CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT

Comments on

Consultation Paper on the Regulatory Framework for the Sale of Foreign Telecom Service Providers' SIM/eSIM Cards for the use in M2M/IoT Devices meant for Export purposes

Introduction

The global expansion of the Internet of Things (IoT) and machine-to-machine (M2M) communication is transforming telecommunications networks. Billions of devices – from smart appliances and vehicles to industrial sensors – are being connected worldwide. Industry forecasts project the number of connected IoT devices to reach around 40 billion by 2030. Many of these devices are manufactured in one country and then **exported for use abroad**, meaning they require seamless connectivity across international borders. In this context, the use of **subscriber identity modules (SIM cards)** or embedded SIMs (**eSIMs**) from foreign telecom service providers has emerged as a practical solution to ensure devices remain connected globally. This development, however, raises important regulatory considerations around licensing, security, and cross-border coordination.

International Regulatory Landscape: Around the world, regulators are grappling with how to accommodate global IoT connectivity while upholding national telecom laws. Approaches vary across jurisdictions. **In the European Union (EU)**, policy-makers have generally adopted an enabling stance toward international IoT connectivity. The EU's Roaming Regulation (EU) 2022/612 explicitly acknowledges permanent roaming for M2M/IoT as *"an important driver for digitising the EU's industry"*, and encourages mobile network operators to accept reasonable requests for wholesale roaming agreements that allow IoT devices to remain connected across borders. In practice, the EU imposes no specific restrictions on long-term roaming or the use of foreign SIM profiles in IoT devices; instead, it expects commercial agreements to facilitate such connectivity in compliance with fair use and competition rules. **In the United States**, there are presently no formal regulations prohibiting the use of foreign SIMs or permanent roaming for IoT, and the approach has been market-driven. U.S. mobile carriers and global IoT service providers often rely on roaming agreements and multi-network eSIM solutions to provide worldwide coverage. This **laissez-faire approach** (shared by countries like Canada and Australia) comes with an understanding that industry-led solutions can address connectivity needs, though some local operators may resist long-term foreign SIM usage for business reasons. By contrast, **several Asia-Pacific and other nations have tighter regulations**. For example, jurisdictions such as *China, India, Singapore, Saudi Arabia and Turkey* insist that IoT devices use locally licensed networks if deployed within their territory, effectively disallowing large-scale use of foreign SIMs in domestic devices. Some countries outright ban "permanent roaming" – the continuous use of a foreign SIM inside the country – after a short period. For instance, Brazil and Turkey have implemented strict prohibitions on long-term roaming by foreign SIMs. These measures are often motivated by security concerns, regulatory oversight of telecom services, and revenue considerations for local operators. The patchwork of global rules means an IoT device might be treated very differently from one country to the next. A device that roams freely under EU regulations may need a local telecom profile when operated in markets with stricter policies. **Thus, global IoT manufacturers and exporters must navigate a complex regulatory landscape**, balancing the goal of ubiquitous connectivity with each nation's legal requirements.

Industry Developments and Technology Trends: In parallel with regulatory evolution, the telecom industry has been innovating to support global IoT connectivity. A cornerstone of this innovation is the advent of the **eSIM (embedded SIM)** and its associated **remote provisioning** capabilities. Unlike a traditional SIM card (which is physically swappable and tied to one operator profile), an eSIM is embedded into the device's hardware and can be programmed "over-the-air" with different operator profiles as needed. This technology has been a game-changer for connected devices crossing borders. **Global standards** have been established to ensure eSIM interoperability and security. The GSM Association's **Embedded SIM Specification** provides a unified, de-facto standard mechanism for the remote provisioning and management of M2M SIM profiles. In essence, a manufacturer can solder a single eSIM chip into an IoT device at the factory, and that eSIM can later be configured with the appropriate mobile network profile in whichever country the device is deployed. This capability allows a device exported from India to automatically switch to a foreign telecom network upon activation, without needing a physical SIM swap. Crucially, the remote provisioning process is designed with robust security measures – industry certification guidelines mandate encrypted connections, data protection, and system integrity throughout the provisioning workflow. By adhering to global standards, eSIM technology ensures that switching carriers or profiles is not only convenient but also secure and trusted by all parties (manufacturers, network operators, and end users). These developments directly address the **need for interoperability and secure device provisioning**: any compliant eSIM-equipped IoT device can securely download and install a new operator profile, enabling interoperability across different carriers while safeguarding the credentials and data involved.

The rise of **global IoT connectivity platforms** further exemplifies industry's response to these needs. Specialized international IoT service providers and Mobile Virtual Network Operators (MVNOs) now offer "global SIM" solutions – often powered by eSIM or multi-IMSI technology – that allow a single SIM/eSIM to access multiple networks worldwide. This mitigates the issue of devices being stranded without service and helps manufacturers simplify logistics by avoiding multiple country-specific hardware variants. For instance, a logistics company can deploy asset trackers embedded with a global eSIM that automatically connects to a local partner network in each country along the shipment route. Such solutions are also aiding compliance: with remote SIM provisioning, if a country's regulations require usage of a local network, the eSIM can load a profile from a local operator to meet that requirement. In this way, **eSIMs enhance both flexibility and regulatory compliance**, allowing devices to dynamically conform to local telecom rules without physical intervention.

International Trends and Future Outlook: Global consensus is building around the importance of adaptable and secure connectivity for IoT. Over the next five years, several key trends are anticipated to shape both technology and policy. First, **eSIM is poised to become the norm** for mobile device connectivity, including IoT devices. Projections indicate that eSIM technology will achieve widespread adoption as the default connectivity method, spurring further IoT innovation and ecosystem growth. This shift is expected to accelerate as next-generation networks like 5G (and soon 6G) mature. 5G networks, with their enhanced bandwidth and low latency, are especially conducive to massive IoT deployments, and eSIM's agility will be crucial for taking advantage of new network capabilities without stranding devices on legacy profiles. Second, the industry is already looking beyond eSIM to **integrated SIM (iSIM)** solutions, where the SIM function is built directly into a device's chipset. iSIM promises further miniaturization and power efficiency for IoT devices, and it leverages the same remote provisioning infrastructure – meaning the regulatory and security considerations for iSIM will closely mirror those for eSIM. As these technologies take root, regulators worldwide are expected to continually refine their frameworks. **International regulatory cooperation** may increase, with agencies sharing best practices on facilitating global IoT connectivity. Notably, discussions are underway in forums and standards bodies on how to handle "permanent roaming" for IoT. While the EU's current approach is to rely on market agreements, there is recognition that some **harmonization of rules or mutual recognition** arrangements could benefit the IoT industry globally. We may see more bilateral or multilateral understandings that allow IoT devices to operate across jurisdictions with a simplified approval process, especially for devices meant for export.

Additionally, **cybersecurity and privacy** will remain front and center. Governments in the EU, US, and Asia-Pacific are introducing stricter IoT security regulations (such as the EU's Cyber Resilience Act and the US IoT cybersecurity labelling program) to ensure that the surge in connected devices does not compromise networks or user data. In the connectivity domain, initiatives like the **GSMA's IoT SAFE** are gaining traction – leveraging the SIM as a secure element to protect IoT data communications at scale. The convergence of connectivity and security means that any regulatory framework for foreign eSIM/SIM usage must also account for protecting device identity and data through strong encryption and authentication standards.

In summary, the **international experience to date highlights a few clear themes**: regulators are generally supportive of solutions that enable global IoT and M2M services, provided national security and consumer protection concerns are addressed; technological advancements like eSIM are reducing technical barriers and enabling compliance with diverse local requirements; and collaborative efforts are underway to anticipate the needs of a rapidly evolving IoT ecosystem. India's burgeoning electronics and IoT manufacturing sector stands to benefit from these global trends. By leveraging eSIM and global connectivity innovations, Indian manufacturers can ensure their export-bound devices are "born connected" and ready for immediate deployment in foreign markets. However, it is imperative to craft a **balanced regulatory framework** that permits such use of foreign TSPs' SIM/eSIM cards in export-oriented devices, while safeguarding national interests (for example, by preventing any misuse of these SIMs domestically in India, and ensuring traceability/accountability of connectivity during the manufacturing and testing phases).

Q1. Which of the following approaches should be followed for regulating the sale of foreign telecom service providers' SIMs/ eSIM cards in India for the use in M2M/ IoT devices meant for export purposes:

(a) To introduce a new service authorisation for the sale of foreign telecom service providers' SIMs/ eSIM cards in India for the use in M2M/ IoT devices meant for export purposes under Section 3(1)(a) of the Telecommunications Act, 2023; or

(b) To include the activity of the sale of foreign telecom service providers' SIMs/ eSIM cards in India for the use in M2M/ IoT devices meant for export purposes within the scope of the proposed service authorisation for the sale/ rent of international roaming SIM cards/ global calling cards of foreign operators in India? Please provide a detailed response with justifications.

Comments :

For the sale of foreign-operator SIMs/eSIMs in India for embedding in M2M/IoT devices destined exclusively for export, two broad regulatory routes present themselves:

1. **A stand-alone "export-IoT-SIM" authorisation under Section 3(1)(a) of the Telecom Act, 2023**, or
2. **Inclusion of that activity within the scope of the proposed "international roaming/global calling card" authorisation**.

Below is a detailed comparison and our recommendation.

1. Nature of the Activity

Feature	Export-IoT SIMs	International Roaming SIMs
End-use	M2M/IoT modules in devices (e.g. trackers, sensors) manufactured in India and shipped abroad.	Human subscribers—voice/data while travelling.
Traffic profile	Predominantly low-volume, machine-to-machine data flows; may be "always-on."	Sporadic high-volume bursts, voice calls, SMS, data roaming.
Billing/Settlement	Likely wholesale data-pool or flat-rate export bundles.	Per-use roaming rates, bilateral IOT settlements.
Security/Sovereignty risks	Embedded devices could be used in unattended or sensitive installations.	Directly linked to known, KYC'd subscribers.
Regulatory precedent	No existing Indian category for export-only IoT SIMs.	Long-established licensing regime under "roaming."

2. Option (a): New Service Authorisation under Section 3(1)(a)

Section 3(1)(a) empowers DoT to grant licences for "telecommunication services" not otherwise classified.

Pros

1. **Tailored Conditions**

    - **Security**: Can mandate encryption, device-level authentication, and periodic audits specific to unattended IoT use.
    - **Quality of Service (QoS)**: Set minimal latency, packet-loss thresholds critical for industrial IoT.
2. **Clarity of Scope**
    - Avoids confusion with human-roaming SIMs; both industry and regulator know exactly which licence applies.
3. **Fee Structure & Accounting**
    - Can prescribe a simple flat “export bundle” fee or wholesale pool, distinct from per-minute roaming tariffs.
4. **Statutory Fit**
    - Section 3(1)(a) is expressly meant to accommodate novel telecommunication services not covered elsewhere.

Cons

- **Licensing Overhead**: Setting up a new category requires drafting specific licence conditions, fee schedules, and possibly amending licence-exemption lists.
- **Time to Implement**: A fresh authorisation may take longer to notify and operationalise.

3. Option (b): Fold into “International Roaming/Global Calling Card” Authorisation

Pros

1. **Regulatory Economy**

    - Leverages an already-established licensing framework (e.g. security deposit, bank guarantee models, inter-operator settlement).

2. **Faster Roll-out**
    - Amend the roaming licence to explicitly mention IoT/export SIMs, avoiding the need to draft an entirely new authorisation.

Cons

1. **Misalignment of Use-Cases**
    - Roaming licences are optimized for transient human subscribers—billing, KYC, numbering plan, and interconnect agreements are all subscriber-centric.
2. **Complex Accounting**
    - Roaming IOT traffic would mix with voice/SMS, complicating reconciliation and revenue-share with foreign carriers.
3. **Security Gaps**
    - Roaming licences do not currently mandate device-level security audits or embedded-SIM provisioning controls.

4. Recommendation

Adopt Option (a): introduce a dedicated "Foreign-Operator Export-IoT SIM" authorisation under Section 3(1)(a).

1. **Statutory Alignment**
    - Section 3(1)(a) expressly empowers grant of licences for emerging telecommunication services not otherwise envisaged by the Act.

2. **Regulatory Certainty**
    - A bespoke licence prevents regulatory arbitrage between consumer roaming and industrial export devices.
3. **Security & Compliance**
    - Enables tailored KYC (for the manufacturer/importer rather than end-user), over-the-air provisioning security standards, and audit requirements suited to IoT.
4. **Ease of Future Amendments**
    - As IoT evolves (e.g. 5G-based NB-IoT export use), conditions can be updated within this single licence category without disturbing the roaming framework.

5. Illustrative Licence Structure (Draft Outline)

Section	Key Provisions
Scope & Definitions	Define “Export IoT SIM/eSIM,” “Manufacturing Entity,” “Embedded Use,” “Outbound Data Bundles.”
Grant of Authorisation	Permit sale/issuance to M2M/IoT device assemblers for exclusively export use.
Security & Provisioning	Mandate GSMA-compliant eSIM provisioning, OTA encryption, device-level authentication.
Tariff & Fees	Flat export data bundle fees; no per-minute voice/SMS charges.
Reporting & Audit	Quarterly traffic reports; annual security audit certificate.
Surrender & Suspension	Grounds for non-compliance, security breach, or misuse penalties.

Conclusion

While piggy-backing on the international roaming/global calling card licence (Option b) may appear administratively expedient, it would conflate two fundamentally different services—human roaming versus machine-to-machine export SIMs—and fail to provide the clarity, security, and tailored conditions that an emerging export-IoT market demands. A new, dedicated authorisation under Section 3(1)(a) (Option a) is therefore both legally sound and operationally optimal.

Precautions :

To **regulate the sale of foreign telecom service providers' SIMs/eSIM cards in India** for use in **M2M/IoT devices meant solely for export**, a careful and balanced framework is needed to **promote exports** while **ensuring national security, traceability, and legal compliance**. The following categories of **precautions** should be taken:

1. **Robust Subscriber Verification (KYC)**
   - Issue SIM/eSIMs only after completing the standard subscriber verification norms applicable to bulk/M2M connections.
   - Require the ultimate purchaser (device OEM or distributor) to submit proof of identity and corporate credentials, and to re-verify on any change of device custody or ownership.
2. **Device Identification & Traceability**
   - Maintain an up-to-date registry of every end-device's unique identifiers (IMEI, ESN, EID for eSIM), including make, model and serial numbers.

- Ensure any change of ownership or transfer is immediately communicated to the licence-holder so the network database can be updated.

3. **Tamper-Proof Logging & Record-Retention**
    - Mandate that all data-, event- and system-logs on the M2M service provider's platform be tamper-evident and stored for a minimum of one year, to facilitate any DoT inspection or lawful-interception requirement.
4. **Packaging & End-User Instructions**
    - Require devices bearing embedded SIMs to carry clear, permanent markings (or accompanying leaflets) stating "Contains SIM inside" and flagging the purchaser's duty to notify any resale or transfer.
    - Impose liability on the last registered owner for any misuse if this instruction is not followed.
5. **Adherence to Technical Standards**
    - Allow only devices and SIM/eSIM-components that meet TEC (Telecom Engineering Centre) certifications or international standards (IEEE, ETSI, GSMA).
    - Prohibit any unauthorised tampering with eSIM modules at the manufacturing stage.
6. **eSIM Profile-Management & Security**
    - Enforce that any profile-download, over-the-air (OTA) update or SM-SR switching be done strictly per GSMA specifications, and within prescribed timelines (e.g., three months for SM-SR integration upon OEM request).

- Preserve lawful-interception capabilities on all profiles, even when roaming on foreign networks.

7. **Roaming Limits & Profile Conversion**
    - If a foreign-issued eSIM is activated on international roaming in India, mandate conversion to one or more Indian TSP profiles within six months of activation or upon transfer of device ownership—whichever is earlier.
    - Discourage use of the 901-XX IMSI series (ITU-allocated for India) by foreign entities until a robust domestic eSIM ecosystem is in place.
8. **Lawful-Interception & Emergency Access**
    - Ensure every imported SIM/eSIM remains interceptable by Indian law-enforcement agencies under Section 5 of the Indian Telegraph Act, and supports emergency-call routing as per national standards.

9. Penalty for Diversion or Misuse

Set clear **penalties for misuse**, including:

- Activation of foreign SIMs in India
- Sale of foreign SIM-enabled devices in the Indian market
- Fines, blacklisting, and cancellation of permissions

10. Record-Keeping & Audit Readiness

- Maintain **transaction records, shipping manifests, and activation logs** for at least 3 years.

    - Be ready to provide **data on sale, integration, and export** to DoT, TRAI, or security agencies upon request.

11. Technical Standards Compliance

- Devices must comply with **international standards** (e.g., 3GPP, ETSI, GSMA).
- Ensure they are not configured to **automatically latch onto Indian networks** upon accidental power-on.

12. Authorised Entities & Licensing

- Only entities **registered with DoT/TEC** or holding an **appropriate license or exemption** should be allowed to sell or embed foreign SIMs/eSIMs in India.
- These entities must declare that the **M2M/IoT devices are solely for export** and will not be activated or used within India.

13. KYC & Subscriber Verification

- Even for export purposes, the **entity purchasing or importing foreign SIMs/eSIMs** should undergo **proper Know Your Customer (KYC)** procedures.
- Maintain a **verified record of each OEM/distributor**, their identity, and usage intent.

14. Traceability & Device Identification

- Maintain a **device-wise registry** of:
    - IMEI, EID, MAC addresses
    - Model/serial number

    - Embedded SIM/eSIM details (IMSI, ICCID)
- Ensure that **ownership and export tracking logs** are maintained for regulatory audits.

15. Export Declarations and Undertakings

- The buyer/seller must submit an **undertaking** stating:
    - Devices with embedded foreign SIMs/eSIMs are not meant for domestic use.
    - SIMs will **not be activated in Indian telecom networks**.
- Export documentation should **clearly identify embedded SIMs/eSIMs** with associated tracking codes.

16. eSIM Profile Control & OTA Security

- Ensure secure management of **Remote SIM Provisioning (RSP)**:
    - Only allow **GSMA-compliant** SM-DP+/SM-SR architecture.
    - Prevent profile downloads within India for foreign SIMs unless approved.

17. Data Privacy & Lawful Interception

- Declare that no **data traffic will pass through Indian networks**.
- Maintain the ability to **cooperate with Indian law enforcement** in case of suspected misuse or diversion.

18. Labeling and Device Marking

- All exported devices must carry clear labels:
    - “**Contains Foreign SIM/eSIM – Not for use in India**”
    - Manufacturer, model, and embedded SIM details

Together, these measures balance the need to promote India's M2M/IoT manufacturing and exports with the imperatives of network security, subscriber traceability, and law-and-order compliance.

Practice in other countries :

The **regulatory practices in other countries** regarding the **sale or use of foreign telecom service providers' SIMs/eSIMs in M2M/IoT devices meant for export** generally reflect a **balance between national security, spectrum management, and promotion of domestic industry**. While India is currently exploring a specific framework for this, here is how **other key jurisdictions regulate this domain**:

1. United States (FCC / NTIA / CBP)

Key Practice:

- The U.S. does **not restrict the embedding of foreign SIMs** into devices meant strictly for export.
- However, **import/export control regulations** under the Bureau of Industry and Security (BIS) apply to communication equipment.
- **FCC Part 15 and 68 compliance** is required if the device operates within the U.S. before export.

Safeguards:

- Devices with embedded SIMs **cannot be activated on U.S. networks unless registered**.
- Customs may inspect devices if there is suspicion of local sale or activation.

EU European Union (EU / ETSI / BEREC)

Key Practice:

- **No prohibition** on the use or embedding of non-EU SIMs for devices **destined for export**.
- The **EU RSP (Remote SIM Provisioning) framework** supports international profile provisioning, but devices must not connect to EU networks using unregistered IMSIs.

Safeguards:

- Manufacturers must comply with **Radio Equipment Directive (RED)** and **CE marking**.
- Export declarations must confirm **no intention of EU market access** unless full regulatory compliance is ensured.

SG Singapore (IMDA)

Key Practice:

- The Infocomm Media Development Authority (IMDA) permits the import and re-export of devices with foreign SIMs.
- No SIM (even embedded) may be used on Singaporean networks unless registered with a **licensed operator**.

Safeguards:

- Exporters must submit **declarations on intended destination** and final use.

- IMDA requires **compliance testing for electromagnetic compatibility** even if the device is not used locally.

CN China (MIIT)

Key Practice:

- **Strict regulatory control** over foreign SIMs and eSIMs.
- Devices with embedded foreign SIMs may be manufactured for export but must be **registered with MIIT** and may not operate on domestic networks.

Safeguards:

- All communication modules are subject to **China Compulsory Certification (CCC)** even for export models.
- Export-only labeling and IMEI registration is mandatory.

JP Japan (MIC)

Key Practice:

- Ministry of Internal Affairs and Communications (MIC) permits embedding foreign SIMs if the device is not activated in Japan.
- Exporting OEMs must obtain **technical conformity certification** for radio use.

Safeguards:

- Must not use non-Japanese SIMs on Japanese networks unless approved.

- Devices must be labeled “Not for use in Japan” if not registered locally.

Global GSMA Practices

Relevant Insights:

- **GSMA Embedded SIM Specifications** (M2M and Consumer) allow **remote profile provisioning** globally.
- **SM-DP+ and SM-SR servers** used to manage eSIMs must comply with **regional regulations**, especially for lawful interception.
- **Use of global IMSI ranges (901-XX)** is under review in several countries due to concerns over jurisdictional traceability.

Key Common Themes Across Countries

Regulatory Aspect	Common Practice
SIM Activation Rules	SIMs must not be activated domestically unless registered with a local TSP.
Labeling & Declarations	Mandatory labels: “For Export Only”; export documentation required.
Lawful Interception Compliance	Embedded SIM/eSIM must allow tracking in case of misuse/diversion.
Technical Certification	Compliance with radio and safety standards, even if device is for export.
Remote Profile Management	eSIMs should support traceable and secure RSP methods.

IN Implication for India

India can take cues from:

- **U.S. customs declarations**
- **EU profile management rules**
- **China's strict domestic network protection**
- **GSMA's standardised eSIM architecture**

A **hybrid approach** that supports export-oriented IoT manufacturing while safeguarding India's networks from misuse would be ideal.

Comparative Table: International Practices on Foreign SIMs in Export-Oriented M2M/IoT Devices

Country/Region	**Use of Foreign SIMs/eSIMs for Export Devices**	**Network Use Restrictions**	**Certification Requirements**	**Remote SIM Provisioning (RSP)**	**Labeling & Export Control**
US USA	Allowed with export intent	Must not activate in U.S.	FCC compliance	GSMA RSP accepted	Marked as "Export Only"
EU EU	Allowed	Must not activate in EU	CE/RED directive	GSMA RSP; SM-DP+/SM-SR mandatory	CE label and export proof
SG Singapore	Allowed	Must not activate locally	IMDA technical approval	Compliant with GSMA	Export declaration required

Country/Region	Use of Foreign SIMs/eSIMs for Export Devices	Network Use Restrictions	Certification Requirements	Remote SIM Provisioning (RSP)	Labeling & Export Control
CN China	Allowed under strict oversight	Strict ban on foreign SIM use	CCC certification	Must be controlled by MIIT	Mandatory IMEI registration
JP Japan	Allowed	Only for export	MIC certification	Profile switching regulated	Labeled “Not for Japan Use”
🌐 GSMA	Permits global RSP standards	National regulations apply	Adopts 3GPP/ETSI standards	eSIM RSP framework universal	SM-DP+/SM-SR location tracked

---

Draft Policy Recommendation for India

1. Purpose

To promote IoT/M2M manufacturing in India for global markets while ensuring traceability, national security, and lawful use of telecommunications infrastructure.

2. Scope

Applies to all entities (OEMs, system integrators, SIM vendors) dealing with **foreign SIMs/eSIMs embedded in devices manufactured or assembled in India solely for export purposes**.

3. Key Provisions

Authorization and Licensing

- Only **DoT-registered entities** may import or embed foreign SIMs/eSIMs.
- A **one-time registration** is required for each batch of SIMs with declaration of country of origin, IMSI range, and intended export destination.

SIM/eSIM Activation Restrictions

- No device with embedded foreign SIMs/eSIMs shall **connect to any Indian mobile network** at any point, including for testing.
- Devices must **remain inactive in Indian territory** and activate only after export.

Labeling and Export Declaration

- All such devices must carry:

“Contains Foreign SIM/eSIM — Not for Use in India”

- Exporters must file **self-declarations with customs and DoT** for every shipment, confirming non-domestic use.

KYC and Traceability

- Maintain **verified buyer records**, IMEI/ICCID/EID logs, and transaction history for **a minimum of 3 years**.
- Ensure that all devices are **traceable up to the end-buyer** abroad.

Remote SIM Provisioning Compliance

- Only GSMA-compliant **SM-DP+/SM-SR systems** shall be used.
- Foreign TSPs must ensure **lawful interception capabilities** as per Indian norms if ever activated in India (even accidentally).

Technical and Safety Certification

- Devices must meet **TEC certification** (or declare exemption) even for export.
- Mandatory electromagnetic compatibility and radio frequency compliance to prevent unintentional emissions on Indian spectrum.

Penalty for Diversion or Misuse

- Heavy penalties (₹10 lakh or more) for:
  - Use of such devices on Indian networks.
  - Selling devices domestically with embedded foreign SIMs.
- Blacklisting of non-compliant OEMs or distributors.

4. Oversight Mechanism

- A dedicated **Export Device Cell** under DoT/TEC to:
  - Monitor declarations
  - Track usage and batch-wise IMEI/EID
  - Coordinate with customs and LEAs

5. Industry Incentives

- Fast-track approvals for compliant exporters.
- Optional **sandbox access for export-focused IoT innovations** under regulatory relaxation.

