRAI should recommend that India's V2X regulatory framework must go beyond spectrum assignment and include a **national, interoperable, secure, privacy-preserving, consumer-protective, and future-ready ecosystem framework**.

Such a framework will:

- Protect road users and vulnerable groups
- Prevent unsafe and fragmented deployments
- Ensure interoperability across vendors and States
- Support Make in India and innovation
- Safeguard privacy and cybersecurity
- Build long-term trust in India's intelligent transport systems

V2X should be regulated as a **public-interest safety infrastructure**, with consumer protection at the centre of every regulatory decision.

Q12. In view of the public welfare-oriented nature of V2X applications and the need to encourage the deployment of such infrastructure and services, should there be spectrum charges levied on spectrum assigned to the V2I communication service authorised entities under the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

Comments :

It is strongly recommended that **no spectrum charges should be levied for V2I communication service authorisation**, and that spectrum in the 5.9 GHz band for V2X applications should be assigned on an **administrative, charge-free basis**. V2X is not a commercial telecom service; it is a **life-saving, public-interest safety infrastructure** designed to reduce road fatalities, protect vulnerable road users, and improve traffic efficiency. Imposing spectrum charges would create unnecessary financial barriers and delay deployment, thereby directly undermining public welfare.

Global regulatory experience clearly demonstrates that ITS spectrum is treated as a **public good**, not a revenue-generating asset. Jurisdictions such as the European Union, the United States, China, Japan, and Korea have adopted **administrative allocation models without auction-based pricing**, recognising that the societal benefits of V2X far outweigh any potential spectrum revenue.

From a consumer protection perspective, imposing spectrum charges would lead to **slower rollout, uneven regional deployment, higher vehicle costs, and reduced safety coverage**, ultimately affecting road users

across India. Therefore, a **zero-charge administrative assignment model**, combined with strong compliance and utilisation safeguards, is the most appropriate regulatory approach.

Background: V2X as a Public-Safety and National-Priority Service

V2X communication is fundamentally different from traditional telecom services. It is designed to:

- Prevent road accidents
- Enable collision avoidance
- Protect pedestrians, cyclists, and two-wheeler users
- Support emergency response systems
- Improve traffic efficiency and reduce congestion

India faces one of the highest road fatality rates globally. In such a context, V2X must be treated as:

- A **public safety infrastructure**, comparable to traffic signals or road signage
- A **national priority intervention**, aligned with road safety and smart mobility goals
- A **non-commercial service**, where benefits accrue to society at large

Spectrum used for V2X is therefore not a tradable commodity but a **public resource for saving lives**.

Global Regulatory Practices for ITS Spectrum Charging

Across major global jurisdictions, a consistent policy approach is observed:

European Union

- ITS-G5 spectrum allocated administratively
- No auction or recurring spectrum usage charges
- Emphasis on interoperability and safety

United States

- 5.9 GHz ITS spectrum allocated for public safety
- No commercial auction model applied
- Focus on enabling V2X deployment

China

- Centralised allocation for C-V2X
- State-supported deployment
- No commercial spectrum pricing

Japan and Korea

- Administrative allocation
- Public-interest driven deployment

Key Global Insight:

No major jurisdiction treats V2X spectrum as a revenue-generating asset. Instead, it is treated as a **public-good resource**.

Economic Rationale for Zero Spectrum Charges

1. Positive Externalities

V2X generates significant societal benefits:

- Reduction in road accidents and fatalities
- Lower healthcare and emergency response costs
- Reduced traffic congestion
- Lower fuel consumption and emissions

These benefits far exceed any potential revenue from spectrum charges.

2. Public-Good Characteristics

V2X exhibits characteristics of a public good:

- Non-excludable (safety benefits extend to all road users)
- Non-rivalrous (one user's benefit does not reduce another's)

3. Market Failure Consideration

Private entities may underinvest in V2X infrastructure due to:

- High upfront costs
- Long payback periods
- Indirect monetisation

Therefore, regulatory intervention is required to remove cost barriers.

Impact of Spectrum Charges

1. Deployment Cost

- Increased cost of RSU deployment
- Higher infrastructure investment burden
- Delayed rollout in cost-sensitive regions

2. RSU Rollout

- Reduced deployment in rural and semi-urban areas
- Concentration in high-revenue urban zones
- Uneven national coverage

3. OEM Adoption

- Increased cost of OBUs
- Reduced integration in entry-level vehicles
- Slower penetration across vehicle segments

4. State Government Participation

- Financial constraints may limit participation
- Reduced investment in public safety infrastructure

5. Consumer Safety

- Reduced coverage leads to:
    - Inconsistent safety alerts
    - Lower effectiveness of V2X systems
    - Increased risk for road users

Recommended Regulatory Model

Zero Spectrum Charge Model (Preferred)

Key Features

1. **Administrative Assignment**
    - Spectrum allocated without auction
    - Based on eligibility and deployment commitments
2. **No Spectrum Usage Charges**

- No upfront or recurring fees

3. **Public-Safety Mandate**
    - Spectrum use restricted primarily to safety and ITS applications

Justification

- Removes financial barriers
- Encourages rapid deployment
- Ensures equitable access across regions
- Aligns with global best practices
- Maximises public welfare

Safeguards for Efficient Spectrum Use

Even without spectrum charges, efficiency must be ensured through:

1. Strict Usage Conditions

- Spectrum limited to authorised V2X applications
- Prohibition of commercial misuse

2. Deployment Obligations

- Minimum RSU deployment targets
- Coverage requirements for highways and urban areas

3. Performance Standards

- QoS requirements for safety messaging
- Latency and reliability benchmarks

4. Monitoring and Enforcement

- Spectrum monitoring by DoT/WPC
- Penalties for non-compliance

5. Periodic Review

- Assessment of utilisation levels
- Reallocation if underutilised

Consumer Protection and Public-Interest Benefits

The proposed model ensures:

1. Faster Deployment

- No financial barriers for infrastructure rollout

2. Universal Safety Coverage

- Equal access across urban and rural areas

3. Affordable Vehicles

- Lower cost of OBUs
- Wider adoption across income segments

4. Protection of Vulnerable Road Users

- Reliable alerts for pedestrians, cyclists, and two-wheelers

5. Increased Public Trust

- Consistent and reliable V2X performance

Implementation Roadmap

Phase 1 (0–2 Years): Policy Adoption

- Notify zero-charge administrative assignment
- Define eligibility and usage conditions

Phase 2 (2–5 Years): Expansion

- Large-scale RSU deployment
- Integration with vehicle ecosystem

Phase 3 (5–10 Years): Optimization

- Continuous monitoring
- Performance-based adjustments
- Integration with advanced ITS systems

Conclusion

Spectrum for V2X must be treated as a **public safety resource**, not a revenue-generating asset.

A **zero spectrum charge administrative assignment model**:

- **Accelerates V2X deployment**
- **Maximises road safety benefits**
- **Avoids cost barriers for industry and governments**
- **Ensures equitable access across India**
- **Aligns with global best practices**

In the Indian context, where road safety is a national challenge, any delay in V2X deployment due to financial constraints would have direct human costs. Therefore, regulatory policy must prioritise **life over revenue**,

ensuring that spectrum serves its highest public purpose—**saving lives on the road**.

Q13. If answer to Q12 is affirmative, whether the spectrum charges for the V2I communication service authorised entities under the proposed V2I communication service authorisation should be determined based on the spectrum charging methodology prescribed by the Department of Telecommunications (DoT) vide its order dated 11.12.2023? If yes, then which of the radiocommunication services specified in the said order, should be taken as basis for calculation of spectrum Charges? Please provide detailed justification in support of your response.

Comments :

It is respectfully submitted that the **DoT spectrum charging methodology dated 11.12.2023 should not be applied to V2I communication services in its conventional form**, as V2I is fundamentally a **public-safety, non-commercial, and welfare-oriented infrastructure**. The application of commercial or quasi-commercial spectrum pricing frameworks—such as those applicable to PMRTS, captive networks, or backhaul—would be inconsistent with the core objective of V2X, which is to **save lives and enhance public safety**.

Accordingly, it is recommended that **V2I communication services should be exempted from standard spectrum charging methodologies and instead be governed by a zero-charge or, at most, nominal administrative fee model**. If TRAI considers it necessary to anchor V2I within the DoT framework, the closest technical analogy would be **short-**

range radiocommunication devices, but even in that case, charges should be minimal or waived for safety-critical applications.

This approach ensures that **deployment is accelerated, costs are minimised, and equitable access is maintained across regions**, while aligning with global best practices where ITS spectrum is treated as a **public good rather than a revenue-generating resource**.