Other key jurisdictions regulate the sale or use of foreign telecom service providers SIM/eSIM in M2M/IoT devices meant for export in India :

In **India**, the regulation of the **sale or use of foreign telecom service providers' SIMs/eSIMs in M2M/IoT devices meant for export** involves **multiple key jurisdictions and regulatory bodies**, each overseeing different aspects such as telecom licensing, equipment standards, import/export control, cybersecurity, and customs compliance.

Below is a list of the **key Indian jurisdictions** and their **respective roles** in this regulatory framework:

Key Regulatory Jurisdictions in India

Authority / Jurisdiction	**Role in Regulation of Foreign SIM/eSIM in Exported M2M/IoT Devices**
1. Department of Telecommunications (DoT)	Apex body for telecom licensing and policy formulation
Grants permission for M2M/IoT connectivity	
Likely to issue regulatory framework for use of foreign SIMs in export-bound devices	

Authority / Jurisdiction	Role in Regulation of Foreign SIM/eSIM in Exported M2M/IoT Devices
2. Telecom Regulatory Authority of India (TRAI)	Advisory and recommendatory body
Issues consultation papers (e.g., on foreign SIM/eSIM sale)	
Recommends licensing terms, numbering, security, and spectrum use	
3. Ministry of Electronics and Information Technology (MeitY)	Oversees electronics manufacturing and export policy
Plays a key role in IoT/M2M roadmap	
Governs data protection, cybersecurity, and cross-border data flow	
4. Telecom Engineering Centre (TEC)	Technical wing of DoT
Defines **Essential Requirements (ERs)** for telecom equipment	
May mandate conformance testing or exemption for export-only devices	
5. Ministry of Commerce and Industry (DGFT)	Regulates **import/export policies** for telecom equipment
Maintains Foreign Trade Policy and ITC-HS Codes	
May issue clarifications on customs codes for devices with foreign SIMs	
6. Directorate of Revenue Intelligence (DRI)	Enforces rules on misuse/diversion of imported/exported items
Investigates cases of foreign SIM-enabled devices used in India	
7. Central Board of Indirect Taxes and Customs (CBIC)	Enforces customs compliance and export control

Authority / Jurisdiction	**Role in Regulation of Foreign SIM/eSIM in Exported M2M/IoT Devices**
Requires declarations and proper labeling for export-bound goods	
May inspect IoT devices embedded with foreign SIMs at ports	
8. National Cyber Security Coordinator (NCSC)	Provides security guidance on **critical telecom infrastructure**
Monitors embedded components including foreign connectivity modules	
9. Ministry of Home Affairs (MHA)	Concerned with **lawful interception and national security**
May require assurance that foreign SIMs are not used domestically or for surveillance	
10. Bureau of Indian Standards (BIS)	Sets quality and safety norms for electronic devices
Some M2M modules may require BIS certification, unless exempted	
11. WPC Wing (Wireless Planning & Coordination) – DoT	Regulates spectrum use and wireless transmission
May specify conditions on foreign-origin wireless M2M modules	
12. NITI Aayog	Think-tank role in IoT, Industry 4.0, and Atmanirbhar Bharat policies
Coordinates policy synergy across sectors	

Inter-agency Coordination

These jurisdictions **interact in tandem** to ensure:

- Export promotion (MeitY, DGFT)
- Telecom and spectrum integrity (DoT, WPC)
- National security (MHA, NCSC)
- Technical and safety compliance (TEC, BIS)
- Prevention of diversion (DRI, CBIC)

Example of Interlinked Oversight

When an OEM wants to manufacture IoT trackers with **embedded foreign SIMs** for export:

- **DoT** must define licensing or permission for such activity.
- **TEC** may exempt the device from ER testing if only for export.
- **CBIC** ensures it is declared properly at customs with labeling "Not for Domestic Use".
- **DRI** tracks diversion risks.
- **MHA** and **NCSC** are involved if any surveillance risk is foreseen.

Recommendation for Unified Oversight

A **nodal body or inter-ministerial task force** (possibly led by DoT and MeitY) could be formed to:

- Streamline the approval process
- Notify unified guidelines for foreign SIMs in export-bound IoT devices
- Monitor traceability and prevent misuse

Other Potential alternative approaches :

Regulating the Sale of Foreign SIMs in IoT Devices for Export in India

Background and Context

Under current policy (the 2022 NOC regime), foreign telecom operators can sell international roaming SIM cards or global calling cards in India to customers traveling abroad, but strict conditions apply – for example, the SIM must be activated within 48 hours before travel and deactivated within 24 hours of the customer's return. Sellers must also perform extensive KYC (Know-Your-Customer) checks, collecting passports, visas or travel documents of the individual user. These rules, while workable for tourist SIM cards, **do not fit the IoT/M2M use-case**. In the IoT scenario, Indian manufacturers need to embed *foreign* SIMs (or eSIM profiles) into devices (e.g. smart appliances, vehicles, sensors) so that upon export the device can immediately connect to the foreign network it is intended for. Often a short activation **in India is required for testing and prototyping** to ensure the device functions properly before shipment. However, the existing NOC policy **strictly limits in-India activation**, which is "not covered under the current regulatory regime". This regulatory uncertainty makes it difficult for Indian exporters to test devices and include the appropriate foreign connectivity.

Compounding the issue, India's new Telecommunications Act, 2023 mandates that any entity providing telecommunication services must obtain an appropriate authorisation from the government. Selling or provisioning foreign operator SIMs in India is considered a telecommunication service activity, meaning it cannot continue indefinitely under an informal NOC framework. In fact, in 2024 the Department of

Telecom (DoT) cracked down on unlicensed foreign eSIM services (e.g. apps like Airalo and Holafly were removed from app stores for operating without the required NOC) – underscoring that **foreign SIM distribution in India must be brought under a clear regulatory authorization**. The goal is to devise a **comprehensive yet streamlined framework** that facilitates IoT exports while addressing security and compliance concerns.

Proposed Regulatory Approaches

TRAI's consultation outlines two primary approaches to regulate the sale of foreign telecom operators' SIMs/eSIMs in India for IoT/M2M export devices. Both approaches would fall under the new *service authorisation* regime established by Section 3(1)(a) of the Telecom Act, 2023 (which requires a government authorization to provide any telecommunication service). The difference lies in whether to create a **new, dedicated category** of authorization or to **leverage an existing/proposed category** by expanding its scope:

Approach (a): A New Dedicated Service Authorisation

One option is to introduce a **separate service authorisation specifically for the sale of foreign TSPs' SIM/eSIM cards for use in export-bound M2M/IoT devices**. This would essentially carve out a new licensing category tailored to this unique activity. The authorisation would be granted under the Telecom Act, with its own defined scope and conditions (distinct from other telecom services). Stakeholders would need to help define the terms and conditions for this new category – for example, **eligibility criteria** (who can apply for the license), the **permitted scope of activities**, the **validity period** of the authorisation, **fees or charges** payable, and compliance obligations. Because this use-case is novel, TRAI has signalled a likely *light-touch regulatory approach* similar to other auxiliary services. Notably, in mid-2024 TRAI had already recommended that the government introduce a light-touch, ten-year authorisation for companies selling or renting international roaming SIM cards of foreign operators. DoT accepted that recommendation in principle, which indicates regulatory willingness to create new service categories for such niche services. By analogy, a new *"Foreign IoT SIM Sales"* authorisation could likewise be created to specifically handle IoT/M2M connectivity needs for exports.

Justifications for a New Authorisation:

The chief argument for this approach is that the IoT/M2M foreign SIM scenario has **distinct requirements** that merit a bespoke framework. Unlike tourist SIM providers who deal directly with individual travellers, IoT SIM distributors would primarily serve enterprise customers (device manufacturers) and involve *integrating SIMs into products* rather than selling SIMs over the counter. A dedicated license can therefore impose targeted conditions: for instance, requiring that these SIMs/eSIMs be **non-functional on Indian networks (except during limited testing)**, simplifying KYC rules (e.g. verifying the **Indian manufacturing company** rather than individual end-users), and mandating specific safeguards before export. It allows TRAI to address *security concerns* in a focused way – e.g. requiring the licensee to keep records of SIM ICCIDs/IMSI and their associated foreign operator, logging test activation dates, and ensuring all active profiles are reported and deactivated in India after testing. The new authorisation could also explicitly handle coordination with other agencies: for example, ensuring import of SIM cards (or download of eSIM profiles) complies with

Customs rules and that any payment to foreign operators for connectivity adheres to RBI's foreign exchange guidelines. By designing a purpose-built license, the government can craft rules that **closely reflect the IoT export workflow**, providing clarity to businesses. Industry stakeholders like CII have indicated support for expanding permissions in this domain, so long as the SIMs are **only functional outside India** (to prevent misuse domestically). A dedicated authorisation could enshrine that principle.

From an administrative standpoint, a separate category also means that an entity interested *only* in providing foreign IoT SIM solutions can apply for this authorisation without needing to obtain any broader telecom license. This lowers entry barriers for specialized IoT connectivity providers or device manufacturers themselves. It isolates the regulatory oversight to the IoT export context, which might simplify compliance since the company would not be mixing this activity with consumer SIM services. Moreover, the license terms can be revisited and fine-tuned as the IoT sector evolves, without unintentionally affecting other services. In summary, Approach (a) offers **clarity and precision**: it cleanly defines a new service with its own rules, ensuring that issues unique to foreign IoT SIM usage (like *prototype testing in India*, *bulk SIM importation*, or *enterprise KYC*) are directly addressed within a singular regulatory instrument.

Potential Drawbacks:

On the other hand, introducing yet another service authorisation adds to the *fragmentation of the licensing framework*. The Telecom Act's new framework already envisions multiple service categories (TRAI's 2024 recommendations span 14 different authorisation rules). A very narrowlyscoped license might only attract a few players, raising the question of whether a full-fledged separate authorisation is warranted for what may be a limited use-case. This approach could also create **duplication of regulatory effort** if there is significant overlap with the already-proposed *"international roaming SIM sales"* authorisation. For example, both the travel-SIM sellers and IoT-SIM providers have common considerations (e.g. ensuring the foreign SIM isn't misused in India, providing reports to security agencies, offering a customer grievance mechanism, etc.). Creating two parallel authorisations might require maintaining two sets of similar rules. Additionally, if a company eventually wants to offer *both* tourist SIMs and IoT SIM integration, under Approach (a) they might need to obtain *two separate authorisations* and comply with two sets of terms – which could increase compliance overhead. Regulators would need to ensure consistency between the two authorisations (e.g. both would likely stipulate government rights to inspect premises and to suspend or revoke the permission in the interest of national security). Maintaining consistency across separate frameworks could become cumbersome. These factors suggest that while a dedicated license is precise, it might be somewhat **inefficient if the activities can be managed together**.

Approach (b): Include IoT SIM Sales Under an Existing Authorisation

The alternative approach is to bring this activity under the umbrella of the **proposed authorisation for international roaming SIM cards/global calling cards of foreign operators**, rather than creating a wholly new category. In other words, the scope of the forthcoming *foreign SIM sales* license (which, as noted, TRAI recommended in 2024 and DoT has agreed to in principle) would be **expanded** to also cover the sale of foreign SIMs/eSIMs for M2M/IoT devices meant for export. The consultation specifically asks stakeholders to consider what **amendments or additional provisions** would be needed in that existing service authorisation's scope and terms to accommodate the IoT use-case. Under this approach, there would be a single broad authorisation (let's call it *"International SIM Distribution Service"* for discussion) that authorizes an entity to: (i) sell/rent foreign operator SIMs to Indian customers for international roaming (travelers), **and** (ii) sell/provide foreign operator SIMs/eSIMs in India for integration into devices destined for overseas markets.

Justifications for an Inclusive Scope:

The main advantage here is **regulatory simplicity and efficiency**. Rather than proliferating license categories, the TRAI can leverage an existing framework and simply extend it. Many foundational requirements are common to both scenarios: for instance, in *either* case the SIMs are not meant to be permanently used in India, so the authorisation would mandate that such SIM cards "can only be used outside India" (except possibly short testing periods). The existing foreign SIM card policy also requires sellers to submit periodic reports to security agencies with details of SIMs sold, user details, period of usage, etc. This reporting requirement could be adapted for IoT: the licensee might report the number of IoT SIMs sold, the recipient manufacturer, and the timeframe of any testing activation. **Combining the regulatory regime** ensures consistency in how foreign SIM services are handled. An operator or company that wants to provide *global connectivity solutions* can deal with a single authorisation process, a single set of fees, and a unified compliance structure. This could encourage more participation and competition in the market, benefiting IoT manufacturers with more choices of providers.

From the perspective of **ease of doing business**, Approach (b) means an Indian entity could potentially cater to both individual travellers and IoT manufacturers under one authorization, if they have the business capability. Even if a provider specializes in one segment, having a unified framework might reduce red tape – they would liaise with the DoT/TRAI under one license system. The terms of the existing international SIM authorisation are expected to be fairly “light-touch” (as TRAI recommended) with a long validity (10 years), which would likely carry over to the IoT use case, thereby avoiding overly onerous renewals or bureaucracy for the companies involved. In essence, Approach (b) avoids reinventing the wheel: since a mechanism to license foreign SIM sales is already being created, it makes pragmatic sense to **widen its scope** rather than draft an entirely new rulebook for a related activity. This can accelerate implementation – IoT SIM provisions could be operational simply by adding clauses to the existing authorisation template – and provide clarity that *all* forms of foreign SIM distribution in India fall under one regulatory umbrella.

Challenges and Considerations:

The inclusive approach must ensure that the **differences in use-cases are properly accounted for within one licence.** The current foreign SIM sale policy (and the envisioned authorisation based on it) is heavily focused on **individual end-users (tourists/business travelers)**. It mandates KYC documents like passport/visa, travel itinerary, and even an undertaking from customers about countries to be visited. These provisions simply do not translate to an IoT context – an IoT device isn't a person with travel plans. Thus, the combined authorisation would need *bifurcated* conditions: one set of KYC/activation rules for foreign SIMs sold to individual travellers, and another set for foreign SIMs provided to manufacturers. For example, KYC for IoT SIMs might involve verifying the credentials of the Indian device OEM (e.g. company registration, authorization letter) and obtaining an undertaking that the embedded SIMs will only be used in exported products. The license terms regarding activation timing would also differ: the *48-hour prior activation* rule for roaming SIMs could be **amended or waived for IoT SIMs**, instead allowing a short window of local activation during production/testing as needed. All such modifications must be clearly delineated to avoid confusion. In effect, the single authorisation would have to cover two sub-services, which could make it lengthier or more complex. There's a risk that a one-size-fits-all license might become **cumbersome if not drafted carefully** – it must not impose irrelevant requirements on IoT SIM providers (for instance, a manufacturer-centric provider shouldn't need to maintain a *tourist customer* grievance hotline or collect passports, etc., which are meaningless for their business). TRAI would need to thoughtfully **amend the scope and conditions** so that each sub-activity is governed appropriately within the same framework.

Another consideration is whether combining them could create any **enforcement gaps**. The foreign SIM authorisation (for travel SIMs) is expected to include security conditions like government inspection rights and emergency suspension powers. These would naturally apply to any licensee, but enforcement might get tricky if, say, a company violates conditions in one domain (e.g. accidentally sells an IoT SIM that gets misused in India) – the penalties and oversight would be handled under the same license as a consumer-facing violation. This is not necessarily a problem, but TRAI must be vigilant in monitoring compliance across both aspects. Despite these nuances, none of these challenges are insurmountable. They mainly require **careful drafting and clear guidelines** within the unified authorisation. With proper scoping (perhaps through separate chapters or schedules for "IoT SIM use-case" vs "International roaming SIM use-case"), Approach (b) can cover the spectrum of foreign SIM sales without sacrificing specificity.

Other Alternatives and Key Considerations

Beyond the two main approaches above, TRAI has solicited views on some *alternative mechanisms* and related issues that could influence the regulatory model:

- **Restricting to Licensed Telecom Operators vs. Open Eligibility:** One fundamental question is *who* should be permitted to carry out this activity. Should it be limited only to existing telecom license holders (e.g. Access Service or Unified Licensees), or can any bona fide Indian company obtain the authorisation/NOC for foreign IoT SIM sales? The consultation specifically asks whether only an entity already holding a telecom licence should be allowed to sell such SIMs, or if **any Indian entity** that meets criteria can be given a NOC/authorisation for this purpose. This is a policy choice: limiting it to licensed telcos could ensure experienced players with established compliance structures (possibly enhancing security), but it would **exclude small/medium IoT firms or SIM resellers** who are not full telecom operators. A more open eligibility (with a simple authorisation/NOC) would encourage specialized IoT connectivity providers and even device manufacturers themselves to partake, boosting ease of business – but appropriate vetting (financial and security clearance) would be needed to prevent fly-by-night operators.

- **Continuation of NOC Regime vs. Formal Licence:** An alternative approach (at least in the short term) could be to continue using an **expanded NOC system** for this specific use-case until the Telecom Act's licensing framework is fully operational. DoT's referral to TRAI was about terms for *issue and renewal of NOC* for importing/selling foreign SIMs for IoT exports. One could imagine DoT simply issuing detailed guidelines and granting NOCs to eligible firms (with conditions tailored for IoT SIM integration) without creating a whole new license category immediately. This would be a stop-gap solution to quickly facilitate the industry's needs. However, once the new Act's rules come into force, any such NOC would likely have to transition into an authorisation. Thus, the NOC approach is essentially the status quo (which industry has found limiting) and is not a long-term substitute for either Approach (a) or (b). It may be useful though to ensure a **grace period or transitional arrangement** so that ongoing IoT projects are not stalled while the formal licensing gets ironed out.
- **Leveraging eSIM Remote Provisioning:** A technical alternative, rather than regulatory, is worth noting. The need to physically import foreign SIM cards could be mitigated by using **eSIM (eUICC) technology with remote provisioning**. Indian manufacturers could ship devices with an empty eSIM module and later download the foreign operator's profile over-the-air once the device is abroad. If feasible, this approach could bypass the need to "sell" foreign SIMs

on Indian soil altogether – meaning perhaps no authorisation would be needed for the SIM aspect (the foreign profile would be loaded by the foreign operator post-export). However, in practice manufacturers often still require a profile on the device to test connectivity before shipment. Also, remote provisioning would still require agreements with foreign operators, and if any profile download occurs while the device is in India (even for testing), it again touches the regulatory domain. Thus, while promising, this is more of a complement to regulation. The **regulatory framework should accommodate new technologies** like eSIM and not impose rules that inadvertently hinder remote provisioning solutions. For instance, if profiles are downloaded in India for testing, the provider facilitating that could fall under the authorised activity.

- **Key Concerns to Address (KYC, Security, and Compliance):** Regardless of which licensing approach is chosen, certain **safeguards and clarifications** are paramount. Firstly, **KYC and record-keeping** must be calibrated to the IoT context: the entity selling or integrating the SIMs should maintain records of which manufacturer or client received the SIMs, the identifiers of those SIMs (so they can be traced if misused), and an affirmation that those SIMs will be used only in devices for export. Traditional individual KYC (passport, etc.) is not applicable here, so rules should specify what constitutes valid KYC for enterprise customers and perhaps require end-use certificates from the manufacturers. Secondly, **security and lawful interception** considerations must be thought through. During the period a foreign SIM is active in India for testing, it will likely operate on roaming (connecting to an Indian network but routing traffic to a foreign network). This could raise concerns about intercepting any communication for security reasons. While the duration and usage would be minimal, DoT may require that the licensee inform security agencies of any test activations or even seek a limited access for lawful monitoring during those tests. In extreme cases, the government might insist that such SIMs be programmed to only attach to networks once the device is out of India (though that would negate testing – so a balance is needed). Indeed, the government will likely reserve broad powers to **inspect premises, audit compliance, and suspend or revoke the permission** if any misuse is detected or in national security interest. Both Approach (a) and (b) should include such clauses.

Additionally, **inter-agency coordination** is an important consideration. Importing large quantities of SIM cards (or telecommunications modules) might trigger customs regulations – they may need to be declared properly, possibly under specific HS codes, and duties (if any) paid. The consultation explicitly asks if there are any regulatory issues with Customs or RBI in this process. For example, **RBI regulations** could be relevant if Indian entities pay foreign operators for connectivity or SIM cards – this might be treated as import of services or goods, requiring compliance with foreign exchange rules. An ideal framework would clarify that obtaining the telecom authorisation does not exempt the licensee from other laws: they must still get any import licenses (if required for telecom hardware) and adhere to forex regulations (such as limits on pre-paid remittances abroad, if they are effectively reselling foreign telecom subscriptions). By identifying these ancillary issues upfront, the TRAI can work with Customs and RBI to issue any necessary clarifications or enable smooth operations (perhaps a one-time customs clearance process for importing SIM batches, etc.).

Finally, a **consumer/enterprise protection** angle: while in IoT cases the "consumer" is not an individual, the end-users of the devices overseas will ultimately rely on connectivity. The reputation of Indian exports could suffer if the SIMs don't work as promised. Thus, **quality-of-service and accountability** should be addressed. The authorisation (especially if under Approach (b)) might require the provider to offer support or service level agreements to the manufacturer, and to have a grievance redressal mechanism (for the Indian manufacturers) akin to what is required for Indian customers in the travel SIM scenario. This ensures that Indian IoT exporters are not left in the lurch by a foreign SIM provider's failure. In summary, any chosen path must consider **KYC processes, security monitoring, inter-agency clearances, and user protection** to create a robust yet facilitative ecosystem. As the stakeholder comments in the TRAI paper suggest, the aim should be to **balance national security and compliance needs with the ease of doing business** for India's growing IoT sector.

Recommendation and Conclusion

After evaluating both approaches, our **recommendation is to proceed with approach (b) – include the IoT/M2M foreign SIM sale within the scope of the proposed international roaming SIM authorisation – with appropriate modifications and safeguards**. On balance, this integrated approach is justified because it builds on an established regulatory framework, thereby reducing duplication and accelerating implementation. The core activity in both cases (foreign SIMs provided in

India for use abroad) is fundamentally similar, and a single authorisation can efficiently accommodate multiple use-cases if carefully structured. TRAI's own earlier recommendation for a foreign SIM selling licence envisioned a light-touch, ten-year authorisation, which aligns well with industry's need for a hassle-free yet secure system. By expanding that framework to IoT devices, India can quickly legitimize and support export-oriented connectivity solutions **without waiting to create a brand-new license from scratch**. This will help Indian manufacturers get the connectivity they need in a timely manner, bolstering our IoT export competitiveness. Importantly, DoT has already "accepted in principle" the concept of a foreign SIM sales authorisation, which means the legal pathway for approach (b) is clear and likely faster to notify.

That said, the recommendation comes with a strong caveat: **all necessary concerns and conditions must be explicitly addressed in the unified authorisation's terms**. The government should incorporate **distinct clauses** for the IoT scenario – e.g. defining how long a foreign SIM may remain active on Indian soil for testing, what records must be kept, and requiring that such SIMs **"shall only be functional outside India"** except during the approved testing period. The authorisation should mandate **proper KYC of the Indian entities purchasing these SIMs** and perhaps a reporting mechanism to ensure transparency to security agencies (this could mirror the monthly reporting of cards sold that is already in the 2022 policy, adjusted for enterprise sales). Furthermore, before operationalizing, DoT/TRAI should consult closely with **Customs and RBI** to iron out any procedural hurdles in importing SIM cards or making foreign payments. If these concerns are addressed, a single expanded licence would provide clarity to all stakeholders and avoid regulatory overlap.

Choosing approach (b) does not mean the IoT use-case is neglected within a broad license – on the contrary, it means the TRAI will handle it **within a proven regulatory structure** but with *bespoke rules carved out internally*. This approach strikes a prudent balance between **regulatory oversight and business flexibility**. It minimizes the administrative burden (both for the government and for businesses that might otherwise need multiple authorisations) while still achieving the objective: ensuring that foreign SIMs for export devices are sold in an authorised, monitored manner in India. The recommendation is to implement approach (b) and to **amend the scope of the international SIM authorisation accordingly**, *combined with detailed guidelines* covering the IoT/M2M specifics. In parallel, the TRAI should keep an open door to any further suggestions – for instance, if stakeholder feedback indicates that a separate authorisation (approach a) would dramatically simplify compliance, that option can be revisited. At present, however, the inclusive licensing approach appears most justified. It leverages existing momentum (since the foreign SIM/light-touch license framework is already underway) and ensures **Indian IoT exporters can get foreign connectivity solutions under a clear, single window of regulation** as soon as possible. By considering all the concerns – security, KYC, inter-agency issues, and industry practicality – and by implementing this recommended approach, India can foster a robust environment for IoT manufacturing and exports while upholding its telecom regulatory principles of security and accountability.

Q.2 In case it is decided to introduce a new service authorisation under Section 3(1)(a) of the Telecommunications Act, 2023 for the sale

of foreign telecom service providers' SIMs/ eSIM cards in India for the use in M2M/ IoT devices meant for export purposes, what should be the terms and conditions for such a service authorisation? Please provide inputs with respect to the following aspects:

Comments :

If a **new service authorisation** is introduced under **Section 3(1)(a) of the Telecommunications Act, 2023** for the **sale of foreign telecom service providers' SIMs/eSIMs in India for M2M/IoT devices meant for export**, the **terms and conditions** must ensure **national security, regulatory compliance, traceability, and export facilitation**. Below is a detailed and structured list of **suggested general terms and conditions**:

Proposed General Terms & Conditions for New Service Authorisation under Section 3(1)(a)

1. Scope of Authorisation

- The authorisation shall strictly permit **sale, provisioning, integration, and testing** of **foreign telecom SIMs/eSIMs** for use **only in M2M/IoT devices that are to be exported**.
- No service shall be extended to devices deployed **within India**, either directly or indirectly.

2. Eligibility Criteria

- Only Indian registered entities (Company/LLP) with a **minimum prescribed net worth** and **clean regulatory history** may apply.
- The foreign telecom operator must be **licensed in its home jurisdiction** and **not subject to international sanctions**.

3. Registration and Licensing

- Registration of the authorised entity under the proposed licence category with DoT/TRAI.
- Maintain a **valid agreement with the foreign telecom service provider**, copies of which must be filed with DoT for vetting.

4. Security & Traceability

- Each SIM/eSIM to be uniquely mapped to a device and its corresponding **IMEI/MAC ID and export invoice**.
- Maintain a **secure, real-time database** accessible to Indian regulatory authorities with:
  - SIM/eSIM ICCID
  - Device identifier
  - Destination country
  - Foreign network details
  - Customs export document reference

5. Export-only Certification

- Devices must bear a **tamper-evident label** stating "Not for Sale/Use in India – For Export Only".
- Must comply with Indian customs rules for export.

6. Data Privacy and Cybersecurity

- The authorised entity shall ensure that:
  - No **real-time data routing** from within India over foreign networks unless anonymized and encrypted.

    - Comply with **CERT-In directives**, including breach reporting.

7. Audits and Reporting

- Quarterly compliance reports to be submitted to DoT/TRAI indicating:
    - Number of SIMs/eSIMs sold/used
    - Country of export
    - Device types
- Subject to **technical and financial audits**.

8. Restrictions and Penalties

- Strict prohibition on:
    - Resale to domestic users
    - Use for surveillance or critical infrastructure
- Penalties for misuse as per Section 42 of the Telecommunications Act, 2023.

9. Validity and Renewal

- Initial validity of **5 years**, renewable based on performance and compliance.
- Subject to revocation if used for unauthorized domestic deployment.

10. Customs and Inter-Agency Coordination

- Coordinate with **DGFT and CBIC** to establish a secure export compliance mechanism.
- Device-SIM bundling must be reflected in **e-way bills and export manifests**.

Optional Clauses Based on Policy Objectives

Clause Type	Description
Value Addition	Encourage assembly or testing of devices in India before export under Make in India
IMEI/SIM Pairing Mandate	Prevent grey market diversion by mandating hardware-SIM pairing
Use Case Filing	File a use case declaration for each product model and export batch

Regulatory Reference

- **Section 3(1)(a)** of the Telecommunications Act, 2023: Empowers the Central Government to authorise entities to provide telecommunication services.
- Should align with:
    - National Cyber Security Policy
    - M2M/IoT framework (TRAI recommendations)
    - Import/export regulations under DGFT and CBIC

(a) Eligibility conditions for the authorisation :

Comments :

If a **new service authorization** is introduced under **Section 3(1)(a)** of the **Telecommunications Act, 2023** for the **sale of foreign telecom service providers' SIMs/eSIMs** in India for **M2M/IoT devices meant for export**, the **eligibility conditions** must ensure:

- Regulatory oversight
- National security safeguards

- Accountability of the licensee
- No misuse for domestic telecom services

Below are the **proposed eligibility conditions** for such authorization:

Proposed Eligibility Conditions for Authorization under Section 3(1)(a) :

(Sale of Foreign SIMs/eSIMs for M2M/IoT Export Use)

1. Legal Entity Status

- The applicant must be a **company registered in India** under the Companies Act, 2013.
- **Partnership firms, individuals, or sole proprietors** shall not be eligible.

2. Foreign Operator Partnership

- The applicant must have a **valid and verifiable agreement** or MoU with the **foreign telecom service provider** whose SIMs/eSIMs are to be sold.
- The foreign operator must be:
  - **Licensed** in its home country,
  - Not listed on any **international or Indian sanctions list**, and
  - Not flagged under any **national security watchlists**.

3. Experience & Technical Capacity

- The applicant must demonstrate **minimum 3 years of experience** in:
  - M2M/IoT device manufacturing, or
  - SIM/eSIM provisioning and export logistics, or

    - Operating under M2M/IoT authorization issued by DoT or other competent authorities.

(This clause may be relaxed for startups under DPIIT-recognized schemes with safeguards.)

4. Net Worth Requirement

- The applicant must have a **minimum net worth** of ₹1 crore (or as prescribed by DoT/TRAI from time to time) to ensure financial credibility.
- Net worth must be certified by a Chartered Accountant and supported by the latest audited balance sheet.

5. Clean Regulatory Track Record

- The applicant must:
    - Not be **blacklisted** by DoT, MeitY, TRAI, or any other Government body.
    - Not be involved in any pending **legal or criminal proceedings** related to telecom misuse, IPR violation, or cyber offences.

6. Infrastructure Requirements

- Must have:
    - A **registered office** in India,
    - Secure data storage and **customer traceability system** compliant with **DoT and CERT-In** standards,
    - Ability to **maintain records** of all SIMs/eSIMs sold and their destination devices.

7. Undertaking on Usage Limitation

- The applicant must submit a **legal undertaking** that:
  - The SIMs/eSIMs sold will be used **only in M2M/IoT devices exported outside India**.
  - No usage will occur **on Indian telecom networks**.
  - The company will comply with **any future directions** from DoT, TRAI, CERT-In, or other statutory bodies.

8. Traceability and Export Compliance

- Applicant must have systems to ensure:
  - **One-to-one mapping** of SIM/eSIM with export device IMEI/MAC ID.
  - Documentation for **customs clearance/export tracking**.
  - Maintain a **device export compliance register** for minimum 5 years.

9. Security Clearance

- Subject to mandatory **security clearance** from the Ministry of Home Affairs (MHA) if required.

10. Other Conditions

- The applicant must not offer or advertise **any service resembling telecom services within India** using the foreign SIMs/eSIMs.
- Any use in **domestically deployed devices** shall be considered a violation and subject to penalties.

Regulatory Rationale

These eligibility criteria are based on:

- Section 3(1)(a) of the **Telecommunications Act, 2023**
- National Security considerations
- DoT's existing policies for **ILDOs, VNOs, and M2M Service Providers**
- TRAI recommendations on **IoT and cross-border SIM use cases**

(b) Application processing fee for the authorisation :

Comment :

If a new service authorisation is introduced under **Section 3(1)(a)** of the **Telecommunications Act, 2023** for permitting the **sale of foreign telecom service providers' SIMs/eSIMs in India** for **M2M/IoT devices meant for export**, the **Application Processing Fee** should be carefully structured to:

- Ensure **regulatory cost recovery**
- Maintain **entry seriousness**
- Not hinder **innovation or exports**, especially for Indian startups and SMEs

Recommended Application Processing Fee Structure

1. Fixed One-Time Non-Refundable Application Processing Fee

Applicant Category	**Recommended Fee (INR)**	**Remarks**
General (Large Enterprises)	As per TRAI recommendation	For well-established firms or MNCs
Startups (DPIIT-recognised)	As per TRAI recommendation	To promote innovation and export readiness

Applicant Category	Recommended Fee (INR)	Remarks
MSMEs (as per MSME Act)	As per TRAI recommendation	Moderate fee to encourage participation
Renewal/Amendment Applications	As per TRAI recommendation	For minor changes or renewals

2. Fee Payment Terms

- The fee shall be:
  - **Non-refundable**, regardless of approval/rejection.
  - Payable **electronically** through Bharat Kosh or designated DoT payment portal.
  - Linked with a **unique application reference number** for audit and tracking.

3. Fee Review and Revision Clause

- The processing fee may be **reviewed every 3 years** by DoT based on:
  - Volume of applications
  - Regulatory cost changes
  - Industry feedback

Justification for Proposed Fee

Principle	Justification
Cost Recovery	Covers administrative processing, due diligence, security vetting, etc.
Barrier-Free Entry	Tiered fee structure ensures SMEs and startups are not priced out

Principle	**Justification**
Alignment with Other Authorisations	Comparable to fees charged for UL-VNO, ILD, and M2M service registration
Export Promotion	Lower fees for export-only services aligns with Make-in-India and Digital India missions

(c) Period of validity of the authorisation and conditions for its renewal :

Comments :

The following **amendments should be made** concerning **validity and renewal conditions**:

Amendments Regarding Validity of the Authorisation

1. **Initial Validity Period**:
   - The authorisation should be granted for an **initial period of 10 years**, in line with existing norms for other service authorisations under Section 3(1)(a) of the Telecommunications Act, 2023.
   - However, for **pilot or restricted scope operations** related specifically to **M2M/IoT export-only purposes**, a shorter initial validity of **3 to 5 years** may be considered, subject to review based on performance and compliance.
2. **Scope-Specific Validity Clause**:
   - A **separate clause should be added** clearly **defining that the authorisation covers only sales intended for use in devices that are being exported from India** and not for domestic telecom usage.

    - Authorisation should be **non-transferable** and tied to the licensee's ability to ensure that such SIMs/eSIMs are **not activated or used within Indian territory**.

Conditions for Renewal of the Authorisation

1. **Renewal Period**:
    - The authorisation may be renewed for **additional periods of 10 years** each, subject to compliance review.
2. **Compliance Review Criteria**:
   Renewal will be granted only if the following conditions are met:
    - **Full regulatory compliance** with TRAI and DoT conditions regarding:
        - Import/export declarations
        - SIM provisioning records
        - Activation logs
        - Proof of use in exported devices (e.g., shipping bills, IMEI/SIM pair verification)
    - **No violation** of domestic service restrictions (i.e., no domestic usage or roaming on Indian networks)
    - **Annual reporting obligations fulfilled**, including third-party audits or declarations verifying usage in exported products.
3. **Security and Traceability Compliance**:
    - Must demonstrate adherence to **lawful interception and traceability obligations** by the home operator of the foreign SIM.

    - Include **binding MoU with foreign telecom service providers** confirming lawful cooperation on data security, misuse prevention, and SIM tracking.
4. **Performance Metrics**:
    - TRAI may prescribe **KPIs or performance benchmarks**, such as:
        - Number of SIMs provisioned vs. number of exported devices
        - Number of compliance violations or user complaints
        - Network usage logs confirming no domestic traffic generation

(d) Service area of the authorisation :

Comments :

If the activity of **sale of foreign telecom service providers' SIMs/eSIMs for M2M/IoT devices meant for export** is included within the scope of the proposed service authorisation for **sale/rent of international roaming SIMs/global calling cards of foreign operators**, the **Service Area definition** must be **carefully amended** to address regulatory control, jurisdictional clarity, and restriction of domestic use.

Amendments to be Made in Respect of the Service Area of the Authorisation

1. Definition of Service Area

A new clause should be inserted to **clearly delineate** the geographical and functional boundaries of the authorisation, such as:

"The Service Area for this authorisation shall be the entire territory of India, but strictly limited to the distribution and provisioning of SIMs/eSIMs for use in devices that are intended solely for export and shall not include any domestic usage, activation, or roaming on Indian telecom networks."

2. Functional Scope within Indian Territory

- Although the **sales activity** (distribution/logistics) takes place **within India**, the **service delivery (i.e., telecom usage)** must **not occur within Indian networks**.
- Hence, an **exemption clause** should clarify that the **foreign SIMs shall not be used for providing telecom services within the Indian service area**.

3. Export-Only Usage Restriction Clause

Include a **restriction clause** to limit the service area operationally to export-bound activities:

"The authorisation holder shall ensure that all foreign SIMs/eSIMs sold under this authorisation are integrated exclusively into M2M/IoT devices meant for export outside India. Any form of usage or activation within India or on Indian telecom networks is strictly prohibited."

4. Customs/Export-Linked Operational Conditions

- The amendment should also reference **linkages with customs/export documentation**, like:
  - Shipping bills

- E-way bills
- IMEI/SIM pairing logs

This will ensure that the "service area" is not only **territorially defined** but also **functionally regulated**.

5. Monitoring & Audit Rights in the Service Area

“The Licensor shall have the right to conduct physical and digital audits of the authorised entities’ operations, warehouses, and distribution centres across India to verify compliance with the 'export-only' usage clause of this authorisation.”

Sample Draft of Amended Clause on Service Area

“Service Area: The authorisation shall permit the licensee to operate throughout the territory of India for the limited purpose of distribution, warehousing, and provisioning of SIM/eSIM cards of foreign telecom service providers intended for use in M2M/IoT devices meant exclusively for export. The authorisation shall not permit any use, activation, or provisioning of services within Indian territory or on Indian public telecom networks. The licensee shall maintain traceable documentation to demonstrate that each SIM/eSIM has been embedded in an export-bound device.”**

Important Regulatory Safeguards

Aspect	Amendment Recommendation
Territorial Scope	India (for logistics and provisioning), **excluding telecom usage**
Functional Use	Only in **export-bound M2M/IoT devices**

Aspect	**Amendment Recommendation**
Network Restriction	**Prohibit use on Indian telecom networks**
Monitoring	Allow **audits** of service points, export documents, and SIM logs
Binding Compliance Clause	Reference to **DoT/TRAI monitoring and penalties** for violations

(e) Scope of service of the authorisation :

Comments :

The **Scope of Service** defined under such an authorisation must be clear, limited to export-oriented use cases, and compliant with national security and regulatory safeguards.

Below are the recommended **terms and conditions** for defining the **Scope of Service** under this proposed authorisation:

Scope of Service: Sale of Foreign SIMs/eSIMs for Export-Oriented M2M/IoT Use

1. Permissible Activities

The authorised entity shall be permitted to:

- Procure, store, configure, and sell (or rent) **foreign telecom service providers' SIMs/eSIMs**.
- Activate and embed these SIMs/eSIMs **only in M2M/IoT devices intended exclusively for export** from India.

- Provide integration support, quality testing, device-SIM pairing, and provisioning services related to the export of such devices.
- Maintain a secure digital infrastructure for authentication, remote provisioning (via SM-DP/SM-SR), and compliance tracking.

2. Usage Limitation

- The **SIMs/eSIMs shall not be activated or used within Indian territory** under any circumstances.
- Domestic usage or resale to Indian end-users or enterprises is **strictly prohibited**.
- Any use of such SIMs within India (whether test or operational) will be deemed a **violation of the authorisation** and attract penal action.

3. Export Obligation

- All SIM/eSIM-enabled M2M/IoT devices must be:
    - Manufactured or assembled in India, and
    - Exported out of Indian territory under valid documentation (shipping bills, IEC codes, etc.).
- The authorisation holder must **submit quarterly export compliance reports** to DoT/TRAI.

4. Traceability and Record-Keeping

- Maintain detailed logs of:
    - SIM/eSIM procurement (foreign source, batch details)
    - Allocation records (IMEI/Device IDs paired)
    - Export destinations (countries, buyers, invoices)

- Records shall be preserved for a **minimum of 5 years** and made available on demand by authorities.

5. Security and Lawful Interception (LI) Compliance

- Since the service pertains to foreign SIMs:
  - The authorisation holder must ensure that **no traffic is routed via Indian networks**.
  - In case of any testing or breach, prompt reporting must be made to DoT and appropriate corrective action taken.

6. SIM Lifecycle Management

- Only pre-approved and whitelisted foreign operators' SIMs shall be allowed.
- Remote provisioning, revocation, and profile changes must be logged and geo-fenced to ensure they remain inactive in India.

7. No Interconnection with Indian Networks

- The service must **not involve any interconnection or peering** with public or private Indian telecom networks.
- Internet breakout, voice, or SMS services using such SIMs within India are expressly **forbidden**.

8. Technology Neutrality

- The authorisation will be **technology-neutral**, covering:
  - 2G/3G/4G/5G/LPWAN/eSIM (GSMA-compliant)
  - Narrowband-IoT, LTE-M, Satellite-enabled IoT (as applicable)

- However, each SIM must be tied to a specific **device class and export purpose**.

9. Restrictions on Roaming & Resale

- The authorisation shall not confer the right to:
    - Offer international roaming services to Indian users
    - Resell or sub-license to other entities without DoT permission

10. Service Area

- The authorised activity shall be **India-wide**, but **only for warehousing, configuration, and export**.
- The actual telecom service shall be **entirely outside Indian jurisdiction**, falling under the regulatory domain of the foreign operator's home country.

Additional Compliance Requirements:

- Valid **Import/Export Code (IEC)** registration
- Compliance with **DGFT export norms** and **customs clearance**
- Registration under the proposed **Authorised M2M Connectivity Provider** framework (if introduced)

(f) Authorisation fee : As per the TRAI.

(g) Know-Your-Customer (KYC) requirements of the customers of the SIM/eSIM;

Comments :

The **Know Your Customer (KYC)** framework should be specially designed to:

- Ensure **traceability and accountability**,
- Prevent **misuse of foreign SIMs in India**,
- And align with **national security and export compliance norms**.

Proposed KYC Requirements for Customers of Foreign SIMs/eSIMs under the Authorisation

1. Customer Definition

KYC obligations shall apply to:

- **Manufacturers, exporters, and system integrators** in India procuring foreign SIMs/eSIMs for embedding in M2M/IoT devices meant for export.
- Any **importer or agency** authorized to handle these SIMs before export.

2. KYC Documentation Requirements

The authorised entity must collect and verify the following for **each customer (B2B client)**:

(a) For Indian Business Entities (Exporters/System Integrators):

- Certificate of Incorporation / Udyam/MSME Registration
- PAN and GST Registration
- IEC (Import Export Code) issued by DGFT

- Proof of office address (utility bill/lease)
- Board Resolution or Authorised Signatory Letter (if applicable)
- Contact person’s Aadhaar/PAN/Passport (for traceability)

(b) For Foreign Buyers (if directly involved):

- Business registration certificate in home country
- Valid import license (if applicable)
- End-user declaration confirming:
    - Devices are for use outside India,
    - SIMs will not be reimported into India

3. Device-Specific Mapping (IMEI/SIM Pairing)

- The KYC process shall include **linking each SIM/eSIM profile with a specific M2M/IoT device ID**, such as:
    - IMEI / EID / MAC address / Device Serial No.
- Maintain logs of:
    - SIM batch → Device model → Export Invoice → Destination Country

4. Record Maintenance & Audit Trail

- KYC records must be **digitally stored** in a secure and retrievable format.
- Retention Period: **Minimum of 5 years** from the date of export or termination of service.
- All records must be made **available to DoT/TRAI/LEAs** on request.

5. Prohibited KYC Practices

- No sale without verified export documentation.
- No bulk anonymous sale without linkage to a licensed exporter.
- No use of Aadhaar for private eKYC under current restrictions unless UIDAI-compliant architecture is used.

6. Geofencing and Provisioning KYC

- Provisioning of eSIM profiles (via SM-DP/SM-SR) must include a **geo-fencing tag** preventing use or activation within Indian territory.
- The provisioning platform should be linked to verified KYC accounts.

7. Periodic KYC Verification and Reporting

- The licensee must submit **quarterly KYC compliance reports** to DoT/TRAI, including:
    - Number of customers onboarded
    - Total SIMs/eSIMs provisioned and exported
    - Anomalies or suspected misuse (if any)

8. KYC Compliance Certification

- Authorisation holders may be required to undergo periodic **KYC compliance audits** by a DoT-empanelled auditor.
- A self-certification and compliance affidavit should be filed **annually**.

Optional Measures (to be considered by regulator):

- Integration with **CDR/IPDR logging** (even for foreign SIM provisioning)
- **IMEI registration** of exported devices via CEIR-like export module
- **Customs interface** for auto-verification of export declarations during SIM provisioning

(h) Period for which a foreign SIM/ eSIM should be permitted to remain active in India for testing purposes :

Comments :

A **strictly limited and controlled timeframe** must be defined for the **activation of such foreign SIMs/eSIMs within India for testing purposes only**.

Proposed Regulatory Guidelines: Activation Period for Testing Foreign SIMs/eSIMs in India

Objective of Testing Period

The intent of allowing activation in India is **only for limited pre-export testing** of device-SIM integration, such as:

- Connectivity handshake checks,
- Firmware update delivery validation,
- Device-SIM pairing validation,
- Remote provisioning testing (SM-DP+/SM-SR platforms),
- Basic QoS / packet exchange verification.

Recommended Conditions and Limits

1. Permitted Testing Duration

- A foreign SIM/eSIM may be **permitted to remain active in India** for **a maximum of 30 days per device** (calendar days, not usage days) **prior to export**.

- In special cases (e.g., complex configurations, satellite-linked IoT, etc.), **extension up to 60 days** may be allowed **only with prior approval** from the DoT/authorized nodal agency.

2. Activation Declaration & Pre-Registration

- Each test activation must be **pre-registered** with:
  - Unique Device ID (IMEI/EID),
  - SIM/eSIM ID (ICCID),
  - Foreign operator profile,
  - Expected export destination,
  - Start & end date of testing in India.
- Must be submitted via a secure online portal for traceability.

3. Geofenced and Limited Network Access

- SIM/eSIM must be **provisioned on test profiles** with:
  - Geo-fencing to restrict data transmission outside test parameters,
  - No access to Indian telecom subscriber services,
  - Throttled or sandboxed connectivity (e.g., via secure APNs).

4. Logging and Reporting

- All test traffic must be **logged and reported** to the DoT at the end of the test window.
- Log must contain:
  - Time of activation/deactivation,
  - Location of usage (via GPS/IP traces),
  - Data packets exchanged.

5. Automatic Deactivation and Export Binding

- The SIM/eSIM must be **automatically deactivated** at the end of the declared test period.
- Proof of export of the device (shipping bill, invoice) must be linked with the tested SIM to prevent misuse.

6. Non-Compliance Penalty

- Usage of foreign SIMs beyond the permitted testing window within India will be considered a **violation of authorisation conditions**.
- Penalties may include:
    - Suspension of the license,
    - Financial fines,
    - Blacklisting of the SIM batch or foreign operator.

Optional Clauses (Regulator Discretion)

National Security:

- Mandatory **remote disabling capability** must be provisioned by the authorisation holder in case of misuse or interception alerts.

Integration with CEIR or Central SIM Registry:

- Test-activated devices may be temporarily registered with a **CEIR-like registry for export-bound devices**, ensuring device traceability and export compliance.

Designated Test Zones:

- DoT may notify certain **test zones or labs** where activation of such foreign SIMs for testing is permitted (e.g., SEZs, IoT testing labs).

Summary Table: Testing Period Guidelines

Parameter	Specification
Max Testing Period (Standard)	30 calendar days
Extended Period (With Approval)	Up to 60 days (with documented justification)
Pre-Registration Requirement	Yes – ICCID, IMEI/EID, foreign operator ID, location, timeline
Network Access Restrictions	Geo-fenced, throttled, test APN only
Logs and Reports	Mandatory submission post-test to DoT
Export Binding	Device must be exported post-testing; linked with shipping details
Penalty for Overuse/Misuse	Suspension, fines, blacklisting, and criminal action (if wilful misuse found)

(i) Penalties for non-compliance :

A **robust penalty framework** is essential to prevent misuse, protect national security, and ensure adherence to export-only restrictions.

Below are detailed recommendations on **Penalties for Non-Compliance**:

Penalties for Non-Compliance under the Proposed Authorisation

1. Legal Foundation

Penalties may be imposed under:

- **Section 46**, **Section 47**, and **Section 51–52** of the **Telecommunications Act, 2023**, and
- Specific conditions notified in the **Licence/Authorisation document** under **Section 3(1)(a)**.

2. Types of Non-Compliance and Corresponding Penalties

Type of Violation	Suggested Penalty
a) **Sale or activation of foreign SIMs for use within India**	₹10 lakhs per violation + cancellation of specific SIM batch + temporary suspension of authorisation
b) **Failure to deactivate test SIMs after permitted window (30–60 days)**	₹5 lakhs per SIM + blacklisting of operator profile for future import
c) **Failure to maintain or produce KYC, IMEI mapping, or export logs**	₹2 lakhs per missing record + compliance audit at licensee's cost
d) **Resale or transfer of foreign SIMs to third-party without authorisation**	₹15 lakhs per transaction + license suspension
e) **Use of unauthorised foreign telecom operators' SIMs**	₹10 lakhs per operator + mandatory destruction of unlisted SIM inventory
f) **Data routing or service interconnection with Indian networks**	₹25 lakhs + criminal liability under national security provisions (with reporting to LEAs)
g) **Filing of false information or documents with DoT/TRAI**	₹20 lakhs + blacklisting of licensee for 3 years
h) **Non-submission of quarterly compliance reports**	₹1 lakh per delayed report per week

Type of Violation	Suggested Penalty
i) **Improper provisioning of eSIM (no geo-fencing/test limitations)**	₹10 lakhs + technical audit of provisioning system
j) **Export of device without linked SIM documentation / misuse in re-imported goods**	₹5 lakhs per device + intimation to DGFT for export blacklisting

3. Graduated Penalty Framework

Penalties may be applied on a **graded basis**:

- **First Offence**: Financial penalty + Show Cause Notice
- **Second Offence**: Higher fine + Temporary Suspension of Services (15–30 days)
- **Third/Subsequent Offence**: Permanent cancellation of authorisation + Entity blacklisting + criminal proceedings (if national security risk is proven)

4. Compounding and Recovery

- Penalties shall be **non-compoundable** where public safety or cross-border misuse is involved.
- For civil breaches (e.g., late filing), DoT may permit **compounding with undertaking and correction**.

5. Compliance Audit and Enforcement

- DoT may conduct **random audits** and technical inspections.
- Authorisation holder must **cooperate with enforcement**, allow data access, and demonstrate compliance infrastructure.

- Failure to submit to audit = deemed violation with separate penalty.