Background: V2I as a Public-Safety and National-Priority Service

Vehicle-to-Infrastructure communication forms the backbone of intelligent transport systems by enabling:

- Real-time safety alerts (collision warnings, red-light violations)
- Traffic management coordination
- Emergency response facilitation
- Protection of vulnerable road users

Unlike commercial telecom services, V2I does not generate direct revenue streams. Instead, it delivers:

- Reduction in road fatalities
- Lower healthcare burden
- Reduced congestion and emissions
- Improved mobility efficiency

Therefore, V2I must be treated as:

- A **public-safety infrastructure**, similar to traffic signals
- A **national strategic asset**, not a commercial service
- A **social investment**, not a revenue source

Overview of DoT's Spectrum Charging Methodology (11.12.2023)

The DoT charging framework provides methodologies for various radiocommunication services, including:

- Public Mobile Radio Trunking Services (PMRTS)
- Captive Wireless Private Networks (CWPN)
- Microwave backhaul links
- Satellite communication services
- Short-range devices (SRDs)
- Other licensed services

These categories are designed primarily for:

- Commercial use
- Enterprise/private network deployment
- Revenue-generating services
- Controlled and predictable usage patterns

The methodology typically considers:

- Spectrum bandwidth
- Geographic area
- Usage type
- Revenue potential or enterprise utility

Assessment of Applicability to V2I

1. Technical Fit

V2I differs significantly from all categories under the DoT framework:

- It operates as a **broadcast, safety-critical system**
- It uses **decentralised communication (PC5 sidelink)**
- It involves **mass-scale deployment across vehicles and infrastructure**
- It is not tied to a specific operator or enterprise

Thus, no existing category fully aligns with V2I.

2. Economic Implications

Applying DoT methodology would result in:

- Increased deployment costs for RSUs
- Higher cost of OBUs for OEMs
- Reduced participation by State Governments
- Slower infrastructure rollout

Given that V2X benefits are largely societal, such costs cannot be easily recovered.

3. Public-Interest Considerations

Charging spectrum fees for V2I would:

- Create **barriers to deployment**
- Lead to **uneven geographic coverage**
- Reduce **effectiveness of safety systems**
- Undermine **consumer protection objectives**

This is contrary to TRAI's mandate of maximising public welfare.

Assessment of Radiocommunication Categories

Closest Category: Short-Range Devices (SRDs)

If a classification is required within the DoT framework, V2I most closely resembles:

- Short-range radiocommunication devices

Justification

- Localised communication range
- Non-commercial usage
- Shared spectrum environment
- Public utility function

However, even SRD classification is imperfect because:

- V2I involves safety-critical messaging
- Requires higher reliability and coordination
- Involves infrastructure (RSUs), not just devices

Recommended Regulatory Model

Primary Recommendation: Zero-Charge Model

Key Features

1. **No Spectrum Charges**
    - No upfront or recurring fees
2. **Administrative Assignment**
    - Based on eligibility and deployment commitments
3. **Public-Safety Mandate**
    - Use restricted to ITS and safety applications

Alternative (If Charges Are Considered): Nominal Administrative Fee

- Minimal fee to cover:
    - Regulatory processing
    - Spectrum management costs
- No linkage to:
    - Revenue
    - Bandwidth usage
    - Geographic scale

Conditional Model (Fallback Option)

- **Zero charges for safety applications**
- **Minimal charges for non-safety applications**, if permitted

Consumer Protection and Safety Implications

The recommended approach ensures:

1. Faster Deployment

- Eliminates financial barriers
- Encourages rapid RSU rollout

2. Universal Coverage

- Enables deployment in:
    - Rural areas
    - High-risk zones
    - Low-revenue regions

3. Affordable Vehicles

- Reduces cost burden on OEMs
- Promotes mass adoption

4. Reliable Safety Messaging

- Ensures consistent system performance

5. Equity Across Regions

- Prevents concentration in urban areas only

Implementation Roadmap

Phase 1 (0–2 Years): Policy Adoption

- Exempt V2I from DoT charging methodology
- Notify administrative assignment model

Phase 2 (2–5 Years): Deployment Expansion

- Monitor utilisation
- Ensure compliance with safety obligations

Phase 3 (5–10 Years): Review and Optimization

- Periodic assessment of:
    - Spectrum utilisation
    - Safety outcomes
- Adjust policy if necessary

Conclusion

The DoT spectrum charging methodology dated 11.12.2023 is **not suitable for direct application to V2I communication services**, as it is designed for commercial and enterprise use cases rather than public-safety infrastructure.