6. Criminal Liability

In cases where SIMs are found to be used for:

- **Espionage, illegal surveillance, terrorism, or smuggling**, etc.,
- The matter shall be escalated to **LEAs and Home Ministry** under national security laws.
- The Telecommunications Act, 2023 **Sections 48–52** provide for **prosecution and imprisonment** in such cases.

7. Suggested Enforcement Provisions in the Authorisation Terms

“Any breach of the Authorisation conditions, including but not limited to activation within Indian territory, violation of permitted testing period, improper KYC, or resale of SIMs, shall attract financial penalty, suspension or cancellation of authorisation, and/or prosecution as per applicable provisions of the Telecommunications Act, 2023.”

Additional Measures (Optional):

- **Whistleblower Clause**: Provision for reporting internal misuse.
- **SIM Reconciliation Audit Mandate**: Half-yearly inventory–export reconciliation.
- **Automatic Penalty Trigger via Portal**: For overdue test SIMs or delayed reporting.

(j) General, commercial, and operating conditions etc. of the authorisation :

Comments :

A robust framework of **general, commercial, and operating conditions** must be prescribed to ensure national security, regulatory traceability, lawful operation, and proper compliance with the export-only mandate.

Below is a structured proposal on the **terms and conditions**:

TERMS & CONDITIONS UNDER THE PROPOSED SERVICE AUTHORISATION

(Foreign SIM/eSIM Sales for Export-bound M2M/IoT Devices)

A. GENERAL CONDITIONS

1. **Authorisation Type & Purpose**
   - This authorisation allows the **procurement, storage, configuration, testing, and sale** of SIMs/eSIMs issued by **foreign telecom service providers**, exclusively for embedding into **M2M/IoT devices manufactured/assembled in India for export**.
   - No domestic service provisioning is permitted.
2. **Prohibited Activities**
   - Use or activation of foreign SIMs for **domestic telecommunications** within India.
   - Resale to Indian consumers or B2B entities for **non-export** use.
3. **Territorial Jurisdiction**
   - Operations under this authorisation are **limited to Indian territory** only for:

        - Import and secure storage of SIMs/eSIMs.
        - Testing under permitted limits.
        - Device integration and export logistics.
    - Telecom services themselves **must not be rendered in India**.
4. **Validity & Renewal**
    - Authorisation shall be valid for **10 years** initially, subject to compliance with terms.
    - Renewable in blocks of 5–10 years based on performance and regulatory review.

B. COMMERCIAL CONDITIONS

1. **Tariff Transparency**
    - The entity shall not collect recurring service fees or data/voice tariffs in India from any user.
    - **Only B2B sales margins** on SIM provisioning/configuration may be charged.
2. **No Indian Numbering Resources**
    - No access to Indian **MSISDNs, E.164 numbers**, or **domestic spectrum-based resources**.
    - Services (data/voice/SMS) must be routed entirely outside Indian telecom networks.
3. **Revenue Reporting**
    - Annual submission of revenue details from SIM/eSIM sales and associated device export value.
    - Declaration of no domestic service revenue is mandatory.
4. **Customs & GST Compliance**
    - Proper documentation for import of SIMs and export of devices.

    - GST compliance for commercial transactions within India.

5. **Foreign Operator Tie-up Disclosure**
    - List of all foreign telecom service providers whose SIMs/eSIMs are being handled must be declared and kept updated.
    - Only **GSMA-compliant or ITU-recognised** operators allowed.

C. OPERATING CONDITIONS

1. **KYC and Traceability**
    - Comply with strict **KYC norms** for all Indian buyers (manufacturers/exporters).
    - Maintain detailed logs of:
        - ICCID, IMEI/EID, device pairing
        - Date of provisioning
        - Export invoice and country of destination
2. **Testing Restrictions**
    - Activation in India permitted only for **testing for up to 30 days** (extendable to 60 with DoT approval).
    - Activation logs must be geo-tagged and submitted monthly.
3. **SIM Lifecycle Management**
    - Maintain SIM provisioning and deactivation records.
    - eSIM provisioning to be handled via secure SM-DP+/SM-SR platforms with traceability.
4. **Data Handling and Security**
    - No Indian data storage or processing allowed on foreign SIMs.
    - Ensure foreign operators comply with **data minimization and encryption** standards.
5. **Regulatory Filings**

- Submit:
  - Quarterly KYC and provisioning reports
  - Half-yearly export-reconciliation reports
  - Annual compliance certificate

6. **Audit & Inspection**
   - Authorised officers from **DoT/TRAI** may inspect facilities, data, and systems at any time.
   - Cooperate in security audits, random checks, and investigations.

D. OTHER CONDITIONS

1. **Interoperability and Standards Compliance**
   - Devices and SIMs must comply with **GSMA Embedded SIM specifications**, and any DoT-specified security guidelines for M2M/IoT.
2. **Cybersecurity & Remote Deactivation**
   - Licensee must be capable of remotely deactivating SIMs upon DoT/LEA instruction.
3. **Termination & Exit Clause**
   - Authorisation can be **revoked** in cases of:
     - National security threat,
     - Willful breach,
     - Misuse of foreign SIMs within India.
   - Exit must involve proper **deactivation of unexported SIMs** and closure report.

Summary Table: Key Conditions

Category	Conditions
General	Export-only scope, 10-year validity, geo-fencing, no domestic telecom use
Commercial	No tariffs from Indian users, GST compliance, revenue declaration
Operating	30-day test SIM use limit, full KYC, traceability, GSMA eSIM standards
Compliance & Audit	Quarterly reports, DoT audit access, secure provisioning & data logs
Penalty Clause	Fines, suspension, or criminal referral for misuse (See previous answer for penalty grid)

Would you like this converted into a **formal draft notification**, **licence template format**, or **PowerPoint briefing** for stakeholders? I can also cross-compare with **international frameworks** (e.g., EU RSP, US FCC export exemptions) if needed.

Cross Comparative Analysis :

cross-comparative analysis between the proposed **India-specific service authorisation** (under Section 3(1)(a) of the Telecommunications Act, 2023) for **foreign SIM/eSIM sales for export-bound M2M/IoT devices**, and relevant **international frameworks**, specifically:

- **EU Regulatory Framework** (RSP/GSMA-based provisioning)
- **US FCC and BIS Export Regulations**
- **GSMA IoT & eSIM Specifications** (Global non-binding standards)

Comparative Table: India vs EU vs US (Export & SIM/eSIM Regulation for IoT)

Parameter	India (Proposed)	EU (RSP, RED, GDPR, etc.)	US (FCC + BIS + EAR)
Scope	Sale/provisioning of foreign SIMs/eSIMs for **export-only** M2M/IoT devices	EU-wide **remote provisioning** allowed with full operator license for both domestic and cross-border use	US regulates both domestic use and **export of devices/services** via **FCC Part 15, 22** and **EAR**
SIM/eSIM Management	Must be GSMA-compliant; only test-activated for 30–60 days; export-bound	Follows GSMA **Remote SIM Provisioning (RSP)** architecture; cross-operator profile management is permitted	GSMA RSP optional; strict device-level regulation (RF emissions, interoperability) under **FCC ID rules**
Domestic Usage Restriction	**Strictly prohibited**	No such restriction; operators can offer roaming/M2M eSIMs across EU countries	No blanket ban; **FCC requires licensing for domestic transmission**, but foreign profiles can be used under M2M exemptions
Testing Period in Territory	Up to **30 days**, extendable to 60;	No specific limit for testing if within	Devices may be tested pre-export; requires **RF testing**

Parameter	India (Proposed)	EU (RSP, RED, GDPR, etc.)	US (FCC + BIS + EAR)
	must be geo-fenced and logged	compliance; CE marking is mandatory for market entry	**clearance** and labelling if transmitting domestically
KYC / User Verification	Mandatory B2B KYC, IMEI/ICCID mapping, device–SIM–export invoice linkage	GDPR-compliant data handling; B2B and consumer models coexist; no mandatory IMEI/ICCID linkage at SIM level	Not required at SIM level; however, **export declaration and end-user verification** needed for BIS-controlled countries
Data Routing Restrictions	No data traffic from India allowed; SIMs/eSIMs must not use Indian networks	No such restriction; regulated under **GDPR and ePrivacy** if EU user data is processed	Data routing generally unregulated unless involving embargoed nations or personal data violations
Network Interconnection	Not permitted with Indian telecom networks	Allowed if operator is licensed in-country or has roaming agreements	Allowed under MVNO/M2M models with regulated network access
Lawful Interception Compliance	No interception within India as services are foreign; logs and reporting mandatory	Lawful interception required under **EU ETSI LI** standards if	LI obligations apply to domestic operators; **CALEA** mandates interception capabilities

Parameter	India (Proposed)	EU (RSP, RED, GDPR, etc.)	US (FCC + BIS + EAR)
		operator is active in EU	
Export Documentation Requirements	Mandatory: IEC, shipping bills, customs, linked SIM logs	Requires CE conformity for devices; no special SIM-related export regulation	Requires **BIS Export Control Classification Number (ECCN)** and, in some cases, end-user certificates
Penalties for Misuse or Domestic Use	Severe: Fines ₹5–25 lakhs, license cancellation, criminal referral	Regulator-led action depending on data breach or illegal transmission	Civil/criminal penalties under **FCC**, **BIS**, or **ITAR** for controlled technologies
Authorisation Validity & Renewal	10 years initially, renewable in blocks of 5/10 years	Typically indefinite if compliance maintained	Annual or multiyear licensing under FCC or BIS depending on scope
Operator Partnership Disclosure	Mandatory: Only GSMA/ITU-recognised foreign TSPs allowed	No such restriction; commercial partnerships disclosed to national regulators where applicable	Encouraged for security vetting but not mandatory under FCC rules

Highlights of International Best Practices Relevant to India's Proposed Framework

EU (RSP & eSIMs)

- **Highly liberalised** environment for cross-border M2M/IoT communications.
- eSIM profiles may be remotely provisioned by the OEM at any time.
- SIMs can remain active indefinitely inside the EU and roam.
- Focus is more on **GDPR/data protection** and **CE conformity**, not SIM activation limits.

US (FCC & BIS)

- Emphasizes **spectrum regulation**, **export control**, and **national security vetting**.
- Export of devices with SIMs must comply with **EAR classifications** and **DoC licensing**.
- Devices using unlicensed foreign telecom services **must not operate domestically** unless explicitly authorized.

Suggestions :

1. **Adopt GSMA RSP Compliance**: Ensure foreign eSIMs follow GSMA RSP architecture for secure and controlled provisioning.
2. **Enforce Export Linkage**: Like the US BIS model, mandate device–SIM–invoice mapping with customs data integration.
3. **Limit Domestic Activation**: Unlike EU/US, India's policy rightly prohibits domestic usage — retain strict control on domestic test windows.

4. **Embed Data Traceability Mandate**: Emulate EU's GDPR-grade compliance for logs, device ID linkage, and lawful traceability.
5. **Leverage CEIR & Sanchar Saathi**: Use India's existing device tracking frameworks (IMEI/CEIR) for enforcement support.
6. **International Operator Vetting**: Mandate a whitelist of GSMA/ITU-recognized TSPs as done in the US FCC MVNO supervision model.

and

(k) Any other aspect. Please provide a detailed response with justifications.

Comments :

Here is a **comprehensive regulatory framework** for the proposed **new service authorisation under Section 3(1)(a) of the Telecommunications Act, 2023**, to regulate the **sale of foreign telecom service providers' SIMs/eSIMs in India** for **use in M2M/IoT devices meant exclusively for export purposes**.

TERMS & CONDITIONS FOR THE NEW SERVICE AUTHORISATION:

(a) Eligibility Conditions for the Authorisation

1. **Registered Entity**: Only Indian entities (Company/LLP/SEZ Unit) registered under Companies Act or LLP Act with valid Import-Export Code (IEC).
2. **Net Worth Criteria**: Minimum net worth of ₹50 lakhs and positive net assets for the last 2 financial years.
3. **No Previous Blacklisting**: The applicant must not have been penalized or blacklisted by DoT, TRAI, or security agencies.

4. **Foreign Tie-up**: Legally valid agreement with the foreign SIM/eSIM provider (including GSMA-certified Remote SIM Provisioning entity) must be submitted.
5. **Data Protection Undertaking**: Undertake compliance with India's Digital Personal Data Protection Act, 2023, and any cyber security norms laid by CERT-In or DoT.

Justification: To ensure credible, export-oriented players with traceable ownership and regulatory accountability are authorised.

(b) Application Processing Fee

- ₹1,00,000 (non-refundable), paid at the time of application.
- Covers background, financial, and technical scrutiny, along with coordination with security agencies.

Justification: Consistent with other telecom authorisations like UL-VNO or ILD/NLD, and to deter frivolous applications.

(c) Period of Validity & Conditions for Renewal

- **Initial Validity**: 10 years.
- **Renewal**: For further 10 years, subject to:
    - Timely payment of renewal fee.
    - Demonstrated compliance with reporting/KYC norms.
    - No violation of national security or misuse.

Justification: Allows stable business continuity with periodic oversight and compliance checks.

(d) Service Area of the Authorisation

- **Pan-India** operation allowed but **usage restricted only for export-bound devices**.
- No domestic retail service or SIM activation for use within Indian territory.
- Devices can be tested in approved Indian labs or factory premises before export.

Justification: Prevents circumvention of Indian telecom market and ensures purpose-specific authorization.

(e) Scope of Service of the Authorisation

- Import, provisioning, storage, and bundling of foreign telecom SIM/eSIMs into IoT/M2M devices for export.
- Provisioning of test connectivity for integration/testing (with time-limited access).
- Prohibition on providing telephony/data services to Indian end-users.
- Compliance with GSMA's RSP for eSIM-based provisioning.

Justification: Clearly defines boundary for export-centric activity and prevents unauthorized domestic telecom usage.

(f) Authorisation Fee

- One-time fee: ₹10,00,000 (for 10-year licence).
- Annual regulatory compliance fee: ₹1,00,000.
- Security audit & compliance verification: ₹50,000/year (if applicable).

Justification: Balanced model – allows DoT to cover regulatory costs while supporting Indian export ecosystem.

(g) Know-Your-Customer (KYC) Requirements

- **Device-level KYC**: All devices containing foreign SIMs must be tagged with:
    - IMEI/Serial Number
    - MAC address
    - Embedded ICCID/eUICCID
- **Batch Reporting**: Each export consignment must be digitally reported to DoT/DoC, linking device identifiers to end destination.
- **Lab Testing KYC**: During testing/demo in India, traceable B2B entity KYC with location must be filed.

Justification: Protects against SIM misuse in India and ensures accountability in global deployment.

(h) Period for Active SIM/eSIM Testing in India

- Foreign SIM/eSIM may remain **active for up to 90 days** in India:
    - In designated test labs or premises approved by MeitY, TEC or DoT.
    - Logs must be submitted post-testing.
    - SIM must be deactivated post-testing or exported.

Justification: Enables integration, debugging, and conformance testing without enabling grey-market operations.

(i) Penalties for Non-Compliance

Violation	Penalty
Activation of SIM for domestic use	₹10,00,000 per instance + Cancellation
Failure to submit batch logs or KYC	₹2,00,000 per batch
Using foreign SIM for UCC/spam	₹5,00,000 + TRAI ban
Repeat violation	Blacklisting for 5 years
National Security breach	Prosecution under Indian Penal Code & IT Act

Justification: Strong deterrence ensures strict conformance, in line with telecom sovereignty priorities.

(j) General, Commercial & Operating Conditions

1. **Reporting Obligations**:
    - Quarterly report of:
        - No. of SIMs/eSIMs imported
        - Device models integrated
        - Destination countries
        - Testing activities in India
2. **Prohibited Actions**:
    - No resale to domestic users.
    - No Indian mobile number portability (MNP).
    - No connection to Indian PSTN/VoIP without separate license.
3. **Audits & Compliance**:
    - Annual audit by DoT/TRAI-appointed agency.
    - Random inspection rights for DoT/TRAI/CERT-IN.
4. **SIM Bank Registry Compliance**:

  - Mapping of foreign SIMs/eSIMs with DoT’s central SIM Bank Registry to prevent grey-market eSIM swaps.
5. **Labeling/Packaging Norms**:
   - Each device must mention: “FOR EXPORT ONLY – Not for Indian telecom usage”.

Justification: Ensures responsible business practices, separation from domestic ecosystem, and security traceability.

(k) Additional Regulatory Aspects to Consider

1. **Remote Provisioning Platform Certification**:
   - eSIM RSP platforms must be certified by TEC or GSMA.
2. **Integration with Customs/ICEGATE**:
   - Real-time reporting of SIM-enabled device exports to ICEGATE/DGFT.
3. **Cybersecurity & Surveillance Coordination**:
   - Authorisation holder must install lawful interception (LI) test module if testing/OTA provisioning is performed in India.
4. **Exit Clause**:
   - In case of closure of operations, leftover SIMs must be deactivated and certified as destroyed/exported.
5. **Foreign Exchange Monitoring**:
   - Remittance declarations and receipts linked to device sale to ensure export authenticity.
6. **UCC Prevention Undertaking**:

- Entities must ensure SIMs are not used for Unsolicited Commercial Communication (UCC) through foreign number spoofing.

CONCLUSION:

This proposed framework balances **India's regulatory priorities, data sovereignty, security concerns, and ease of doing export business**. It aligns with:

- **National Digital Communication Policy (NDCP) 2018**,
- **Telecommunications Act, 2023 (Sec 3(1)(a))**, and
- International norms (EU RSP, US M2M carve-outs).

Q3. Alternatively, in case it is decided to include the activity of the sale of foreign telecom service providers' SIMs/ eSIM cards in India for the use in M2M/ IoT devices meant for export purposes within the scope of the proposed service authorisation for the sale/ rent of international roaming SIM cards/ global calling cards of foreign operators in India, what amendments should be made in respect of the following terms and conditions of the said service authorisation:

(a) Scope of service :

Comments :

The **"Scope of Service"** clause in the authorisation must be **amended and clarified** in the following way:

Proposed Amendment to "Scope of Service" Clause

Current Scope (Indicative Wording):

“The Authorisation permits the licensee to sell or rent international roaming SIM cards or global calling cards of foreign operators within India, primarily for outbound international travellers.”

Proposed Amended Scope of Service (Revised Draft):

“The Authorisation permits the licensee to:

(a) Sell or rent international roaming SIM cards or global calling cards of foreign telecom service providers in India, intended for use by outbound international travellers; and

(b) **Sell embedded SIMs (eSIMs) or physical SIM cards of foreign telecom service providers in India to manufacturers, exporters, or system integrators** for use in **Machine-to-Machine (M2M) and Internet of Things (IoT) devices**, **exclusively meant for export purposes**, subject to adherence to applicable data security, Know-Your-Customer (KYC), and device registration norms as may be specified by the Department of Telecommunications (DoT).

The licensee shall ensure that such SIMs/eSIMs are:

- Not activated for commercial use within the territory of India except for limited-duration testing as permitted under regulatory guidelines;
- Mapped and tagged to export-bound IoT/M2M devices under valid export documentation;

- Not sold to or activated for individual domestic consumers or for permanent in-country usage.”

Justification for Amendment

1. **Clarity of Dual Use:** The amendment ensures that the existing authorisation holder can engage in both B2C (international roaming users) and B2B (export-oriented IoT/M2M vendors) models.
2. **National Security Safeguards:** Use of words like *“export-bound”*, *“limited-duration testing”*, and *“mapped to devices”* ensures SIMs/eSIMs are not misused in India.
3. **Regulatory Control:** Explicitly mentioning **compliance with DoT/KYC/data localization norms** protects national telecom sovereignty.

Alignment with International Practices

- **EU eSIM RSP Regulations** allow export-mapping of profiles linked to devices being manufactured in the EU.
- **U.S. FCC Rules** allow foreign M2M connectivity for exported devices but mandate non-domestic use declarations.
- **GSMA IoT Guidelines** also distinguish between *permanent roaming* and *“test-use before export”* profiles.

Optional Add-on Clauses

It may also propose:

- A **testing duration cap** (e.g., 30 days) for SIMs used during device quality control in Indian facilities.

- A **reporting obligation** to DoT for all SIMs activated under this scope, including IMEI-SIM mappings.

(b) Eligibility conditions for the authorisation :

Comments :

The **“Eligibility Conditions”** clause must be **appropriately amended** to reflect the nature of business, accountability, and national security requirements for such an export-linked activity.

Proposed Amendment to “Eligibility Conditions” Clause :

Current Eligibility (Indicative Wording):

“Any Indian company registered under the Companies Act, 2013 and having Foreign Direct Investment (FDI) within the prescribed limits is eligible to apply for this authorisation.”

Proposed Amended Eligibility Conditions (Revised Draft)

In addition to existing eligibility conditions, the following shall apply when the licensee intends to undertake the activity of sale of foreign telecom service providers’ SIMs/eSIMs for use in M2M/IoT devices meant for export:

1. **Entity Type:** The applicant shall be an Indian company incorporated under the Companies Act, 2013.
2. **Experience Criteria:** The applicant must have demonstrable experience in:
   - M2M/IoT device manufacturing, integration, or
   - International SIM/eSIM distribution, or
   - Export-related telecommunications services.

3. **Regulatory and Security Clearance:**
    - The applicant must obtain clearance from the Department of Telecommunications (DoT) and Ministry of Home Affairs (MHA), particularly under security-sensitive norms if handling eSIM provisioning or international profile downloads.
    - All foreign partnerships or contractual arrangements with global telecom operators must be declared at the time of application.
4. **Infrastructure and Accountability:**
    - The applicant shall have appropriate infrastructure to manage:
        - eSIM Remote SIM Provisioning (RSP) platforms, or secure partnerships with GSMA-certified providers;
        - Testing facilities for short-term activation in India, with logs/reporting capabilities;
        - Traceability mechanisms for mapping SIM/eSIM to export-bound M2M/IoT devices.
5. **Compliance Declaration:**
    - The applicant shall submit an undertaking that such SIMs/eSIMs will not be sold for permanent or commercial use within India and are strictly meant for devices to be exported.
6. **FDI & Control Requirements:**
    - FDI in the applicant company shall be subject to the existing sectoral cap and must comply with Press Note 3

(2020 series) guidelines regarding investments from countries sharing a land border with India.

Justification for These Amendments

- **Security Sensitivity**: eSIMs allow remote profile provisioning; thus, stricter vetting of applicants is needed.
- **Export Use Confirmation**: The experience and infrastructure requirement ensures the service is genuinely used for export-linked IoT/M2M deployments.
- **Alignment with TRAI/DoT Precedents**: Similar criteria exist in M2MSP registrations and in IoT-related UCC and KYC frameworks.

Comparison with International Practice

Jurisdiction	**Eligibility Feature for M2M/IoT SIM Use for Export**
EU	Only entities with GSMA-accredited RSP platforms or OEM status are allowed to embed eSIM profiles for export.
USA (FCC)	Exporters must declare that foreign SIMs are not for use in the U.S.; resellers must have device traceability.
Singapore	Requires registration of each M2M SIM and linkage with export-bound hardware before activation.

(c) Application processing fee for the authorisation :

As per the TRAI recommendation.

(d) Period of validity of the authorisation and conditions for its renewal :

Comments :

If the activity of the **sale of foreign telecom service providers' SIMs/eSIMs for M2M/IoT devices meant for export** is included within the scope of the proposed **international roaming SIM/global calling card authorisation**, the **"Period of Validity and Conditions for Renewal"** must be amended to reflect:

- The extended operational risks (e.g., export compliance),
- Long-term project cycles in IoT/M2M manufacturing,
- National security and accountability audits.

Proposed Amendment to "Period of Validity and Conditions for Renewal"

Revised Clause – Period of Validity

The period of validity of the service authorisation should remain **10 years**, extendable by another **10 years** upon successful renewal, unless otherwise notified by the Department of Telecommunications (DoT).

However, if the licensee undertakes the activity of selling foreign telecom SIMs/eSIMs for use in M2M/IoT devices meant exclusively for export, the following additional conditions shall apply:

Additional Provisions for M2M/IoT-Export Activity

1. **Initial Compliance Period:**
    - During the first **3 years**, the licensee shall be subject to **annual audits** on:
        - SIM/eSIM traceability,
        - Device–SIM binding for export,

        - Short-term activation/testing records,
        - Foreign operator agreements.

2. **Mid-Term Review Clause:**
    - A **mid-term review at the end of 5 years** shall be mandatory to assess:
        - Ongoing compliance with national security, data protection, and KYC norms.
        - Linkage of issued SIMs with actual exports (verified through DGFT/ICEGATE data).
3. **Renewal Conditions:**
    - Renewal shall be subject to:
        - Clean compliance record with respect to TRAI/DoT/KYC regulations,
        - No pending penalties or serious violations,
        - Updated details of foreign telecom tie-ups and Remote SIM Provisioning (RSP) platforms, if applicable,
        - Declaration of any changes in device/application type or scope of export destinations.
4. **Export Compliance Certification:**
    - A certificate from an authorised export agency (e.g., DGFT-recognized body) must be submitted every **two years** affirming that such SIMs/eSIMs are used solely in export-bound devices.

Justification for Enhanced Renewal Conditions

- **Export Cycle Duration:** IoT/M2M devices have long design → testing → production → export cycles (2–5 years).

- **eSIM Lifecycle Risk:** Remote profile provisioning (RSP) may change ownership post-sale. Regular reviews ensure accountability.
- **National Security Oversight:** Periodic reviews allow government to monitor evolving global telecom relations and risks.

Global Comparison

Country	**Validity (IoT SIMs for Export)**	**Review Mechanism**
USA (FCC)	10 years (IoT-focused MVNOs)	Bi-annual self-certification, revocable license
Germany	5 years (GSMA-certified operators)	Mandatory 3rd-party audit for IoT exports
Singapore	3 + 7 years split	Renewal only after device usage reconciliation

Optional Add-on Clauses

- DoT may **reserve the right to suspend** the export activity under this authorisation in case of:
  - International sanctions,
  - National security alerts,
  - Data routing or misuse concerns.

(e) Service area of the authorisation :

Comments :

The **"Service Area"** clause of the authorisation needs to be appropriately amended to address the **distinct operational geography** of both services.

Proposed Amendment to "Service Area" Clause

Current Indicative Clause (for existing services):

"The service area for this authorisation shall be the entire territory of India."

Revised Clause – Dual-Service Area Definition

"The service area under this authorisation shall be defined as follows:

(a) **For international roaming SIM cards and global calling cards:** The entire territory of India, wherein the licensee may sell or rent SIMs/cards to customers intending to travel abroad.

(b) **For the sale of foreign telecom service providers' SIMs/eSIMs for M2M/IoT devices meant for export:**
The entire territory of India, subject to the following conditions:

- Such SIMs/eSIMs shall be sold or embedded only into devices that are **manufactured, assembled, integrated, or prepared for export** within India.
- These SIMs/eSIMs shall **not be activated for commercial use within India**, except for **limited short-term testing or quality control** in designated industrial premises or IoT laboratories registered under applicable government schemes (e.g., MeitY/DoT/SEZs).
- The **end-use of such devices must be outside the territory of India**, and documentary evidence of export must be retained by the licensee for audit purposes.

The licensee shall not sell such SIMs/eSIMs to individual domestic consumers or for usage in devices meant for the Indian market.”

Optional Addendum:

“DoT reserves the right to impose **geo-fencing, profile-usage controls, or activation-restrictions** on such foreign SIMs/eSIMs through policy notifications or technical directives if national security or data sovereignty concerns arise.”

Justification for Amendment

Concern	**Amendment Benefit**
Territorial restriction	Ensures SIMs are not misused within India
Export-specific usage	Reinforces the intent of enabling export-linked M2M/IoT integration
Testing allowance	Allows practical leeway for manufacturers to perform functional validation
Traceability and audit	Facilitates compliance tracking with customs/export regulations

International Practice Comparison

Country	**SIM Service Area Restrictions for IoT/Export**
USA (FCC/CBRS)	Devices using foreign SIMs must declare end-use abroad; domestic use not allowed unless tested in certified labs
EU (RSP/eSIM)	Permits foreign profiles in manufacturing hubs but restricts use within EU unless operator registered

Country	SIM Service Area Restrictions for IoT/Export
Singapore	Authorisation valid nationally, but foreign SIMs must be declared as "for re-export" in licensing terms

(f) Authorisation fee :

As per TRAI Guidelines.

(g) General, commercial, and operating conditions etc. of the authorisation :

Comments :

The **General, Commercial, and Operating Conditions** of that authorisation must be carefully amended to accommodate the unique nature of this specific use-case.

Here is a **detailed proposal of amendments**:

1. Purpose-Specific Operational Scope

Amendment:

The authorised entity should be permitted to sell or lease SIMs/eSIMs of foreign telecom service providers exclusively for use in M2M/IoT devices intended for **export out of India**. These SIMs/eSIMs shall not be used for general telecom usage or activated for regular domestic services in India.

Justification: Prevents circumvention of domestic telecom licensing by foreign entities.

2. Geo-Fencing & Network Access Restrictions

Amendment:

The foreign SIM/eSIM should be **permitted to remain active in India only for a maximum of 30 days** during testing, configuration, or demonstration prior to export. Post this period, activation/use in India must automatically terminate or be blocked by the authorised entity.

Justification: Avoids misuse within Indian territory and ensures purpose-limited temporary activation.

3. KYC & Tracking Obligations

Amendment:

The authorised entity should:

- Undertake **KYC verification** of the OEM or export-manufacturer.
- Maintain a **log of device identifiers (IMEI, MAC, etc.) and export destination**.
- Ensure that each SIM/eSIM is **mapped to a unique device ID** and intended export invoice/shipping documentation.

Justification: Provides traceability, reduces fraud or illegal resale of foreign SIMs in India.

4. Labeling & Export Declaration

Amendment:

All such SIMs/eSIMs must be clearly labelled and classified under **"For export only – Not for domestic use"**, and such declarations must be included in customs export documentation and shipping invoices.

Justification: Distinguishes export-use SIMs from regular roaming cards, helps customs and law enforcement.

5. Network Access Terms

Amendment:

The authorised entity should ensure that **no telecom services (voice/data/SMS)** are consumed through Indian telecom networks beyond the permitted activation period for testing. Any such access shall trigger an automatic deactivation protocol.

Justification: Prevents bypass of Indian telecom network authorisations and spectrum regulation.

6. Data Security & Lawful Interception Compliance

Amendment:

The authorised entity should retain access and provide logs related to foreign SIM/eSIM activity during the testing phase within India. If requested, these logs must be made available to Indian law enforcement and DoT under lawful interception provisions.

Justification: Ensures national security even during the short activation window in India.

7. Revenue Sharing or Levy (If Applicable)

Amendment:

If any service consumption occurs within India (even temporarily), a **prescribed levy or revenue-share** mechanism may be introduced based on the value of service usage or number of activations.

Justification: Ensures fair commercial treatment and avoids revenue loss to Indian telecom ecosystem.

8. Annual Filing & Device-wise Reporting

Amendment:

The licensee should submit an **annual self-certified report** detailing:

- Number of SIMs/eSIMs sold or leased
- Foreign operators involved
- Export destination countries
- Device categories (e.g., EV trackers, smart meters)

Justification: Supports regulatory oversight and trend analysis for export-focused telecom usage.

9. Prohibition on Retail Resale

Amendment:

The authorised entity should not engage in **retail sale to general public** or offer these SIMs/eSIMs via digital platforms (e.g., e-commerce websites) to individuals. Only registered exporters or M2M/IoT OEMs may procure them.

Justification: Prevents misuse as international roaming alternatives by individuals.

10. Penalty Clause for Misuse

Amendment:

Any instance of unauthorised activation or use of these SIMs/eSIMs in India beyond prescribed limits should attract **penalties under the Telecommunications Act 2023**, including potential suspension of authorisation.

Justification: Enforcement clarity.

(h) Any other aspect? Please provide a detailed response with justifications :

Comments :

Here is a **detailed and structured response** outlining the necessary **amendments to the service authorisation** terms and conditions **if the activity of sale of foreign SIMs/eSIMs in India for M2M/IoT devices meant for export** is **included under the proposed service authorisation for international roaming/global calling SIMs** of foreign operators under Section 3(1)(a) of the *Telecommunications Act, 2023*:

Proposed Amendments to the Terms and Conditions of the Service Authorisation

(a) Scope of Service

Amendment:

The scope should include:

"Sale or lease of foreign telecom service providers' SIMs/eSIMs in

India exclusively for use in M2M/IoT devices intended for export outside India. These SIMs/eSIMs must not be activated for domestic telecom usage, except for limited testing.”

Justification:

This limits domestic misuse, clearly distinguishes export-focused usage, and protects Indian network security.

(b) Eligibility Conditions for the Authorisation

Amendment:

The applicant must:

- Be an Indian-registered company under Companies Act, 2013
- Have a valid Import-Export Code (IEC)
- Have tie-ups with foreign telecom operators under documented MoUs
- Be engaged in **manufacturing, assembling, or exporting M2M/IoT devices**
- Maintain infrastructure for customer KYC, activation monitoring, and export verification

Justification:

Ensures legitimate players, prevents misuse by resellers, supports Make-in-India exporters and traceability.

(c) Application Processing Fee

Amendment:

A **moderate one-time fee**, e.g., ₹50,000 to ₹1,00,000 per authorisation, to cover administrative and background verification costs.

Justification:

Aligns with other service-based authorisations and deters non-serious applicants while encouraging MSME exporters.

(d) Period of Validity & Conditions for Renewal

Amendment:

Validity: **5 years**, renewable for further 5-year blocks. Renewal Conditions:

- Continued compliance with export declarations
- No violations of Indian telecom/network usage limits
- Submission of annual device/SIM-wise compliance reports

Justification:

Longer duration supports operational stability and MoU terms with foreign operators, with strong compliance accountability.

(e) Service Area of the Authorisation

Amendment:

The service area shall be **"Pan-India"**, but restricted to authorised manufacturing units/export entities. Activation of these SIMs/eSIMs must be geo-fenced and restricted for use only in test networks during pre-export testing.

Justification:

National coverage for industrial hubs but limited operational telecom footprint within India.

(f) Authorisation Fee

Amendment:

A **modest annual authorisation fee** (e.g., ₹1,00,000 to ₹5,00,000) based on scale of operation (number of SIMs, volume of export turnover), or a **per-SIM slab fee model** may be considered.

Justification:

Ensures cost-recovery and proportional fee burden; avoids entry-barrier for smaller export units.

(g) General, Commercial, and Operating Conditions

Key Additions:

Clause	Amendment	Justification
Activation Window	SIMs/eSIMs may be activated in India for **up to 30 days** for testing only	Prevents long-term illegal usage
KYC Norms	KYC of corporate buyer/exporter (not retail users) + device ID & destination	Ensures traceability
Export Declaration	Mandatory linkage to shipping bill/invoice number under Customs Act	Prevents domestic resale
Prohibited Use	Use in India beyond test window is a violation; triggers penalty/suspension	Ensures legal compliance
Data Retention	Maintain logs of sale, activation, export, device IDs for **3 years**	Enables audit/tracing

Clause	Amendment	Justification
Lawful Interception	Temporary testing usage in India must allow DoT access for lawful interception	Protects national security

(h) Any Other Aspects to be Considered

1. Labeling Requirement

All SIMs/eSIMs must be **permanently labelled "For Export Use Only – Not for Domestic Telecom Use in India."**

Justification: Ensures physical traceability; helps Customs and DoT inspectors.

2. IMEI–SIM/eSIM Mapping

Each SIM/eSIM must be mapped to a unique IMEI/MAC address of the device before export.

Justification: Prevents black-market SIM resale and device spoofing.

3. Audit & Compliance Inspections

DoT/TRAI may conduct periodic inspections/audits or require test-activation logs to verify no Indian network usage beyond declared purpose.

Justification: Maintains regulatory oversight and compliance assurance.

4. Penalty for Violation

Any violation shall attract penalties under *Sections 21, 24, and 33 of the Telecommunications Act, 2023* including suspension, blacklisting, and monetary fines.

Summary Table: Proposed Terms at a Glance

Term	**Proposed Amendment**	**Rationale**
Scope	Export-only M2M/IoT SIMs	Prevent misuse
Eligibility	Indian entity with IEC + OEM/exporter	Ensure credibility
Processing Fee	₹50K–₹1L	Administrative coverage
Validity	5 years	Long-term planning
Service Area	Pan-India (testing only)	Industrial access
Authorisation Fee	₹1L–₹5L annually or slab-based	Fair monetisation
Ops Conditions	Activation limits, KYC, export log, penalties	Full regulatory control
Other Aspects	Labeling, IMEI mapping, audit rights	Prevent abuse, aid enforcement

Q.4 Whether there are any regulatory issues including those related to the agencies such as RBI, customs etc. in respect of the import of foreign telecom service providers' SIM/ eSIM cards for the use in M2M/ IoT devices meant for export purposes? Please provide a detailed response with justifications.

Comments :

Regulatory Issues in Importing Foreign SIM/eSIMs for IoT Devices (India)

SIM cards and eSIM modules are crucial for connectivity in IoT/M2M devices. Importing foreign SIMs for integration in export-bound devices raises multi-faceted regulatory questions.

Background and Context

Indian manufacturers of IoT (Internet of Things) and M2M (Machine-to-Machine) devices are increasingly looking to embed **foreign telecom service providers' SIM cards or eSIM profiles** into their products before shipping them overseas. This allows devices to **instantly connect to local mobile networks in the destination country**, enabling "out-of-the-box" functionality for end-users abroad. For example, a smart appliance or vehicle made in India could contain a pre-installed SIM from an overseas operator so that upon export, it can immediately use that operator's network. However, this practice sits at the intersection of several regulatory domains. Below is a structured analysis focusing on key regulators and laws:

Department of Telecommunications (DoT) – Licensing and Telecom Regulations

Under Indian law, **no telecommunication service can be provided without authorization**, and SIM provisioning is tightly regulated. Until recently, there was **no explicit license category for selling or using foreign SIMs in India**, but DoT handled this via a "No Objection Certificate" (NOC) regime. Notably, DoT's January 2022 policy update allowed **foreign operators to sell/rent international roaming SIM cards in India for**

travelers, but only with an NOC and under strict conditions. These conditions included full **Know-Your-Customer (KYC)** verification (passport, visa, travel details) for each customer and a rule that **such SIMs must not be used on Indian soil except for roaming by travelers**. NOC holders must submit monthly reports to Indian security agencies with details of all SIMs issued and to whom. The NOC is valid 3 years and requires the holder to obtain any other needed clearances (e.g. from RBI or Customs). DoT can suspend or cancel the NOC in the interest of national security or "for the proper conduct of telegraphs" (a term from the old Telegraph Act).

Current challenge: The existing NOC policy was designed for **international roaming SIM cards sold to Indian travelers**, not for IoT manufacturers embedding foreign SIMs. Indian IoT exporters have petitioned DoT, pointing out **practical difficulties in applying the 2022 NOC rules to the M2M/IoT use-case**. For example, KYC documentation meant for individual travelers doesn't map neatly when a SIM is installed in a device that will be sold to a foreign client. Likewise, the 2022 rules *"strictly limit in-India activation"* of foreign SIMs, which is problematic for manufacturers who **need to test or prototype devices in India using the foreign SIM/eSIM before export**. Currently, a foreign SIM obtained under NOC cannot be activated on Indian networks (except incidental roaming), so companies have struggled to do quality assurance on their products. DoT itself acknowledged that **short-duration local activation for testing is often necessary** for export-bound devices, yet the current regime provides no clear allowance for this.

Telecommunications Act, 2023: India overhauled its telecom law with the Telecommunications Act, 2023 (replacing the 1885 Telegraph Act). The new

Act reinforces licensing requirements and broadens the scope of regulated services. Under this Act (and the Unified License framework it envisages), *any provision of telecom services or network access in India requires authorization*. Notably, **M2M/IoT connectivity is explicitly brought under licensing** – providers of M2M connectivity for use within India must obtain an Access Service authorization under the Unified License. While this covers domestic IoT connectivity, it also underscores that **facilitating connectivity, even via foreign SIMs, is a regulated activity**.

Implication: Until such a license or revised NOC policy is in place, importing foreign SIMs for IoT integration operates in a gray zone. Companies currently must seek an NOC exemption on a case-by-case basis. Indeed, **multiple Indian manufacturers have approached DoT for NOCs to import and use foreign SIM/eSIMs in devices meant for export**. The likely outcome is a dedicated **"International M2M Connectivity" authorization** that will spell out the terms under which foreign SIMs/eSIMs can be imported, integrated, and briefly activated for testing in India. Importantly, both industry and regulators concur that **these SIMs/eSIMs should only be operational for live service outside India** – any usage in India must be limited to testing or demo purposes. If a foreign SIM were to be used to provide local connectivity in India (beyond roaming), it would violate licensing norms since the service would bypass Indian licensed networks and security oversight.

Indian SIMs in exported devices: The regulatory issue is two-sided. Just as foreign SIMs in India raise questions, so does the export of devices containing Indian telecom operators' SIMs. Under current Unified License rules, Indian mobile network operators are licensed to provide services within India (with roaming abroad for subscribers traveling). If an IoT manufacturer embeds, say, an Airtel or Jio SIM in a device and sells it to a foreign customer, that device will operate on foreign networks under roaming. Regulators worry this could become **"permanent roaming"** – an Indian SIM used indefinitely outside India by a non-Indian end-user. This scenario is generally disallowed or discouraged: many countries (including India) impose restrictions on permanent M2M roaming to ensure **devices eventually use a local service**. Indian operators would face KYC challenges (the end-user abroad is not their domestic subscriber) and compliance issues, and foreign regulators might object to a large-scale deployment of Indian SIMs in their territory (similar to how India objects to large foreign SIM deployments on its soil). Any new framework will likely clarify that **if Indian telcos' M2M SIMs are used in exported products, they must still comply with Indian licensing (e.g. the manufacturer or the telco must ensure KYC and security monitoring) and any foreign local laws**. In practice, the industry trend is to avoid permanent roaming by using eSIM technology to swap to a local profile when the device reaches its destination. Regulators are essentially nudging toward that model while formulating interim rules to permit the initial foreign SIM integration.

Ministry of Electronics and IT (MeitY) – Data Security and IT Rules

MeitY oversees electronics manufacturing, digital services, and data protection policies in India. While DoT handles telecom licensing, MeitY's concerns in this context revolve around **data security, privacy, and device integrity** for IoT. Several issues fall under its purview:

- **Data Protection:** IoT/M2M devices often collect personal or sensitive data (e.g. location, usage patterns, health metrics). If the exported devices will handle personal data of foreign individuals (say EU citizens), the manufacturer must ensure compliance with applicable data protection laws like the EU's GDPR. GDPR imposes strict requirements on data controllers and processors, including **privacy by design, informed consent, limited purpose use, and cross-border transfer safeguards**. An Indian manufacturer shipping a connected product to Europe could be considered a data **controller** or **processor** under GDPR if it continues to have access to the data. This means implementing measures for **secure data handling, transparency with users, and honouring rights (like data deletion or access requests)**. For instance, any telemetry data sent back to India from EU devices would require a lawful transfer mechanism under GDPR (currently, GDPR allows transfers to India in absence of an adequacy decision if standard contractual clauses or other safeguards are used). Manufacturers need to clearly inform customers about what data is collected and obtain any necessary consents.

- **India's Personal Data Protection Regime:**

Domestically, India's **Digital Personal Data Protection Act, 2023 (DPDP)** is coming into force. While the DPDP Act primarily protects data of persons in India, it reflects MeitY's emphasis on data security and could indirectly affect IoT exporters. For example, if any personal data from the devices (even of foreign users) is processed or stored by an entity in India, robust security controls are required by law. MeitY would expect companies to follow **"data protection by design and by default"** principles, building strong encryption and access controls into IoT products. Additionally, MeitY has been framing IoT security guidelines – covering aspects like device authentication, network security, and encryption standards for IoT/M2M communications. Ensuring that imported eSIMs or SIMs do not introduce vulnerabilities (e.g. ensuring the SIM profiles are securely provisioned and cannot be misused to exfiltrate data) would be part of a compliance checklist.

- **Cross-Border Data Flow & Localization:**

  There is an ongoing policy conversation in India about localization of certain categories of data (though the latest DPDP Act has relaxed blanket localization in favour of notified restrictions). Telecom data is sensitive: under telecom rules, **communication logs and user identifiers must often be accessible for lawful interception and security monitoring by Indian authorities**. A foreign SIM in an IoT device, even if not used in India after testing, raises a question – during testing or manufacture, any data the device transmits will go via a foreign network/cloud. Such **cross-border data transfer** could bypass Indian networks and thereby Indian law enforcement's direct reach. This is one reason the **2022 foreign SIM NOC policy required NOC holders to provide information to security agencies and allowed DoT to suspend services for security reasons**. MeitY, in coordination with DoT and intelligence agencies, should want assurances that allowing foreign SIMs for IoT export **will not compromise national security or cyber security**. Likely, the new authorization will include conditions like: the foreign SIM must not be used for any local connectivity beyond testing, all devices/SIMs details must be logged, and perhaps even that **any data**

collected during in-India testing be stored in India or shared with authorities on request (mirroring obligations on Indian telcos).

- **IoT Device Standards:** MeitY has been involved in setting technical standards and best practices for IoT. The Telecommunication Engineering Centre (TEC, under DoT) issued an **"M2M Security Guidelines"** report, and MeitY has an IoT division that earlier released a draft IoT policy. One relevant aspect is **encryption and cryptographic controls**. SIM cards inherently use encryption (e.g., for authentication on networks). Generally, **commercial encryption used in telecom (like SIM authentication algorithms) is permitted** and telecom licensees must support lawful interception capabilities. As long as the foreign SIM's network usage in India is minimal, encryption isn't a direct regulatory barrier. However, if the IoT device itself uses strong encryption for its data (say end-to-end encryption of sensor data back to overseas servers), it must comply with any Indian encryption export/import controls. Currently, **mass-market encryption products are freely importable**, but India does restrict import of certain high-grade encryption hardware. Standard SIM/eSIM technology would be considered mass-market (used in phones globally) and not subject to special license from MeitY, but companies should ensure compliance with any future **encryption guidelines** that MeitY might enforce for IoT (there has been discussion of mandating decryption capabilities or specific encryption standards for IoT networks).

In summary, MeitY's lens should be on **data and cyber-security**. It should coordinate with DoT to ensure that allowing these foreign SIMs does not create a blind-spot for regulators or a privacy risk. Companies need to follow not just telecom rules, but also IT Act rules (e.g. reasonable security practices under IT Act Section 43A) and upcoming data protection obligations. If the IoT devices handle personal data, **GDPR and analogous laws** in other export markets (like CCPA in California, etc.) must be addressed as part of product compliance.

Reserve Bank of India (RBI) – Foreign Exchange and Payments

Importing SIM cards or eSIM subscriptions from foreign telecom operators involves cross-border commercial arrangements, which brings **foreign exchange regulations** into play. RBI, through the **Foreign Exchange Management Act (FEMA)** and related rules, governs how payments in foreign currency are made and how such transactions are classified.

Payment for Import of SIMs/Services:

If an Indian entity imports physical SIM cards, it must pay the foreign supplier (which could be an operator or an intermediary) in foreign currency. Similarly, if the arrangement involves purchasing an eSIM profile or a bundle of connectivity (data plans) to be embedded in the device, that typically constitutes an import of telecom service. These transactions are generally **permissible current account transactions** under FEMA – telecom services or electronic components are not on any prohibited list. However, importers must follow RBI's procedural requirements: use authorized dealer (bank) channels, adhere to documentation, and use the correct **purpose codes** for remittances (likely "import of telecommunications services" or "import of software/technology" depending on how it's classified). RBI's Master Circular on Imports stipulates that **payments for imports should be**

completed within the stipulated time (usually within 6 months from shipment for normal goods) and any advance payment for imports must be backed by proper documentation or guarantees. In our scenario, an IoT manufacturer might either pay upfront for a batch of SIM cards and a data plan, or have a contract where they pay per active device. As long as these payments are bona fide and properly documented (invoices, import declaration etc.), RBI approval is typically not required – they fall under the automatic route. Indeed, the DoT's NOC terms explicitly note that **the NOC holder is "expected to obtain all required clearances from...RBI"**, implying that companies must ensure FEMA compliance but there isn't a special RBI permit beyond standard forex rules.

Foreign Exchange (Forex) Considerations:

One nuance is **valuation and transfer of assets**. Physical SIM cards themselves are low-value hardware, but what's really being "imported" is the capability to access a foreign network (a service value). If foreign SIMs are imported free-of-cost or on loan (for example, a foreign operator might provide SIMs at no cost, charging only for usage later), this might need to be reflected properly in customs and accounting records (perhaps as having a token value). Moreover, if an Indian company bundles a foreign connectivity service with its device (e.g., "free 1-year connectivity included"), it is essentially reselling a service. **RBI's Foreign Exchange rules would view this as the Indian company first importing the service (paying the foreign provider), then exporting a combined product**. The pricing and invoicing should be set at arm's length to ensure no violation of transfer pricing or misrepresentation of value (particularly if the foreign provider is related or if the service cost is significant). Companies might also need to consider

withholding taxes on payments abroad for services – under Indian tax law, certain cross-border service payments incur Tax Collected at Source or withholding; though telecom services paid to a foreign operator might qualify as import of services for business, potentially subject to a withholding tax unless a tax treaty applies. RBI would indirectly be involved since remittances require submission of Form 15CA/CB for tax compliance.

Repatriation and FEMA compliance:

On the flip side, if for any reason a foreign SIM/eSIM needed to be returned or deactivated and a refund issued, the company must repatriate those funds to India within prescribed time. FEMA has rules for **unutilized import advances and for export earnings repatriation**. For example, if an Indian firm paid for 10,000 SIM profiles but only used 8,000 (and the contract allows refund for unused), the balance should ideally be brought back or managed per FEMA guidelines.

At present, **no specific FEMA restrictions target SIM card imports**, but the involvement of foreign telecom services does raise one regulatory question: Are these foreign SIM-enabled services considered a form of foreign operator doing business in India? RBI, in tandem with DoT, shut down app-based eSIM providers (Airalo, Holafly) earlier in 2024 because they hadn’t obtained DoT NOCs. Part of that issue was consumer protection and security, but also the financial aspect – **Indian customers were paying in rupees for connectivity provided entirely by foreign entities**. In those cases, payments may have been routed through app stores without clear FEMA classification. By contrast, an IoT manufacturer is not reselling to Indian customers, but integrating service for a foreign end-user, so the revenue for the service likely comes from abroad (part of the device sale). That actually is a **foreign exchange inflow**: the Indian exporter charges their overseas client for the device (which includes connectivity cost). Essentially, the Indian company will use a portion of that revenue to pay the foreign SIM provider. This is a normal trade transaction (export earnings and import of input service), but from an **RBI perspective, careful bookkeeping is needed** to net these off correctly. The company may need to demonstrate to banks/regulators that the **foreign exchange being remitted out (for SIM services) is related to an export**, which can help avail benefits or at least ensure compliance. For instance, under FEMA, advance payments for imports above a certain value may require guarantees if goods/services aren't received in 6 months – companies will have to manage such timelines (perhaps by aligning SIM service payments with device delivery).