A **zero-charge administrative assignment model**, or at most a **nominal administrative fee**, is the most appropriate regulatory approach.

This ensures:

- **Accelerated V2X deployment**
- **Maximum public safety benefits**
- **Removal of cost barriers**
- **Equitable access across India**
- **Alignment with global best practices**

In the context of India's road safety challenges, regulatory policy must prioritise **saving lives over generating revenue**, and spectrum policy must reflect this fundamental principle.

Q14. If answer to Q12 is affirmative, whether the spectrum charges for the V2I communication service authorised entities under the proposed V2I communication service authorisation should be levied as a percentage of Adjusted Gross Revenue (AGR)? If yes, are there any specific operational/ non-operational revenue items that should be included in/ excluded from AGR for the purpose of determination of spectrum charges? Please provide your response with detailed justification.

Comments : **No Comments.**

Q15. If response to questions 13 and 14 is negative, then what should be the appropriate methodology for determination of spectrum charges for the V2I communication service authorised entities under the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

Comments : **No Comments.**

Q16. For spectrum assigned to the V2I communication service authorised entities under the proposed V2I communication service authorisation, what should be the appropriate payment terms for spectrum charges, if any? Please provide your response with detailed justification.

Comments : **No Comments.**

Q17. What are the potential sources of revenue, if any, for an V2I communication service authorised entity under the proposed V2I communication service authorisation? Please provide your response with detailed justification.

Comments : **No Comments.**

Q18. What should be the definitions of Gross Revenue (GR), Applicable Gross Revenue (ApGR), and Adjusted Gross Revenue (AGR) for V2I communication service authorised entity under the proposed V2I

communication service authorisation? Further, what should be the relevant items of revenue, exclusions and deductions and consequent definitions of GR, AGR and ApGR? Please provide your response with detailed justification.

Comments : No Comments.

Q19. What revenue components should be included in, or excluded from, the computation of Gross Revenue (GR), Applicable Gross Revenue (ApGR) and Adjusted Gross Revenue (AGR) for the purpose of determining authorisation fees or spectrum charges for the proposed V2I communication service authorisation? Please provide your response with detailed justification.

Comments : No Comments.

Q20. Whether revenue derived from safety-related V2X services under the proposed V2I communication service authorisation should be excluded from the computation of AGR, in view of their public interest and non-commercial nature? Please provide your response with detailed justification.

Comments :

It is strongly recommended that **revenue derived from safety-related V2X services should be excluded from the computation of Adjusted Gross Revenue (AGR)**, subject to clear definition, ring-fencing, and audit safeguards. Safety-related V2X services—such as collision warnings,

emergency braking alerts, vulnerable road user alerts, and hazard notifications—are inherently **public-interest, life-saving functions** and do not constitute commercial telecom services in the conventional sense.

Including such revenue within AGR would create a **regulatory and financial disincentive** for OEMs, infrastructure providers, and service entities to deploy and integrate these safety features at scale. This would directly undermine public safety objectives and could result in safety features being limited to premium segments or subscription-based models, thereby excluding large sections of road users.

A **targeted exclusion model (Option B)**—where safety-related V2X revenue is excluded from AGR with strict definitions and audit mechanisms—is therefore the most balanced and consumer-centric approach. This ensures that **public safety is prioritised without creating loopholes for misuse**, while remaining consistent with the broader licensing and revenue framework.

Background: AGR, Licence Fee, and Public-Interest Services

The AGR framework in India forms the basis for computation of licence fees and spectrum usage charges for telecom service providers. It is designed to capture revenue derived from **commercial telecom services**, ensuring fair contribution to public exchequer.

However, historically and conceptually, **public-interest and non-commercial services have received differentiated treatment**, including:

- Universal Service Obligation Fund-supported services
- Emergency and disaster communication systems

- Government and public-safety communication networks

These precedents establish that **not all revenue streams linked to communication infrastructure are appropriate for AGR inclusion**, particularly when the primary objective is **public welfare rather than commercial gain**.