In summary, **RBI's role is to ensure all cross-border payments are kosher and within the law**. Importing SIMs/eSIM services is allowed, provided one follows standard FEMA rules on imports. Companies should coordinate with banks for proper remittance codes and possibly inform RBI if any unconventional payment model is used. The upcoming regulatory framework might explicitly clarify that NOC/license holders for foreign SIMs must comply with FEMA and even obtain "foreign exchange clearance" if needed (though typically this is handled via AD banks). There is no indication that RBI would impose additional restrictions like caps or special approval for paying foreign telecom operators – it's treated like paying any technology supplier abroad. However, RBI would be concerned if there's any element of revenue sharing that affects telecom revenues taxable in India or if pre-paid instruments are involved (e.g. if the company in India collects money in rupees for a foreign SIM subscription, this starts to look like a cross-border payment service – likely not the case here since the devices are exported). The bottom line is **FEMA does not prohibit this activity**; it simply mandates that the money flows must be transparent and through normal banking channels, with all dues (tax, etc.) taken care of.

Customs and Import Controls

When importing the physical SIM cards or embedded SIM modules, **Indian Customs laws and import policy** come into play. The good news is that **SIM cards are not on any restricted or prohibited import list** – they are classified as a type of electronic storage/"smart card" device. The typical HS Code for SIM cards is **8523.5210** (under HS 8523: "Discs, tapes, solid-state non-volatile storage devices, smart cards..."). Indian tariff listings explicitly have an entry for "Smart cards: SIM cards" under HS 85235210. According to the Indian Customs tariff, **SIM cards are freely importable (Import Policy: "Free")** and carry a basic customs duty of 0%. Only GST (Integrated GST) applies – usually **18% IGST on the value**. In other words, from a pure customs standpoint, **one does not need an import license to bring in SIM cards**; they can be imported like any other electronic component by paying the applicable GST and clearing them through customs.

However, there are a few practical considerations and conditions during import:

- **Declaration and Valuation:**

  Each shipment of SIMs must be properly declared. Even though the intrinsic hardware value of a SIM card is minimal (a few rupees each), customs will require an appropriate valuation. If the SIMs are imported with pre-loaded data plans or airtime, typically the value of the physical card is declared, not the service value. The service (connectivity) is not “imported” at the port – only the tangible goods are. The customs invoice should ideally reflect the cost (if any) of the blank or programmed SIM cards as provided by the foreign operator. If the cards are provided for free (with charges to come later for usage), there might be nominal value declared. This is generally acceptable but must align with transfer pricing norms if the supplier is related.

- **NOC Documentation:**

While customs regulations don’t mandate a license, in practice customs officers might flag unusual imports like thousands of active SIM cards. They could ask for an NOC or authorization from DoT to ensure the importer is permitted to handle telecom SIMs. In scenarios in recent years, importers of telecom equipment (e.g., mobile base stations) needed WPC (Wireless Planning & Coordination) or other clearances. For SIM cards, there is no WPC requirement since SIMs are passive devices (they do not emit radiofrequency themselves; the device modem does that). Nonetheless, because SIMs enable telecom access, customs may internally have instructions to verify DoT permissions if the quantity is large. The evolving framework (discussed above) is likely to formalize that process. **Post-framework, an importer of foreign SIMs/eSIMs for IoT would show their license or NOC at customs as evidence** that the import is legitimate. This ensures coordination between DoT and Customs – preventing unauthorized entities from importing SIMs in bulk.

- **Technical aspects:**

Each SIM card typically contains encryption technology (for authentication to networks). India’s import policy in the past had restrictions on certain encryption products, but ***commercial SIMs are standard telecom equipment and not subject to separate encryption import licenses***. They fall under the broad exemption for mass-market crypto products. Additionally, eSIMs (embedded SIM chips) might be imported as solderable MFF2 form-factor chips. These would likewise be classified under electronic components (possibly under HS subheadings for integrated circuits if not under 8523). If an IoT manufacturer instead uses “remote provisioning” (i.e., the eSIM profile is downloaded over-the-air in India), then physically nothing crosses the border – but in that case, the **import is of a service (telecom profile provisioning)** which circles back to FEMA/RBI handling rather than customs.

- **Import for Re-export:**

Since the SIMs are being imported solely to be integrated into products that will be **exported**, companies can avail certain duty exemptions. Under customs rules, if you import inputs for use in manufacturing exports, you may not need to pay IGST upfront (for example, via an Advance Authorization or under bond if working in an SEZ or bonded warehouse). Given basic duty is zero, the main saving is IGST. Companies might evaluate schemes like duty drawback or GST refunds on exports to recover any tax paid on SIM imports. Customs will be concerned that **proper records are kept to show**

those SIMs indeed got exported inside products, to prevent any misuse (e.g., an importer claiming duty-free import for export but then diverting SIMs for local use, which would be illegal). This ties into inventory control and audit by customs (for instance, if operating under a bonded manufacturing warehouse, every SIM in must be accounted as product out).

- **HS Codes and Documentation:**

  It's worth explicitly noting the HS code in import documents to avoid misclassification. HS 85235210 clearly covers SIM cards. There are other related codes (for example, one might wonder if a SIM is ever classified under "8542.1010 – Smart Cards" or similar; historically, SIMs have been under 8523). Using the correct HS ensures the correct duty (0% basic) is applied. On the customs entry, the description should state "SIM cards (programmable smart cards for telecom) – for M2M devices – not for retail". Providing such detail can preempt questions. Invoices from the foreign provider should ideally mention the ICCID/identifiers of the SIMs or at least the quantity, which also helps link them to export products later.

In conclusion, **customs law does not ban or specially restrict SIM/eSIM imports**, but **customs enforcement will intersect with telecom regulations**. Importers should be prepared to furnish any telecom department clearance and maintain an audit trail that these SIMs are used as intended (in export devices, not activated for local use). Under the upcoming policy, importing these SIMs with a new service authorization from DoT will likely be straightforward – customs will treat it as a normal import of components, with the onus on the license holder to follow conditions (like ensuring no unauthorized local sale/use). The **harmonized code 8523.5210** and associated import conditions (basic duty free, IGST 18%) confirm that bringing in SIM cards is legally allowed in India. Any import-export practitioner would advise to also check if **any other ministries' clearances are needed** – for example, sometimes electronics require BIS (Bureau of Indian Standards) certification. In this case, SIM cards are not listed under mandatory BIS electronic items (those tend to be things like adapters, phones, etc.), so no BIS certification is required for SIMs.

Unified Licensing and New Authorizations (Telecom Services)

Aside from the physical import and data considerations, a core question is: **Does an Indian company need a telecom license to integrate and effectively "provide" connectivity via foreign SIMs?** The answer is trending towards **"Yes, a form of authorization is required**, albeit a lighter one than a full-fledged telecom operator license. Under the previous Indian Telegraph Act regime, selling foreign SIM cards in India was not a licensed service category, hence the ad-hoc NOC arrangement. Now, under the **Telecommunications Act, 2023**, the government has power to create new categories of **license, registration, or permission** for any telecom-related service. TRAI has explicitly noted that **international SIM card services of foreign operators should be covered under a new service authorization** in the Unified License framework.

This prospective authorization can be seen as analogous to a **"Virtual Network Operator (VNO) for International Connectivity"**. It would not grant spectrum or the right to operate a network, but would permit the entity to **legally market, sell, and support foreign mobile services within India for specific purposes**. Obligations likely to be attached to such authorization include:

- **Compliance with security/Lawful Intercept requirements:**

  The authorized entity may be required to maintain records of all SIMs/eSIMs sold, the persons or products to which they were provisioned, and share data with law enforcement upon request. They might also facilitate interception by coordinating with the foreign provider if needed during the SIM's brief usage in India. (For example, if an imported SIM is suspected to be misused while in India, the Indian authorities would reach out through the authorized entity to the foreign operator).

- **Subscriber Verification/KYC:**

  Even though these SIMs are for devices, KYC in a broad sense may still apply. The DoT might mandate that the **Indian manufacturer (or SIM provider) obtain an undertaking that the SIM-equipped device will be used only outside India** and maintain a record of the foreign buyer or destination. Essentially, instead of end-user KYC like with travelers, it could be **"KYC of the supply chain" – knowing which company or client the SIM is going to**. This ensures traceability if a problem arises.

- **Roaming and Functional Restrictions:**

  The authorization would formalize that these SIMs **cannot be offered for Indian domestic use**. They should only latch onto Indian networks under normal international roaming agreements and ideally only for testing. There might even be technical measures encouraged, such as the SIM profiles being set to not work beyond a certain period in India or not allow local calling within India.

- **Unified License (UL) implications:**

  If an IoT device maker does **not** obtain this new authorization themselves, they might partner with an existing authorized entity. As of Dec 2024, 29 entities held DoT NOCs for international SIM/card rental services (these are companies that traditionally provide SIMs to tourists/business travelers). Those companies could conceivably extend their NOC scope to cover M2M devices, or new players (maybe the device makers or global IoT connectivity firms) will enter. Under UL rules in the new regime, these service authorizations will be part of the **unified licensing system** – meaning the holder must be an Indian company, pay a license fee (likely a nominal one, possibly a percentage of revenue or fixed fee), and follow general license terms (like not infringing on the domain of licensed telcos within India). TRAI indicated the approach should be "light touch" with minimal entry barriers, so the aim is not to over-regulate, but to provide legal clarity.

- **International Roaming Service Provider License:**

  It's worth noting that selling foreign SIMs to Indian outbound travelers is already an established NOC category, and TRAI has recommended turning that into a formal **license authorization valid for 10 years**. This could be termed an **"International Global Calling Card/ SIM Provider"** license under the new Act. The IoT export use-case might fall under the same authorization or get a slightly different one. The consultation specifically asks if a *separate* category is needed for "foreign SIMs in export-only devices" or if it can be subsumed into the international SIM provider authorization. There may be differences in conditions (e.g., KYC for individual vs. device use), but likely a single broad authorization will cover both, with specific provisions for IoT/M2M.

- **Unified License (Telecom and Broadcasting):**

The query also mentions broadcasting. Under India's telecom framework, broadcasting services (like DTH or teleport services) currently require separate licenses from Ministry of I&B and WPC, but the new Telecom Act hints at a converged approach. If, for instance, a broadcasting company wanted to use embedded SIMs in broadcast equipment (say a news camera that livestreams via 4G using a foreign SIM when reporting abroad), they too would come under these rules. The **Telecommunications Act, 2023** explicitly covers all telecommunication services, which includes broadcasting carriage (though content is regulated separately). So a broadcaster integrating connectivity in its hardware would either use licensed Indian SIMs or if attempting to use foreign SIMs, would need this same authorization. In short, **any industry (telecom, broadcasting, automotive, healthcare etc.) using foreign SIM connectivity as part of its offering will have to ensure an authorized route** – either obtaining the license or sourcing SIMs through an authorized provider.

Finally, one should note that the **government's stance is driven by national interest considerations**. They want to encourage manufacturing and export of IoT devices from India (as highlighted by the National Digital Communications Policy 2018 and the DoT's 2015 M2M Roadmap), but without undermining Indian telecom regulations. By setting up a clear licensing mechanism, India can facilitate IoT exporters (making it easier to get foreign connectivity in devices) while still **retaining oversight and ensuring no revenue leakage or security lapse**. For example, DoT wouldn't want a scenario where foreign M2M SIMs are freely available and start getting used in domestic IoT deployments (which could hurt local operators and evade lawful interception). The new authorization and NOC conditions will be calibrated to prevent that, by binding the use to export purposes only. We can expect obligations for periodic reporting to DoT of how many SIMs were imported, used, exported, etc., under the principle of accountability.

International Compliance and Treaties

When dealing with cross-border telecom services and data, **international regulations and agreements** also come into play. Indian companies must be mindful of the following:

- **Roaming and IMSI Allocation (ITU Regulations):** The **International Telecommunication Union (ITU)** allocates country codes and network codes used in SIMs (the IMSI numbers). Foreign SIMs used in devices will typically have an IMSI of the foreign operator's country or a special *"global IMSI"* (ITU has a 901 MCC for global services). India as a country has an interest in ensuring these numbering resources are used appropriately. The TRAI in past recommendations acknowledged ITU's global SIM concept and even suggested that **India should recognize ITU-assigned global M2M SIM codes (MCC 901)** for use in devices. So if a foreign SIM belongs to a global M2M service (like those operated by international IoT MVNOs), the Indian regulators would treat it as foreign and ensure it's authorized via the discussed mechanism. From an ITU perspective, using a foreign or global IMSI in India is not a violation per se (roaming is part of international telecom agreements), but permanent usage would usually require either a local license or an agreement. Many countries have **bilateral or multilateral agreements on telecom services**, primarily through the framework of the WTO (India is signatory to the GATS telecom reference, meaning it allows certain value-added service imports) and regional forums. There's also the **International Roaming Agreements** between operators – though those are commercial, regulators often facilitate them. Indian operators have roaming agreements with foreign operators, which is how a foreign SIM gets service in India. These operate under the principle of reciprocity and adherence to visited network's lawful intercept laws (the visited network – e.g. Jio or Airtel – can intercept even foreign roamers if legally required, and then share info via the foreign operator). The presence of a foreign SIM in India therefore engages **global cooperation for security** – for example, if an issue arises, Indian law enforcement might use Mutual Legal Assistance Treaties (MLATs) or direct liaison with the foreign operator's country to obtain subscriber details or data. This is one reason DoT insisted on monthly reporting by NOC holders of every SIM sold and to whom, to ensure traceability.

- **Data Protection (GDPR and others):**

  We touched on GDPR under MeitY's section, but broadly, when exporting devices internationally, companies must navigate various data privacy laws:

  - **GDPR (EU):** If the IoT device will process personal data of individuals in the EU, GDPR compliance is mandatory. Non-compliance can lead to hefty fines, which could indirectly become an issue for Indian exporters if something goes wrong. Exporters should implement **data minimization, encryption of personal data in transit and at rest, and mechanisms for users to exercise their rights**. For instance, an automotive IoT unit sending telemetry to India might need the user's consent and perhaps an EU-to-India data transfer mechanism like Standard Contractual Clauses.
  - **Other jurisdictions:** Different countries have their own laws – e.g., California's CCPA/CPRA for user data, Singapore's PDPA, etc. While these typically bind the entity operating in those jurisdictions or handling those citizens' data, an Indian manufacturer providing a connected service might indirectly become responsible. Partnering with the foreign network provider can help – often the connectivity provider (e.g., a European telco) will ensure compliance for the network data. But any application data the device sends to the Indian company's cloud would be the company's responsibility under privacy laws.
- **Export Control Regulations:**

In some cases, there could be **technology export controls** to consider. For example, the EU has strict rules like GDPR which we discussed, but also consider if India had any export control on cryptographic technology in IoT devices (currently India's export control list (SCOMET) doesn't list simple encryption in consumer IoT). The U.S. has regulations (EAR) that might restrict export of devices to sanctioned countries if they contain certain advanced telecom tech. If an Indian device with foreign SIM was re-exported to a third country under sanction, it could raise issues via the foreign operator or globally. These are edge cases but worth noting.

- **Bilateral Treaties and Agreements:**

India has mutual agreements with many countries for cooperation in telecom and cybersecurity. For instance, **Interpol or country-to-country MLATs** allow sharing of information for criminal investigations. If a device with a foreign SIM is involved in an incident, Indian and foreign agencies will cooperate under those frameworks. Also, India and the EU have dialogues on data protection (for a potential adequacy decision in future). Ensuring that IoT exports uphold data security can bolster India's reputation in such negotiations. On the telecom front, there are international forums (like the **ITU and APT** – Asia-Pacific Telecommunity) where India participates to shape IoT/M2M standards and regulations. TRAI's efforts to create a formal license for foreign SIM use in exports may actually set a precedent globally and align with how other countries are tackling **permanent roaming restrictions**. As mentioned earlier, many large economies **prohibit or limit permanent inbound M2M**

roaming (China, Brazil, etc. ban it; others like EU allow it but monitor). India's developing framework is in line with this global regulatory trend: encourage localization of connectivity (to local SIMs) but allow flexibility for manufacturing and testing.

- **Lawful Interception and Security Treaties:**

  Telecom data intercept is usually governed by national laws, but when a foreign SIM is in India, the ability to intercept communications (for security surveillance) depends on international cooperation. Typically, the Indian visited network can intercept the call/data (since it travels over its airwaves), but to decipher subscriber identity or content fully, they might coordinate with the home network. India is not part of the "Five Eyes" intelligence alliance, but it does have bilateral intelligence-sharing arrangements. One could imagine scenarios where, say, an IoT device with a foreign SIM is temporarily active in India and used in a crime – Indian agencies would have to work with the foreign telecom operator (via the authorized Indian entity and the foreign regulator) to get information. The regulatory framework will aim to minimize such friction by requiring a local point of contact (the license holder) who can quickly liaise with foreign providers.

In summary, internationally, **compliance is twofold**: comply with foreign laws when exporting (data privacy, device standards, etc.) and ensure India's own security is not compromised by the use of foreign connectivity. Fortunately, the use-case here is **export-oriented**, so once the device leaves India, it falls under the importing country's jurisdiction for telecom use. The Indian manufacturer's responsibility beyond that is mainly to ensure the device meets those destination regulations (proper certifications like CE/FCC marks for the radio, etc., which are standard steps in product export).

To illustrate, consider an Indian company exporting smart meters to Europe with an eSIM from a European carrier pre-loaded. The company must ensure the device's cellular module is certified for use in Europe (CE certification), the eSIM profile meets EU telecom regulations, and GDPR compliance is addressed for any consumer data. Meanwhile, before export, the company must comply with Indian rules to legally import that eSIM and test it. This interplay requires careful compliance management but is certainly navigable with the frameworks being put in place.

Sector-Specific Implications and Other Industries

Telecom Sector:

For India's telecom operators, the import of foreign SIMs for IoT could be seen as both a challenge and an opportunity. Domestic mobile operators might worry about losing out on connectivity for devices that end up overseas. However, since these devices aren't meant to use Indian networks except possibly in testing, the impact on local telecom business is minimal. In fact, Indian telcos may benefit by providing roaming services during the testing phase and could also partner with global IoT connectivity firms to offer their own "global SIMs." (Notably, **Tata Communications** – part of an Indian conglomerate – is already an ITU-allotted global SIM provider, showing Indian companies are venturing into that space). The new regulations will ensure a **level playing field** – foreign SIMs can be integrated only under oversight, so Indian telcos' interests (security, revenue accountability) are protected. Telecom companies that have M2M divisions will also need to adapt: for example, if Airtel wants to embed its SIM in devices for global use, it might seek a license extension or partner with foreign carriers. The Telecom and broadcasting sectors, being heavily regulated, are used to such licensing regimes – so incorporating foreign SIM usage via a license is in line with how these sectors operate (much like DTH requires licenses, ILD voice requires licenses, etc., now global IoT connectivity will require a form of license).

Broadcasting Sector:

Although not immediately obvious, broadcasting equipment is increasingly connected (for instance, news cameras streaming via 5G, satellite news gathering kits with SIM backup, etc.). If any broadcasting entity in India plans to export equipment that includes SIMs (say a satellite radio device with a SIM for backup connectivity in remote areas), they would face the same import/licensing issues. Additionally, broadcasters deal with content regulations which won't directly be affected by SIM import, but if their equipment transmits data abroad, they must ensure no conflict with content laws (e.g., if a device streams Indian content abroad via a foreign SIM, it's mostly fine, but if it were the reverse – foreign content into India bypassing controls – that would be an issue). In general, the **implications for broadcasting** are not unique beyond the connectivity aspect; they simply must comply as any tech company would with SIM import rules.

Automotive and Other Industries:

Automotive, healthcare, energy, consumer electronics – these are sectors likely to embed connectivity in products. Many automakers, for instance, include eSIMs in cars for telematics and infotainment. If those cars are made in India and shipped globally, the manufacturer may prefer to install a SIM that works in the destination (or a global roaming SIM). The regulatory framework we discussed will equally apply to them. Such companies might not traditionally think of themselves as "telecom providers," so they will need to either acquire the proper authorization or source their connectivity through an authorized provider. This adds a **compliance layer to industries** that are otherwise not telecom-focused. For example, a car company might team up with a global IoT SIM provider who has the Indian NOC/license, rather than itself dealing with DoT. Likewise, a medical device manufacturer exporting connected health monitors to, say, the US might embed a foreign SIM – they too must ensure the import and integration is approved. The **IoT use-cases span sectors like utilities (smart meters), agriculture (sensor devices), security (CCTV with 4G backhaul)**, and all of them will benefit from a clear policy that such foreign SIM integration is allowed with conditions. It prevents uncertainty – companies won't fear their shipment being held or their factory testing being illegal. Instead, they'll have a straightforward way to comply.

Cross-Industry Data Concerns:

Another implication across industries is data sovereignty. For instance, if a smart healthcare device is sending patient data from India to a foreign server via a foreign SIM (perhaps during testing or if used by an international patient in India), it could raise compliance issues under health data protection laws (like HIPAA in the US or upcoming Indian health data rules). Companies in sensitive sectors must doubly ensure encryption and consent for any such data transfer. But if devices are only activated abroad for end-use, then each industry will handle data under the destination country's laws (with the manufacturer possibly having contractual obligations to protect that data).

Conclusion:

In conclusion, importing foreign SIM/eSIM cards for integration into IoT/M2M devices intended for export is **permissible in India**, but subject to a tapestry of regulatory requirements. Indian authorities – DoT in particular – are carving out a regulated pathway to facilitate this practice. Companies engaging in it must navigate telecom licensing (NOC or new authorisation), comply with import duties and procedures (HS 85235210, IGST etc.), follow foreign exchange rules for paying the service provider, and address data security both for Indian testing and international deployment. The **Telecommunications Act, 2023** and TRAI's ongoing consultation are poised to provide formal clarity and ease of doing business in this realm, aligning India's policy with global norms while safeguarding national interests. By obtaining the necessary authorisations and implementing strong compliance measures (KYC, security, reporting), manufacturers in any sector can leverage foreign SIM technology to make their exported IoT products seamlessly connected, all without running afoul of Indian laws. The coordinated oversight by bodies like DoT, MeitY, RBI, and Customs ensures that **the integration of global connectivity into "Make in India" devices is done in a responsible, legally sound manner** – fostering innovation and exports on one hand, and protecting Indian networks, revenue, and data sovereignty on the other.

Q5. Whether there are any regulatory issues including those related to the agencies such as RBI, customs etc. in respect of the export of Indian telecom service providers' M2M SIMs/ eSIMs for the use in M2M/ IoT devices meant for import purposes? Please provide a detailed response with justifications.

Comments :

Regulatory Considerations for Exporting M2M SIMs/eSIMs from India

DoT Licensing and M2M Compliance Requirements

Indian telecom service providers (TSPs) must comply with Department of Telecommunications (DoT) licensing norms when exporting M2M SIMs or eSIMs for IoT devices. Under the Unified License (UL) framework, providing M2M connectivity is permitted **either via a dedicated M2M service authorization or under existing access service licenses**. In 2022, DoT introduced an *M2M Service* category in the UL regime, allowing licensees to obtain an M2M authorization (Categories A/B/C for national, telecom circle, or district level, respectively) to offer M2M connectivity services. Notably, a fully licensed TSP can provide M2M services directly **without needing separate M2M service provider registration**, whereas third-party IoT platform providers (M2M Service Providers or M2MSPs) must register with DoT. Any entity seeking a UL or UL (M2M) must be an Indian-incorporated company, ensuring Indian jurisdiction over the service.

KYC and Numbering:

M2M SIMs in India follow special Know-Your-Customer and numbering rules to maintain security and traceability. Since October 2018, new M2M mobile connections use a **13-digit numbering scheme** (as opposed to standard 10-digit phone numbers) as mandated by DoT. DoT's May 2018 guidelines also allowed issuing bulk M2M SIMs to enterprise users (like device OEMs) under *revised KYC norms*. For example, **device manufacturers can be the initial subscriber for pre-embedded SIMs** in their products, subject to strict verification. The manufacturer/OEM must complete subscriber verification before embedding the SIM in the device, and **when the device is sold or transferred to an end-user, that end-user's credentials must be updated with the TSP** to maintain proper KYC records. This enables a controlled transfer of SIM ownership while complying with subscriber verification rules. DoT's M2M SIM instructions also historically imposed "**restrictive features**" to prevent misuse – for instance, earlier M2M SIM profiles could only communicate with a limited set of fixed numbers or services (to curb unauthorized voice use), though these restrictions have been liberalized over time. In practice, M2M SIMs are generally intended for data and telemetry; any voice/SMS capabilities are often constrained per DoT's directions to ensure they are used strictly for machine communications.

License Conditions:

The UL requires TSPs to adhere to all standard telecom regulations even when SIMs are exported for integration into devices. Notably, **service area limitations and security conditions continue to apply**. The SIMs in question will ultimately operate on Indian telecom networks (with Indian IMSIs), so the TSP remains accountable under its license for those connections. If the devices activate abroad (even temporarily), they do so via international roaming agreements, which is allowed under the UL framework as incidental service. However, the operator must ensure compliance with any **applicable UL clauses on international usage and data handling**. For example, **Clause 39.23(viii) of the Unified License bars licensees from transferring any subscriber-related information outside India**, except for limited cases like international roaming billing or foreign users roaming on Indian networks. This means that subscriber data and authentication details for these SIMs should remain stored in India, and only the minimal data necessary (e.g. roaming billing records or network queries) should cross borders during the period the SIM is outside. The TSP's obligations for **lawful interception, call data recording, and subscriber record-keeping** continue uninterrupted by the physical export/import of the SIM; the SIMs must be provisioned and used in a manner that allows the operator to meet these compliance duties once the device is active on the Indian network. In summary, from a licensing perspective the TSP must ensure that it has the proper authorization (UL with access/M2M service), follows M2M SIM issuance guidelines (13-digit numbers, KYC, usage restrictions), and does not breach any license conditions by virtue of the SIMs briefly leaving the country.

Cross-Border Data Flow, Cybersecurity, and Data Localization

When M2M SIMs or eSIMs are sent abroad and later activated in India, regulators are attentive to how data (both user data and network/authentication data) is handled across borders. **Indian telecom regulations impose strict data localization requirements for subscriber information.** As noted, the UL prohibits transferring any subscriber account information or user data outside India, except for the limited purpose of supporting international roaming services. In practical terms, this means Indian operators must ensure that sensitive data (e.g. SIM authentication keys, customer identities, usage records) remain within Indian-controlled systems. If the IoT devices perform any data communication while abroad (for testing or bootstrapping), the TSP should ideally route those communications through its Indian network or roaming partners such that any customer data resides on servers in India. This also implies that **remote provisioning or profile activation for eSIMs should be done securely and in line with Indian security mandates**.

From a broader policy angle, **India's data protection and cybersecurity framework also affects IoT/M2M deployments.** The Ministry of Electronics and IT (MeitY) has enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), which introduces conditions on cross-border personal data flows and possible localization for certain data categories. If the IoT devices collect or transmit *personal data* (for example, vehicle location tied to individuals, health telemetry, etc.), the data fiduciaries must ensure compliance with the DPDP Act. This may involve only transferring personal data to countries approved by the government, meeting consent and security requirements, and potentially storing certain sensitive data within India. In essence, any user-related data gathered via these SIM-enabled devices could be subject to **data export restrictions or encryption norms under MeitY's frameworks** (e.g. requiring equivalent protection standards abroad or government whitelisting for foreign storage). Companies should conduct data mapping to confirm whether IoT data is personal or critical and implement controls accordingly (such as anonymization or local data centers) to satisfy these emerging legal requirements.

Cybersecurity Requirements:

Both DoT and MeitY emphasize strong security in the M2M/IoT ecosystem. The DoT's licensing conditions already mandate protection of network and subscriber data (including preventing unauthorized interception and ensuring encryption strength within allowed limits). For IoT specifically, **DoT's Telecom Engineering Centre (TEC)** has issued an IoT Security *Code of Practice* and guidelines (March 2023) to secure devices and networks end-to-end. These guidelines encourage measures like regular firmware updates, vulnerability disclosure policies, unique device passwords, and adherence to international security standards for IoT devices. When exporting Indian eSIMs to be soldered in devices abroad, the manufacturer and TSP should implement robust cyber hygiene – e.g. **ensuring the eSIM is provisioned over encrypted channels, and that no sensitive credentials are exposed during the supply chain**. DoT's 2018 permission for eSIM usage explicitly requires that **network operators meet lawful interception/monitoring requirements and prevent device manufacturers from tampering with the eSIM or its profiles**. This implies that the cryptographic elements of the SIM (IMSI, authentication keys, profile data) must remain secure and accessible only to authorized systems. Indeed, in June 2025, DoT further tightened eSIM infrastructure security by mandating that **Subscription Manager** servers for eSIM (the SM-SR/SM-DP systems enabling remote SIM provisioning) be located in India and certified under GSMA's Security Accreditation Scheme. Only licensed TSPs, their registered M2M service partners, or authorized Indian entities can operate these eSIM management servers, and they must integrate with each other per global (GSMA) standards for secure profile download/switching. In short, any cross-border data exchange for provisioning or managing these SIMs is tightly controlled: **the core SIM profile and subscriber data are managed on Indian soil, under Indian jurisdiction, with internationally accredited security standards**.

These measures collectively address government concerns that IoT devices (often deployed in critical infrastructure or handling large volumes of data) could become channels for data leaks or cyberattacks if not properly regulated. By enforcing data localization for telecom data, insisting on secure eSIM management, and rolling out IoT-specific security best practices, DoT and MeitY aim to mitigate risks associated with sending SIMs and data across borders. Exporters should therefore implement **strong encryption, secure handling of SIM credentials, and compliance with data protection rules** at every stage (manufacture, transit, and deployment) to satisfy these regulatory expectations.

Customs and Export-Import Regulations (DGFT and Customs)

Exporting SIM cards or eSIM modules from India and subsequently re-importing them inside devices engages various trade regulations. Fortunately, **SIM cards are not a restricted commodity for export** – they are classified under HS Code 8542 or 8523 (as “electronic integrated circuits” or “smart cards”) and are generally freely exportable under India’s trade policy. The Directorate General of Foreign Trade (DGFT) does not list SIM cards or standard cryptographic smart-cards on the restricted or prohibited export lists, meaning Indian TSPs can ship out M2M SIMs with a simple export declaration. Companies will need a valid Importer-Exporter Code (IEC) registration (a mandatory license for any importer/exporter) and must follow standard customs procedures for export of the SIM hardware. It's advisable to accurately state the description (e.g. "Telecom SIM cards for M2M use, programmable, unloaded or inactive") and value of the SIMs on export documentation, even if they are low-value items, to ensure transparency and compliance with customs valuation norms.

When the IoT devices with embedded SIMs are **imported back into India**, the customs treatment will depend on how the shipment is structured. If the devices are being imported as finished goods for sale, the presence of an embedded SIM typically does not invoke any special prohibition – it will be seen as a component of the device. The importer will declare the overall device (for example, a "GPS tracker" or other IoT gadget under its appropriate HS code) and pay any applicable customs duty on the full product value, which inherently includes the SIM's value. There is **no specific import duty on SIMs separately** if they come integrated, beyond the duty on the host device. (Standalone SIM cards imported would likewise fall under a "smart card" category, which in practice often has low or zero duty due to ITA exemptions, but in our scenario they are part of a larger product.) Indian Customs may, however, scrutinize the devices to ensure they comply with other import requirements: for instance, if the device is a communication equipment, it might require Wireless Planning & Coordination (WPC) Wing approval or compliance with mandatory certification (like the Telegraph Act Equipment Type Approval or the Electronics Standard BIS registration) – those are obligations on the device hardware, not on the SIM itself. The SIM being present should not alter the device's classification, but the **importer should ensure to mention the**

inclusion of "subscriber identification module" in the documentation, as a matter of completeness and to preclude any confusion during inspection (since an active SIM could theoretically raise questions if the device is capable of transmitting on arrival). Generally, customs does not treat an inactive pre-installed SIM as a security concern, but it is wise to keep the SIMs **inactive (not generating network traffic) until after customs clearance** to avoid any appearance that a device was operating on a network before regulatory approvals.

One key consideration is **India's re-import rules and duty implications** if the SIMs were exported only for assembly and then brought back. India allows goods that were exported for processing or integration into final products to be re-imported with duty relief in certain cases (for example, under customs provisions for outward processing or if covered by specific notification). If the export and re-import are part of the same business transaction (e.g., the Indian TSP sends SIMs to an overseas OEM and then that OEM ships the final devices to India), the companies might explore claiming benefit under duty drawback or exemption for the Indian-origin component. However, given the relatively low value of SIM cards and the fact that the final IoT devices will be subject to whatever duty is applicable, this may not be economically significant – any duties paid on the small SIM component would be minimal. **In practice, most such IoT devices (especially if related to smart infrastructure or automotive) might even be exempt or attract low duty under various schemes**, but this is case-specific to the product category. The main point is that **there is no outright customs bar on importing devices with embedded Indian SIMs**. The customs authorities care primarily about correct classification, valuation, and compliance with any standards (e.g. safety/WPC) for the device. As long as those are in order, the presence of an Indian SIM (even one that will be activated on an Indian network) is not a reason for refusal or additional duty.

In summary, from a DGFT/customs perspective, **M2M SIMs are treated as regular electronic goods – freely exportable and importable**. Exporters should ensure proper documentation and obtain an IEC. Importers of the finished devices should declare the devices accurately and adhere to any relevant import standards. There are no special export permits or customs duties targeted at SIM cards or eSIM profiles themselves. (Notably, the cryptographic capabilities of SIMs – used for authentication – are considered part of standard telecom equipment and are not subject to separate export control licensing, since they fall under mass-market telecom encryption which is exempt from special SCOMET authorization in most cases.) Thus, so long as general customs rules are followed, the regulatory burden on moving these SIMs across borders as part of IoT devices is relatively straightforward.

Financial and Foreign Exchange Regulations (RBI/FEMA)

The export of SIM cards and subsequent re-import of IoT devices also brushes against financial regulations, though mainly in the ordinary course of cross-border trade. The Reserve Bank of India (RBI), through FEMA (Foreign Exchange Management Act) rules, regulates how payments for exports and imports are handled. In this scenario, an Indian TSP might "sell" the SIM cards (or provide them) to a foreign device manufacturer or to its own overseas subsidiary for integration. **Any export of goods from India must be realized in an approved foreign currency payment within the**

stipulated timeframe (usually within 9 months) under FEMA's export of goods rules. Therefore, if the SIMs are provided for a fee, the Indian exporter (telecom operator) should invoice the foreign buyer and ensure the foreign exchange is remitted back via normal banking channels. Often, though, SIMs could be supplied as part of a broader commercial arrangement (for instance, the operator might not charge separately for the SIM hardware, instead bundling it with future service revenue or providing it as a free component to encourage the use of its network). If provided at zero cost, it would be wise to still have documentation (perhaps a nominal value or a consignment note) for customs; FEMA compliance in that case would mean there's no payment to realize, but the transaction should be reported as required.

Crucially, **there are no special RBI licenses or approvals needed to export telecom equipment like SIMs**, beyond the standard export/import framework. M2M connectivity itself, once the devices are imported and activated, will generate revenue in INR from Indian end-users or enterprises. Those telecom service revenues are domestic transactions (subject to normal license fee and GST, but not a FEMA issue). One aspect to consider is if the IoT device manufacturer (if foreign) will pay the Indian TSP for connectivity or services while the devices are outside India. If, for example, the Indian operator provides testing connectivity or roaming service abroad during the manufacturing stage, any charges for that could be considered an *export of services*. Indian operators are allowed to provide international roaming services and to receive payments from foreign carriers or intermediaries for such usage – this is part of current account transactions permitted by RBI. The funds flow typically works via roaming agreements (the foreign network bills the Indian operator for use, and the Indian operator ultimately recovers costs through its subscriber or a B2B contract). **From a FEMA perspective, these are routine telecom settlement transactions, not requiring separate permission.** The operator should ensure that any foreign currency payments it must make (e.g. to a foreign roaming partner for testing done abroad) are done under an appropriate purpose code (likely "telecom services payment") and that any foreign currency earned (if the foreign OEM pays for the SIMs or a provisioning fee) is repatriated.

Also, if the Indian TSP is *investing* in an overseas venture for this purpose (say, setting up an international distribution arm or entering a joint venture to embed its SIMs in products), then ODI (Overseas Direct Investment) regulations and capital outflow rules would apply – but that scenario goes beyond a simple export of SIMs. Assuming it's a straightforward trade arrangement, **the financial regulations boil down to: use normal banking channels, adhere to export payment realization timelines, and comply with invoicing and customs valuation norms**. The RBI does monitor exports via the EDPMS (Export Data Processing and Monitoring System) to ensure payments come in; as long as the telco properly accounts for the SIM shipments (even if free of cost, a fair notional value should be declared) and any ensuing receipts, there should be no issue. There is no specific foreign exchange restriction on *sending electronic SIM profiles or activation data across borders* – these are considered part of service provisioning. However, the operator should be mindful of data storage rules (as discussed above) which indirectly have a bearing on foreign IT expenses: e.g., paying a foreign platform to manage eSIM provisioning might be disallowed if it means subscriber data leaves India. In light of that, DoT's requirement to keep eSIM management in-country also aligns with FEMA compliance, since it avoids any complication of paying for foreign data hosting of subscriber info.

In summary, **no unique RBI or FEMA approvals are required for this use-case beyond standard export/import finance rules**. The key steps are to ensure an IEC is in place, transactions are correctly documented, and foreign exchange, if any, is handled per FEMA norms. The telecom operator should also consider informing its lead bank about the nature of the transaction, especially if the export is of significant value, so that any compliance queries can be addressed. By following general good practice in trade finance (timely payment reconciliation, accurate declarations), the financial regulatory aspect should remain routine.

International Roaming and Remote eSIM Activation Considerations

A distinctive regulatory aspect of this scenario is that the SIMs might be **activated or have to function while the devices are still abroad** (prior to being imported into India). For physical SIM cards, the TSP could choose not to activate them until the devices reach India (they could be shipped inactive and only commissioned on the network upon or after import). In many cases this is preferable to avoid complexities. However, for **testing or device initialization**, sometimes the embedded SIM needs to latch onto a network temporarily outside India. If an Indian M2M SIM connects to a foreign network (e.g., to transmit a test signal or download an update in the factory), it will do so under international roaming. **Indian telecom licenses do allow subscribers to roam internationally** under agreements with foreign operators, and the current rules don't forbid an M2M SIM from doing so. This would be treated similarly to any Indian mobile customer traveling abroad and using their SIM – i.e. permissible. That said, regulators generally expect that *permanent* deployment of Indian SIMs outside India is not done to circumvent local regulations. In our case, since the devices are *coming back to India*, the roaming is by nature temporary. TSPs should ensure that such roaming usage is in line with any bilateral roaming agreements and that the SIMs are provisioned with roaming-enabled profiles if needed. It's worth noting that some foreign jurisdictions have limits on long-term roaming by foreign SIMs (to protect their own operators), but a brief usage during manufacturing or logistics is unlikely to raise concern.

For **remote provisioning of eSIMs**, the situation is slightly different. An eSIM (eUICC) embedded in the device can be shipped with no profile or with a bootstrap profile. Indian authorities have now outlined clear rules for how M2M eSIM profiles are to be managed. As of mid-2025, **any remote provisioning of an Indian network profile onto an eSIM must involve Indian-controlled infrastructure**. Only licensed Indian operators or registered M2M service providers can run the SM-DP (Subscription Manager – Data Preparation) or SM-SR (Subscription Manager – Secure Routing) functions that download and manage eSIM profiles. If a device is abroad and needs to download an Indian operator's profile, that profile will be generated and issued by the operator's (or its partner's) SM-DP in India. The communication to the device might occur over the internet (e.g. via Wi-Fi or a foreign carrier's data connection), which is acceptable so long as it adheres to the GSMA security standards. The **regulatory concern here is to prevent any unauthorized or untracked provisioning**. DoT's new instructions even state that an entity controlling eSIMs (like an OEM with its own SM-SR) must integrate with any Indian TSP's provisioning server on request and facilitate profile switching within specified timeframes. This ensures that if, say, a car manufacturer embedded an eSIM and later decides to switch the connectivity to a different Indian operator, the process is supported and cannot be blocked – promoting flexibility but also oversight of profile swaps.

For the exporting TSP, if they want the eSIM to be **ready to use on arrival in India**, they might provision the profile in the device *over-the-air while it's still overseas*. This is allowed, but they must do it through the sanctioned channels (their GSMA-certified SM-DP/SR platform in India) and maintain logs of the transaction as required. The profile download itself will be encrypted and secure; however, some data (like the fact that a particular eSIM ID was provisioned with a certain IMSI) will necessarily traverse global networks. Regulators accept this as long as the control systems are in India and the data in transit is protected. It's also prudent to coordinate such provisioning with the device OEM to possibly perform it in a controlled environment (e.g., connect the device to a secure Wi-Fi at the factory to fetch the profile) to avoid any random roaming usage.

International roaming charges and rules will apply if the device actually connects to a foreign mobile network using the Indian SIM. The TSP should be aware that any usage abroad (even for testing) could incur roaming fees. Commercially, this might be handled via special IoT roaming plans or by whitelisting certain foreign networks for testing. There's no specific regulatory bar on incurring roaming for M2M devices, but from a business/regulatory prudence angle, operators typically would minimize it or explicitly account for it (to ensure, for instance, that such SIMs aren't later misused solely abroad). The **DoT and TRAI have also been examining the broader issue of "permanent roaming" SIMs** in IoT contexts. In fact, TRAI released a consultation in 2022-2023 about the use of *foreign* SIMs in devices meant for India and vice versa, to decide if new rules are needed to address those cases. The prevailing stance is that devices used in India should eventually have an Indian SIM (to allow Indian lawful intercept and emergency access), whereas devices exported out of India can use foreign SIM profiles. In our case, we are aligning with that philosophy: the devices destined for India indeed carry Indian SIMs. Thus, **the use case is actually pro-regulator in the sense of enhancing national oversight** (as opposed to a device coming in with a foreign SIM). Still, until guidelines are formally updated, operators doing large-scale eSIM provisioning to devices abroad might choose to keep DoT informed or seek an explicit no-objection, just as a matter of good practice. (DoT has a provision where *"innovative solutions"* in SIM usage can be referred for approval – while that usually meant foreign SIMs for export, an operator could analogously clarify their plan to export and re-import SIM-embedded gadgets to ensure regulators are comfortable.)

In summary, **international roaming and remote activation for these SIMs are permissible but regulated**. The Indian TSP must use proper roaming agreements and adhere to the new eSIM management rules. Any profile downloads or activations from outside India must go through Indian-controlled systems. There should be no violation of the device's intended use (the SIMs should ultimately be used in India, not to offer unintended service abroad). By following these principles, the operator stays within the bounds of both Indian regulations and international norms for SIM usage.

National Security and Surveillance Considerations :

National security is a thread running through all the above regulatory facets – the Indian government's policies on M2M SIMs are heavily influenced by lawful surveillance and security needs. **One major reason India insists on local SIMs for IoT devices is to ensure lawful interception and monitoring capabilities for those devices' communications.** An Indian-issued SIM (with an Indian MSISDN/IMSI) falls under the Indian lawful intercept regime, meaning that Indian law enforcement agencies (LEAs) can, with proper warrants, surveil the device's communications through the telecom operator's monitoring systems. If the same device used a foreign SIM in India, Indian authorities might not readily access the data, creating a security gap. This concern is evidenced by DoT's directive in January 2022 requiring that any sale of foreign operator SIMs in India get a special NOC, and indicating that unorthodox connectivity arrangements would be reviewed case-by-case. By **exporting Indian SIMs to embed in devices that will re-enter India**, the TSP and device maker are actually aligning with the security mandate that *devices in India use Indian connectivity*. This avoids the scenario of "permanently roaming foreign SIMs" on Indian soil, which DoT and TRAI have been actively trying to curtail for security reasons. In fact, applicants for M2M service provider registration must declare if they use any foreign SIM connectivity, underscoring the sensitivity of the issue.

However, the export-import use case still raises a few security points to manage:

- **KYC and Traceability:** It is vital that every SIM/eSIM can be traced to a responsible entity at all times. During the period the SIMs are outside India (before the devices are sold to end-users), they are typically under the custody of the device manufacturer or an integrator. DoT's

M2M guidelines, as noted, allow bulk issuance of SIMs to such entities, but hold the entity responsible for their use. The OEM should maintain an internal log of which SIM (by number/IMSI) went into which device, and ultimately which customer received that device. This information must be available to the TSP and law enforcement when needed. In addition, **if any SIM is lost or stolen in the supply chain, it should be reported and deactivated immediately** to prevent misuse (e.g., someone taking an active SIM and using it illicitly before the device arrives in India). The telecom license already has conditions requiring immediate reporting of lost SIMs or any suspicious usage, which would apply here as well.

- **Lawful Interception and Monitoring:** The TSP must ensure that its lawful interception systems are configured to handle these M2M SIMs. Notably, M2M SIMs might be configured to only connect through packet data (and maybe SMS) and to specific servers. Nonetheless, they fall under the same interception laws (Indian Telegraph Act and related DoT security directives) as normal SIMs. DoT has reminded operators that **services on eSIMs must fully support lawful interception** and that no feature of eSIM technology should prevent the operator from performing surveillance as required. For example, if a device is using an Indian SIM while roaming abroad and an Indian LEA needs to intercept it, the operator should have a means (in cooperation with the roaming partner) to capture those communications. Typically, with modern networks, data roaming traffic can be brought back to the home network or accessed via international gateways, so interception is possible. The new eSIM regulations also facilitate interception by ensuring the operator (and not the device OEM) controls the loading of profiles – this prevents an OEM from, say, secretly loading a foreign profile or altering the SIM such that Indian authorities lose visibility. It effectively closes the door on any “backdoor” profiles that could be used to bypass local networks.

- **National Security Directives:** India has in recent years issued directives to secure the telecom supply chain (for instance, the **National Security Directive on Telecom** which creates a list of trusted vendors for network equipment). While SIM cards have not been the focal point of such directives, operators should source their SIMs from reputable manufacturers with proven security. If the SIMs or eUICCs are sourced internationally, the operator might vet whether the manufacturer has had any known security issues. Thus far, there is no requirement that SIMs must be procured from a “trusted” list, but given SIMs carry encryption keys, using established vendors with GSMA certifications is a de facto expectation.
- **Remote Access and Data Centers:** DoT forbids remote access to telecom networks from outside India without permission. In the context of eSIM, if the manufacturer or any foreign entity were to have access into the operator’s SIM management platform, that would be sensitive. The operator should therefore ensure that any management of these SIM profiles from abroad (for instance, the OEM checking activation status) is done via secure channels and with DoT’s clearance if it involves network access. Generally, network elements (like HLR, SM-SR) should reside in India, which the operator will be complying with per the rules.
- **Surveillance and Traffic Routing:**

For M2M devices, sometimes companies use international roaming solutions that route data to foreign servers. We worry that critical data (say, from an Indian energy grid sensor) might be sent abroad directly via a foreign network, beyond Indian oversight. Using Indian SIMs mitigates this, since even if the device is abroad briefly, once in India its traffic goes through Indian mobile networks. Moreover, the operator can exercise controls like IP whitelisting, VPN tunnels, etc., to confine where the data goes. DoT's prior M2M instructions required that M2M SIMs have "restrictive features" – e.g., they could be restricted to communicate only with certain IP addresses or only through the packet core (no voice). The rationale was to limit their misuse as general communication tools. Although some restrictions were relaxed, the principle remains that these SIMs are for specific IoT data, which inherently reduces their attractiveness for misuse and makes any anomalous usage easier to spot by security agencies.

In conclusion, **the export and re-import of Indian M2M SIMs should be managed in a way that upholds India's national security objectives**. The arrangement actually supports security by ensuring IoT devices use Indian-network SIMs subject to Indian law. The involved parties must diligently follow KYC, maintain auditable trails of SIM custody, and adhere to the technical security requirements (like not disabling intercept capabilities and using only government-approved profile management systems). DoT has issued multiple circulars and guidelines (2018, 2019, 2025) addressing these points – from mandating 13-digit SIMs for traceability to obligating device makers to handle subscriber verification for embedded SIMs. By following these, the TSP and device manufacturer can confidently demonstrate that **no regulatory red lines are being crossed in the export-import process**. All relevant agencies – DoT, MeitY, DGFT, RBI, and national security apparatus – have their concerns addressed: the telecom license and M2M guidelines cover licensing/KYC; data localization and cyber laws cover data handling; customs and DGFT cover the physical movement; financial rules cover payment flows; roaming/eSIM rules cover the international activation; and security directives cover lawful intercept and surveillance readiness. Each of these aspects must be documented and justified (with references to the respective licenses, laws, or DoT circulars) in a compliance brief before undertaking the export of SIMs, to ensure a smooth and lawful operation.

Q.6 Whether there are any other issues related to the subject matter? Please provide a detailed response with justifications.