Nature and Role of Safety-Related V2X Services

Safety-related V2X services include:

- Collision avoidance warnings
- Emergency braking alerts
- Red-light violation warnings
- Work-zone and hazard alerts
- Vulnerable road user protection (pedestrians, cyclists, two-wheelers)

These services are:

- **Real-time and latency-sensitive**
- **Non-discretionary in nature** (must function universally)
- **Public-good oriented**, benefiting all road users irrespective of who pays
- **Often embedded within vehicle systems or infrastructure**, not standalone revenue services

They are fundamentally different from:

- Infotainment services
- Fleet management solutions
- Subscription-based connected car services

Economic and Social Benefits of Safety-Related V2X

Safety-related V2X services generate **significant positive externalities**, including:

1. Reduction in Road Accidents and Fatalities

- Early warnings prevent collisions
- Protection for vulnerable road users

2. Lower Public Health and Economic Burden

- Reduced emergency response costs
- Lower hospitalization and rehabilitation expenses

3. Improved Traffic Efficiency

- Smoother traffic flow
- Reduced congestion

4. Environmental Benefits

- Lower fuel consumption
- Reduced emissions

These benefits accrue to **society at large**, not just the service provider or user.

Impact of Including vs Excluding AGR

If Included in AGR

1. Deployment Disincentive

- Service providers may avoid investing in safety infrastructure
- OEMs may limit integration

2. Increased Cost of Safety Features

- Costs passed on to consumers
- Safety features become premium offerings

3. Fragmentation

- Uneven adoption across regions and vehicle segments

4. Reduced Public Safety

- Lower penetration of life-saving systems

If Excluded from AGR

1. Accelerated Deployment

- Incentivises rapid rollout

2. Universal Access

- Safety features available across all vehicle categories

3. Lower Cost Burden

- Reduced financial pressure on OEMs and operators

4. Enhanced Public Welfare

- Wider safety coverage

Recommended Regulatory Treatment

Exclusion of Safety-Related V2X Revenue from AGR (with Safeguards)

1. Definition of Safety-Related V2X Revenue

Safety-related V2X revenue should include:

- Revenue from services that:
    - Directly prevent accidents
    - Provide real-time safety alerts
    - Protect vulnerable road users
    - Support emergency response
- Embedded safety features within vehicles or infrastructure

2. Exclusions from Safety Category

The following should NOT qualify:

- Infotainment services
- Commercial fleet analytics
- Advertising-based services
- Subscription-based non-safety services

3. Ring-Fencing Mechanism

Entities must:

- Maintain **separate accounting for safety-related V2X revenue**
- Clearly distinguish:
    - Safety vs non-safety revenue streams

4. Audit and Compliance

- Periodic audit by:
    - DoT / TRAI designated authorities
- Mandatory:
    - Disclosure of revenue classification
    - Certification by statutory auditors

5. Treatment of Bundled Services (Assumption)

Where safety features are bundled within broader offerings:

- A **reasonable apportionment model** should be adopted
- Based on:
    - Cost allocation
    - Functional classification
- Conservative approach to avoid misuse

Safeguards Against Misuse

To prevent misclassification:

1. **Clear Regulatory Definitions**
    - Standardised list of safety services
2. **Pre-Approval Mechanism**
    - Certification of safety services
3. **Audit Trails**
    - Mandatory documentation
4. **Penalties for Misclassification**
    - Financial penalties

    - Withdrawal of exemption
5. **Independent Oversight**
    - Multi-agency review mechanism

Consumer Protection and Equity Implications

The proposed approach ensures:

1. Universal Safety Access

- Safety features available across all vehicle segments

2. Affordability

- No artificial cost escalation due to AGR

3. Equity Across Regions

- Rural and low-income regions benefit equally

4. Trust in V2X Systems

- Reliable and widely available safety features

5. Protection of Vulnerable Road Users

- Broader coverage improves safety for pedestrians and two-wheelers

Implementation Roadmap

Phase 1 (0–1 Year): Policy Definition

- Define safety-related V2X services
- Notify AGR exclusion framework

Phase 2 (1–3 Years): Reporting and Compliance

- Introduce:
    - Accounting guidelines
    - Reporting formats
- Begin audits

Phase 3 (3–5 Years): Review and Refinement

- Evaluate:
    - Deployment impact
    - Safety outcomes
- Refine definitions and safeguards

Conclusion

Excluding safety-related V2X revenue from AGR is essential to ensure that **public safety is not treated as a taxable commercial activity**.

A **ring-fenced exclusion model with robust safeguards**:

- **Promotes rapid deployment of life-saving technologies**
- **Maximises public safety and welfare**
- **Prevents cost barriers and inequity**
- **Maintains integrity of the AGR framework**

In the Indian context, where road safety is a critical national concern, regulatory policy must ensure that **financial mechanisms do not discourage the adoption of technologies that save lives**.

Q21. What should be the appropriate entry fee for V2I communication service authorised entities under the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

Comments : No Comments.

Q22. What should be the appropriate terms and conditions for bank guarantees for the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

Comments : No Comments.

Q23. What should be the applicable minimum equity and minimum net worth requirements for authorised entities under the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

Comments : No Comments.

Q24. What should be the applicable application processing fee for the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

Comments : No Comments.

Q25. What should be the applicable rate of authorisation fee for proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

Comments : No Comments.

Q26. Apart from the financial provisions discussed earlier, are there any other financial terms and conditions that should be made applicable for the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

Comments : **No Comments.**

Conclusion :

In light of the detailed submissions made herein, it is respectfully concluded that the proposed regulatory framework for Vehicle-to-Everything (V2X) communication must be firmly anchored in the **public-interest mandate** embodied in the Telecommunications Act, 2023, and the constitutional obligation of the State to ensure **safety, welfare, and equitable access** for all citizens. V2X communication, by its very nature, constitutes a **public-safety infrastructure** and not a conventional commercial telecom service. Accordingly, the regulatory architecture must reflect this distinction through appropriate safeguards, obligations, and consumer-centric protections.

It is therefore submitted that the framework adopted by TRAI and subsequently by the Government of India must ensure that:

1. **Safety-related V2X services are treated as essential public-interest services**, and no citizen is denied access to life-saving alerts or cooperative safety applications due to affordability constraints, OEM-specific restrictions, or technological incompatibilities.
2. **Interoperability across all RSUs and OBUs is mandated as a legal requirement**, supported by harmonised ITS stack standards,

conformance testing, and certification. Fragmentation of safety systems would directly compromise consumer safety and must be prevented through enforceable regulatory conditions.

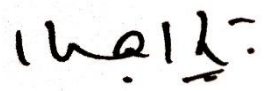
3. **A National V2X Security and PKI Framework** is established under statutory authority, ensuring authentication, pseudonymity, certificate lifecycle management, and misbehavior detection. This is essential to protect consumers from cyber-risks, privacy violations, and manipulation of safety messages.
4. **Mandatory Testing and Certification (MTCTE)** is applied to RSUs and OBUs in a phased manner, ensuring compliance with EMI/EMC, RF safety, cybersecurity, and technical performance requirements. Only certified, safe, and interoperable devices should be permitted for deployment in public spaces or vehicles.
5. **Spectrum for safety-critical V2X applications is assigned on an administrative, non-auctioned, low-cost or zero-cost basis**, consistent with global best practices. Safety-related V2X revenue should be excluded from AGR to prevent cost burdens from being passed on to consumers and to ensure universal accessibility.
6. **Clear separation of safety-related, operational, and commercial V2X revenue streams** is incorporated into the licensing and accounting framework, ensuring transparency, accountability, and consumer protection.
7. **A coordinated multi-agency governance mechanism** is established, involving DoT, TRAI, MoRTH, MeitY, BIS, state governments, and relevant technical bodies, to ensure uniform implementation, enforcement, and continuous oversight of V2X systems across India.

8. **Consumer rights, privacy, and grievance redressal mechanisms** are explicitly incorporated into the regulatory framework, ensuring that citizens have access to remedies, information, and protections in case of device failures, safety-message issues, or cybersecurity incidents.

Taken together, these measures will ensure that India's V2X ecosystem evolves in a manner that is **safe, secure, interoperable, affordable, and equitable**, fully aligned with international best practices and the expectations of a modern, rights-based regulatory regime. The adoption of such a framework will not only reduce road fatalities and enhance public safety but will also position India as a global leader in intelligent transportation systems and next-generation mobility innovation.

Accordingly, it is respectfully submitted that TRAI may consider the recommendations contained in this submission and incorporate them into the final regulatory framework, thereby upholding the paramount objective of **consumer protection and public welfare** while enabling a robust, future-ready V2X ecosystem for the nation.

Thanks.



(Dr.Kashyapnath)
President