Comments :

A. Likely Regulatory Issues (Next 5 Years)

Category	Potential Regulatory Issues
1. National Security & Surveillance	- Unauthorized use of foreign SIMs/eSIMs within India- Risk of bypassing lawful interception protocols- Difficulty in enforcing surveillance or security norms on foreign telecom networks
2. Cross-border Data Flows & Jurisdiction	- Violation of Indian data localization norms (under DPDP Act or sector-specific rules)- Ambiguity about jurisdiction over data breaches, user privacy, or lawful access to M2M device data
3. Taxation & Customs Compliance	- Misuse of export route to avoid duties- Improper classification or declaration under HS codes-

Category	Potential Regulatory Issues
	Evasion of GST by proxy sales or unregistered vendors
4. SIM Misuse & Grey Market	- Activation of foreign SIMs in India illegally- Difficulty in tracking use in non-exported or diverted devices- Emergence of black-market trade of foreign eSIM profiles
5. Licensing Ambiguity	- Confusion over which entity is responsible (Importer/Device manufacturer/Foreign telco)- Disputes between DoT/TRAI/MHA/Customs/RBI on oversight
6. Lack of Traceability (KYC/GEO-FENCING)	- Non-compliance with Indian KYC standards- Absence of real-time traceability during testing/production- Problems during device recalls or firmware upgrades
7. Interference with Domestic Networks	- Unauthorized roaming or auto-connection to Indian networks- Potential security risk from unregulated device traffic
8. International Sanctions or Geopolitical Risk	- Dependency on SIMs from countries under sanctions- Need to quickly revoke licenses or authorisations if geopolitical relationships change
9. Accountability in Case of Cybercrime or IoT Failures	- Lack of clarity on responsibility in case an IoT device with foreign SIM is involved in cybercrime or industrial accident
10. Consumer Protection Abroad	- If Indian consumers use such devices abroad, unclear remedies or support- Misrepresentation or non-transparency about roaming cost/data privacy

---

B. Precautionary Measures / Regulatory Safeguards to Be Taken

1. Clear Licensing Regime

- Introduce a **dedicated Service Authorization category** under Section 3(1)(a) of the *Telecom Act, 2023* for **"Export-bound Foreign SIM/eSIM Handling"**
- Mandate registration of entities engaged in import/export of M2M/IoT devices with SIMs

2. Robust KYC & Activation Protocols

- Require Indian entities to perform **local KYC for testing-phase activations**
- Ensure **IMEI–SIM–Device linkage records** are maintained and audit-ready

3. Time-Bound Activation Windows

- Permit foreign SIMs to be **activated only during manufacturing/testing for up to 90 days**
- Ensure automatic **deactivation post-export**, with export-bill cross-verification

4. Customs and Export Oversight

- Enforce proper **HS code declaration**, labelling, and export tracking
- Link with **ICEGATE / DGFT systems** for device-SIM mapping

5. Network Access Safeguards

- Prohibit these SIMs from **permanently registering on Indian networks**
- Mandate **geo-fencing or IMSI-whitelisting** to detect violations

6. Data Privacy & Sovereignty Compliance

- Require foreign SIM/eSIM providers to **adhere to Indian DPDP Act** obligations if personal data is processed during testing
- Ensure cloud storage for logs is compliant with **cross-border data norms**

7. Accountability Clauses

- Agreements must include clauses on **liability in case of misuse, espionage, or device malfunction**
- Indian partner/importer should be the point of contact for **enforcement, consumer complaints, or cybersecurity audits**

8. Monitoring & Reporting Obligations

- Mandate quarterly or real-time reporting of:
  - Number of SIMs activated
  - Testing locations
  - Export destinations
  - Deactivation confirmations

9. Adherence to Global Norms

- Align with **ITU-T recommendations**, **ETSI standards**, and best practices from **FCC (USA)** or **EU GDPR/CE** for harmonized global acceptance

10. Cross-Regulator Coordination

- Formal MoU between **DoT, TRAI, MEITY, MHA, DGFT, Customs, RBI** for shared oversight
- Set up a **single-window dashboard** for compliance monitoring and SIM/device traceability

Forward-Looking Considerations

Area	Suggested Proactive Steps
AI/ML & IoT Integration	Build a framework for regulating **edge computing** and **autonomous M2M decisions** in exported IoT systems
Satellite Connectivity	Clarify policy on eSIMs that auto-switch between **terrestrial and satellite links**
India Stack Integration	Consider optional integration with **DigiLocker/e-KYC stack** for traceability
Dispute Redressal Mechanism	Establish dedicated cell within TRAI for disputes arising from **cross-border M2M export incidents**
National Trust Registry	Create an **IoT SIM/eSIM Export Registry** (public and auditable) for stakeholders to track source/destination of foreign-activated devices

Global Regulatory Outlook for Foreign SIMs in IoT Devices (2025–2030)

The rapid globalization of the Internet of Things (IoT) has led device manufacturers to embed foreign telecom service providers’ SIM cards or eSIMs into products destined for export. This approach enables *out-of-the-box* connectivity for Machine-to-Machine (M2M) and IoT devices across borders. However, it also raises complex regulatory issues. Governments and regulators worldwide are increasingly scrutinizing the **sale and usage of foreign SIM/eSIM cards in IoT devices** due to concerns ranging from legal compliance and technical constraints to cybersecurity threats and geopolitical implications. Over the next five years, these concerns are expected to intensify alongside IoT's growth (projected **27+ billion connected devices by 2025**). This report analyzes the key regulatory risks – legal, technical, cybersecurity, and geopolitical – associated with using foreign SIMs in export-bound IoT devices. It also examines sector-specific concerns in automotive, healthcare, and consumer electronics, anticipates challenges from emerging technologies (AI-enabled IoT, autonomous systems, edge computing), and recommends safeguards to ensure security, compliance, and traceability.

Major Regulatory Challenges and Risks

Legal and Compliance Issues

Telecom Licensing & Permanent Roaming:

Every country mandates that cellular services on its soil be provided by authorized operators. The use of a foreign SIM means the device remains tied to a foreign operator ("*permanent roaming*"), which can violate local telecom licensing laws. During the 2010s, regulators in **Brazil, China, India, Turkey** and others explicitly **banned or restricted permanent roaming** for IoT/M2M devices. Some rules outright prohibit long-term roaming; others impose local registration or tax requirements that a roaming SIM cannot meet. Regulators are motivated to **protect local telecom markets and enforce laws like lawful interception** (ensuring authorities can monitor communications). As a result, IoT devices that try to operate indefinitely on a foreign SIM risk being deemed illegal or getting disconnected by regulators or host networks. Table 1 summarizes examples of national policies:

Table 1: Selected Countries' Stances on Foreign IoT SIM/Permanent Roaming

Country/Region	Regulatory Stance (IoT SIM in Foreign Devices)
Brazil	*Banned:* Permanent roaming not allowed; IoT devices must use local licensed operator connectivity for long-term use.
China	*Banned:* Foreign SIMs effectively prohibited in-country; devices must join local networks (strict licensing) and comply with data localization policies.
India	*Banned (with exceptions):* Permanent roaming disallowed; foreign SIM/eSIM usage requires a special NOC (No-Objection Certificate) for export-only devices, with KYC and the condition that the SIM *not* function within India.
Turkey	*Banned (short-term limit):* Permanent roaming blocked after a brief period; law mandates local eSIM profiles and local data storage for IoT connectivity (e.g. a 2020 rule stalled car imports until foreign eSIMs were replaced with local profiles).
Oman	*Time-Limited:* International IoT SIMs allowed up to 90 days; beyond that, the device must register locally or get regulatory approval.
EU (Europe)	*Allowed (currently):* No explicit ban on permanent roaming (EU free roaming rules apply for EU-based operators); however, specific regulations (e.g. **eCall** emergency system in cars) **require a local cellular profile** for compliance. European regulators (BEREC) are studying IoT roaming and may update rules in coming years.
USA & Canada	*Allowed (no law against it):* Regulatory authorities have not banned permanent roaming, but **mobile carriers often restrict or forbid long-term roaming in contracts**

Country/Region	Regulatory Stance (IoT SIM in Foreign Devices)
	(to prevent abuse). Large fleets of foreign IoT devices can be throttled or cut off by host networks under these commercial policies.

Import/Export Compliance:

Incorporating foreign SIMs into devices raises additional compliance issues in the device's country of origin. For example, in India manufacturers must obtain a **NOC (No Objection Certificate)** to import and embed foreign SIM/eSIMs in IoT products for export. Regulators are evaluating if a new **service authorization category** is needed for such SIM providers. Authorities like customs and central banks may get involved – e.g. ensuring that importing SIM hardware, or paying foreign service providers, meets import/export and foreign exchange laws. There are also **Know-Your-Customer (KYC)** obligations: even if the SIM is intended for use abroad, regulators often require verification of the entity responsible. India's policy, for instance, demands passport/ID checks for customers of foreign SIMs and periodic reports to security agencies with details of SIM card buyers. In the IoT context, this could translate to requiring the manufacturer or exporter to be the registered "customer" for those SIMs and to maintain records tying each SIM to an exported device (to prevent misuse in the domestic market).

Data Sovereignty and Privacy Laws:

Data transmitted via a foreign SIM may be routed through the foreign provider's core network and servers in other jurisdictions. This triggers **data sovereignty** concerns, as many countries mandate that certain data (especially personal or sensitive data) be stored or processed locally. As of 2024, **71% of countries have data privacy laws** (and ~9% more have pending bills), many of which restrict cross-border data transfers. For example, health or financial data collected by an IoT device may **violate GDPR or other privacy laws if automatically sent to foreign servers** without proper safeguards. Regulators may thus require that IoT devices with foreign SIMs implement **data localization** (keeping data within national borders or providing local data break-out). Some jurisdictions insist that even if connectivity is foreign, the **internet gateway or cloud server be local** to ensure oversight. Compliance with these intersecting laws (telecom and data protection) is becoming a major hurdle – indeed, regulatory hurdles have extended IoT product time-to-market significantly (up ~80% since 2020) according to industry reports.

Liability and Enforcement:

As regulations tighten, companies exporting IoT products face uncertainty about how rules will be enforced. Non-compliance can lead to **devices being abruptly disconnected** from networks after a grace period (often without warning), potentially rendering critical equipment non-functional. There are documented cases: when Turkey introduced its eSIM localization mandate, major car OEMs **could not import connected cars and had to disable certain connected services (like eCall)** to avoid violating the law. Such interventions carry business and legal risks – product recalls, contractual breaches, or even penalties for failing to meet local telecom laws. Manufacturers also face the prospect of needing **multiple product variants (SKUs)**:

one with a foreign SIM for permissive markets and others with local SIMs for restrictive markets. This complicates supply chains and could raise legal questions around product conformity in different regions. Over the next five years, we expect more countries to formalize IoT-specific telecom rules (some via class licenses or operator partnerships) and to strengthen cross-border enforcement cooperation, increasing the legal complexity for global IoT deployments.

Technical and Operational Challenges

Permanent Roaming vs. Local Profiles:

From a technical standpoint, the core challenge is ensuring devices stay connected globally **without violating local network rules**. Traditional SIM cards are tied to one “home” operator and rely on roaming agreements for foreign connectivity. But roaming agreements were designed for temporary travel, not permanent device deployment. Many have built-in time limits (e.g. 30–90 days) after which the device is flagged as *permanent* and may be blocked. Furthermore, some newer cellular IoT technologies like NB-IoT have limited roaming support. The emerging solution is the **eSIM (embedded SIM)** with **Remote SIM Provisioning** capability, which allows devices to **download a local carrier profile over-the-air** in the destination country. With eSIM (and related multi-IMSI technology), a single SIM can switch identities to a local network as needed. In theory, this means an IoT device can ship with a foreign “bootstrap” connectivity profile and later localize itself to comply with local regulations. Indeed, standards like **GSMA SGP.32 (2023)** have streamlined remote provisioning for IoT.

However, **technical constraints** remain. Some regulations (e.g. Turkey's) require not just a local profile, but that **all provisioning infrastructure be operated by a local carrier** – meaning the eSIM must be provisioned via local servers, not a foreign cloud. This necessitates complex arrangements (e.g. partnering with local mobile operators for eSIM management). If the **over-the-air (OTA) provisioning fails**, a device can become unreachable and effectively "bricked" in the field. Unlike consumer devices, IoT gadgets are often unattended or in remote locations, so manual SIM swaps or troubleshooting are impractical. Thus, **OTA reliability** is critical – manufacturers must design fallback logic and test profile swaps extensively. Additionally, if a device localizes its SIM, the original provider might **lose end-to-end control of connectivity** (shifting to the local carrier's core network). This can disrupt unified service management; for example, the device's IP address, security policies, or VPN routing might change once it's on a local core. Operators are developing solutions (like **global IoT connectivity platforms and private IoT APNs**) to maintain a level of control and uniform security even after localization, but these are still evolving.

Interoperability and Standards:

IoT devices are deployed across **multiple industries and countries**, each with their own technical standards and spectrum bands. Ensuring a foreign SIM will work seamlessly everywhere is non-trivial. For example, a device might need certifications for each country's network (radio frequency compliance, permitted bands, etc.). The **technical standards for eSIM** are global, but their implementation can vary. In the next five years, we may see fragmentation in eSIM technology: different regions could enforce their own security standards for SIM provisioning. There is also the rise of **iSIM** (integrated SIM, built into the chipset). iSIMs promise even greater flexibility, but regulators might have concerns about how to audit or control an embedded, non-removable subscriber module.

Network Technology Evolution:

As networks advance (e.g. **5G with network slicing**, upcoming 6G), new technical issues will arise. Network slices could be dedicated to IoT or critical communications and might not support roamers by default for security reasons. **Edge computing** (processing data on local servers closer to the device) is becoming common to reduce latency and comply with data laws. IoT devices may be expected to use local edge nodes for certain services – if they stay on a foreign core network, they could be cut off from local edge benefits or regulatory-required services. For instance, emergency services like *eCall in vehicles* require the device to connect to local emergency infrastructure; technically this might fail if the SIM is still on a foreign network. Regulators in automotive have anticipated this, hence **eCall regulations explicitly mandate local connectivity ability**. Overall, the technical trend is toward **"localization" of IoT connectivity** when devices cross borders, and solutions like multi-IMSI eSIMs, local core network partnerships, and distributed cloud infrastructure will be essential for compliance. Companies will need to invest in more sophisticated connectivity management to navigate the patchwork of technical requirements emerging worldwide.

Cybersecurity and Privacy Concerns

Network Security & Data Interception:

Using a foreign telecom network for device connectivity can introduce unique cybersecurity risks. Data transmitted through foreign carriers might be subject to **interception or surveillance by foreign governments or threat actors**, especially if the data is sensitive. The signaling protocols that enable roaming (SS7 for 2G/3G, Diameter for 4G/5G) are known to have vulnerabilities that have been exploited in the past for espionage or fraud. From a national security perspective, allowing critical IoT devices (e.g. in infrastructure or healthcare) to communicate via an overseas network is seen as a potential **attack vector**. It could bypass local network monitoring and make it harder for the home country to detect and mitigate threats. For example, state-sponsored cyber groups have leveraged weaknesses in telecom signaling to target devices and networks amid geopolitical tensions. This risk is amplified if the foreign SIM's home country is not a trusted ally. We may see new regulations requiring "*prior evaluation*" of foreign connectivity providers for cyber risks or even outright bans on using SIMs from certain nations in critical IoT deployments (analogous to bans on foreign hardware like routers or cameras in sensitive sectors).

Device Security & Updates:

IoT devices are infamously vulnerable, often lacking strong authentication or encryption. If a device's connectivity is cut off (due to roaming restrictions or network issues), it may miss important security updates or patches, leaving it exposed. Conversely, if a hacker gains control of an IoT device, a foreign SIM could allow them to exfiltrate data out of the country undetected or use the device as part of a botnet that is harder for local authorities to track. Ensuring **secure communications** over foreign networks is crucial – IoT devices should use end-to-end encryption for data in transit (so that even if foreign network operators inspect traffic, sensitive content is protected). There are industry initiatives like **IoT SAFE** (which uses the SIM as a secure element for IoT data encryption/PKI) that could help enhance security irrespective of the carrier. Regulators are also stepping in: many countries (UK, EU, U.S., etc.) have introduced or proposed baseline **IoT cybersecurity standards** – such as requiring unique device passwords, vulnerability disclosure policies, and secure update mechanisms. By 2025, the **EU Cyber Resilience Act** and similar laws will likely mandate that connected products meet certain security criteria. This means any IoT device (foreign SIM or not) must be designed with security in mind (e.g. resisting unauthorized SIM profile changes, preventing SIM cloning, and safeguarding data).

KYC and Privacy:

Another cybersecurity aspect is the abuse of foreign SIMs for anonymity or fraud. Traditionally, anonymous prepaid SIMs have been used for illicit purposes; governments responded with mandatory SIM registration (often requiring passports or even biometrics for SIM purchase). IoT SIMs are usually issued to companies, not individuals, but regulators worry that foreign M2M SIMs could be repurposed for illegal use (since they might not be subject to local KYC). This ties into **traceability**: authorities want to know *who* is responsible for each device and be able to trace a device's communications if it's involved in wrongdoing. Hence, we see proposals to record each IoT SIM's ICCID/IMSI, device IMEI, and end-use details at the point of export or activation. Privacy regulations also require careful handling of any personal data that IoT devices collect. For instance, an automotive IoT system might collect driver behavior or location – if such data is funneled to a foreign cloud via the SIM, user consent and compliance with laws like GDPR are needed. Over the next five years, **AI-enabled IoT devices** (discussed later) will collect even more intimate data, raising the stakes for privacy. Regulators will expect robust encryption, anonymization, and possibly **on-device data processing (edge AI)** to minimize raw data transmitted across borders.

In summary, the cybersecurity and privacy risks demand a dual approach: hardening the *devices and data* themselves against threats, and managing the *network pathways* to prevent malicious interception or misuse. Any regulatory framework allowing foreign SIMs in exports must include strict cybersecurity requirements (secure provisioning, data protection, incident reporting) to mitigate these risks.

Geopolitical and Market Dynamics

National Security & Sovereignty:

IoT connectivity has become a matter of sovereignty. Countries view the prospect of foreign-controlled connectivity in devices within their borders with suspicion. From a geopolitical perspective, **telecom networks can be weaponized** – for surveillance, disruption, or influence. If a country A's exported device uses country B's SIM/network when deployed in country C, it creates a complex chain of dependencies. Country C might worry that country B (through its telecom company) could gather intelligence on C's territory or users via the device's communications. Likewise, country A (the exporter) might worry that if relations sour with country B (the SIM provider's country), service could be cut off to all its exported devices. These concerns are not hypothetical: in recent years, geopolitical disputes have led to sanctions affecting technology and communication services (e.g. restrictions on Huawei equipment, sanctions on telecom services in certain regions, etc.). It is plausible that **certain nations could ban IoT devices that rely on SIMs from adversary nations** for critical sectors – for example, a Western country might forbid critical infrastructure sensors from using Chinese-based eSIM connectivity, or vice versa.

Trade and Economic Factors:

The use of foreign SIMs in devices also has an economic dimension. Local mobile operators fear losing revenue if devices bypass local SIMs in favour of foreign ones. This has led to lobbying for regulations against permanent roaming (to force IoT OEMs to procure local connectivity instead). In some cases, regulators frame the issue in terms of unfair competition: a foreign MVNO (Mobile Virtual Network Operator) providing IoT service nationally via roaming might undercut local carriers who paid for spectrum licenses. For instance, **permanent roaming is perceived as competition to local operators** and has driven some to renegotiate roaming agreements or push for revenue-sharing from IoT devices. Over the next few years, we might see **bilateral or regional agreements** to handle IoT roaming – perhaps treaties or pacts that allow some level of IoT roaming in exchange for data-sharing or fees. The EU's examination of M2M roaming suggests a possible coordinated approach in that region, potentially influencing global norms.

Global Standards and Diplomacy:

Geopolitically, standards bodies (like the ITU, GSMA) will be battlegrounds for these issues. There is already an **international M2M SIM**

numbering standard (e.g. country code 901 for global services) – but adoption depends on national regulators permitting those “global” SIMs. Diplomatic efforts may aim to create a harmonized framework so that an IoT device can legally operate globally without dozens of national SIM swaps. However, given current trends, a fully liberalized environment is unlikely; instead, the norm is leaning toward **“local empowerment”** – requiring foreign providers to team up with local entities. Some countries (e.g. Saudi Arabia, as noted in regional studies) require foreign IoT service providers to set up a local presence or get a local telecom license to serve IoT devices in-country. This essentially forces foreign SIM providers to naturalize into the local ecosystem if they want to persist.

In summary, geopolitics injects a layer of uncertainty: regulatory regimes could shift quickly with political winds, and companies must monitor export controls and international policies. IoT connectivity could even become a bargaining chip in trade negotiations (“allow our IoT devices to operate in your country and we’ll reciprocate”). The next five years will likely see **heightened scrutiny of cross-border IoT communications** in light of national security, and possibly the emergence of *trusted zones* of connectivity (where, for example, devices can roam freely among allied countries but face restrictions elsewhere).

Industry-Specific Regulatory Concerns

Various industries deploying connected devices face unique regulatory concerns related to foreign SIM usage. Below we examine three key sectors – **automotive, healthcare, and consumer electronics** – highlighting how regulations and risks manifest in each:

Automotive (Connected Vehicles)

Modern vehicles are increasingly equipped with IoT capabilities – from telematics and infotainment to critical safety systems. Automakers often embed eSIMs to provide connectivity (for features like live navigation, OTA updates, or emergency calls) across multiple countries. **Regulatory issues for automotive IoT include:**

- **Emergency Services Compliance:** In many jurisdictions, regulations like Europe's **eCall mandate** require that a car in an accident **must be able to dial local emergency numbers** and transmit its location to local responders. If a car were relying on a foreign SIM locked to a distant home network, this call might not route correctly. Thus, automotive eSIM implementations must ensure a local carrier profile is available specifically for emergency calling (or roaming agreements cover emergency access). Regulators will not approve vehicles that can't meet these life-saving connectivity requirements.
- **Cybersecurity and Safety Standards:** The automotive industry is subject to stringent safety regulations. New UNECE WP.29 regulations on vehicle cybersecurity (adopted in EU, Japan, etc.) require manufacturers to mitigate cyber risks in vehicles. Connectivity is a major attack surface – a foreign SIM connecting to foreign networks could be seen as a higher risk if those networks are less trusted. Manufacturers must demonstrate that even if connectivity goes through foreign carriers, security controls (encryption, authentication) are in place. Additionally, **ISO/SAE 21434** (an automotive cyber standard) and related regulations push automakers to secure the entire supply chain – which includes vetting telecom

partners. Regulators may ask automakers to provide risk assessments for using certain foreign connectivity providers in their cars.

- **Data Privacy and Localization:** Connected cars generate data on drivers, vehicle performance, locations, etc. Privacy laws like GDPR treat much of this as personal data. If an exported car sends data back to the manufacturer's servers overseas via an onboard SIM, it constitutes cross-border data transfer. Automotive companies must navigate data consent and localization requirements per market: China, for example, has laws that automotive data (like geolocation or camera imagery) collected in China must be stored in China. A car with a foreign SIM that directly streams data out would violate that; hence manufacturers like Tesla have had to set up local data centers and possibly use local connectivity in such markets. We anticipate more nations implementing **vehicle data sovereignty** rules, given the sensitivity (cars can map cities, record surroundings, etc.). Regulations may require that foreign SIMs in cars either tunnel data to a local cloud or hand off to a local carrier soon after the vehicle is imported.
- **Type Approval and Telecom Compliance:** When cars are homologated (approved) for sale in a country, regulators check radio equipment compliance. The SIM/eSIM and its profiles might become part of that approval. For instance, authorities could insist that the eSIM be provisioned with an approved local operator profile by default for their market. We could see the emergence of **regional IoT connectivity approvals** – e.g. a car model might need a certificate from the telecom regulator that its connectivity setup meets local

norms. This adds another layer to car manufacturing (beyond safety and emissions testing).

In summary, the automotive industry must ensure that **connectivity in vehicles is not only global and convenient but also locally compliant and secure**. The trend is towards hybrid solutions: global eSIMs for flexibility, combined with local network integrations for compliance. Over the next five years, as vehicles become even more autonomous and data-hungry, expect tighter integration between automotive regulations and telecom requirements.

Healthcare (IoMT – Internet of Medical Things)

IoT in healthcare includes wearables, implantable devices (pacemakers with telemetry), remote patient monitoring systems, smart hospital equipment, etc. These devices often transmit highly sensitive personal and health data and can even be life-critical. Regulatory concerns in this sector include:

- **Patient Data Protection:** Healthcare data is protected by strict privacy laws (such as HIPAA in the US, GDPR in Europe, and various national health data acts). If a medical IoT device uses a foreign SIM to send patient vitals to a cloud platform overseas, it might breach data export restrictions or require patient consent that is hard to obtain for an embedded device. Regulators will likely require that **medical IoT data either stays within the country or is transferred securely to jurisdictions with equivalent data protection**. In the EU, for example, sending personal health data to a cloud outside the EU may require specific legal safeguards. Thus, healthcare IoT firms may need to incorporate **edge computing** – processing or storing data locally (e.g. on a hospital server) and only sending aggregated or anonymized data through the foreign network.

- **Device Safety and Reliability:** Many medical devices must be certified by health authorities (like FDA approval in the US or CE marking in EU). If a device's therapeutic function could be impacted by connectivity issues, regulators will scrutinize that. For instance, a wearable insulin pump might adjust dosing based on remote commands; if it loses connectivity due to a foreign SIM being blocked or network latency, there's a safety risk. We anticipate regulators will demand **risk mitigation plans for connectivity loss**. This could mean requiring a device to have fail-safes (e.g. default to a safe mode if disconnected) or even dual SIM capability (one primary SIM and a secondary local SIM for backup connectivity in critical devices).
- **Regulatory Approvals & Clinical Data Laws:** Using foreign SIMs might complicate obtaining regulatory approval for medical devices. Agencies could ask: who has access to the data path? Is there any chance patient data could be intercepted by foreign entities? The answers could affect approval. Additionally, clinical trials data transmitted from devices across borders might violate local trial regulations if not properly handled. Expect health regulators to coordinate with telecom regulators on guidelines for **medical device connectivity**, emphasizing encryption, authentication, and possibly requiring that foreign network providers sign agreements to uphold privacy (or routing data via secure VPNs into the country).
- **Traceability in Healthcare IoT:** Traceability is crucial in healthcare – if a device malfunctions, you need to trace its usage and data logs.

With foreign connectivity, traceability can suffer if data records reside in another country or if the SIM isn't registered locally. To counter this, regulations might require that **each connected medical device be registered in a national database** (serial number, SIM number, who's responsible, etc.). Some countries already require registering medical devices; adding connectivity info could be next. This ensures if there's an alert about a foreign SIM being misused or an incident, the device can be quickly identified and located.

In summary, the **healthcare IoT sector will face a very cautious regulatory environment**: the tolerance for risk is low because human lives and sensitive data are at stake. Foreign SIMs will only be acceptable if strong assurances are in place regarding data security and continuous service. Manufacturers should be prepared for exhaustive compliance steps when deploying connected health devices internationally (including possibly negotiating connectivity that routes through local health data hubs).

Consumer Electronics and Smart Devices

This category is broad – encompassing smart home appliances, wearables, personal gadgets, smart city sensors, and industrial IoT devices used by consumers or businesses. Key regulatory and risk considerations here include:

- **Consumer Protection and Privacy:** Consumer IoT devices (like smart speakers, GPS trackers, kids' smartwatches, etc.) often collect personal data. Many jurisdictions are adopting specific **IoT consumer security regulations** – e.g., the UK's Product Security and Telecommunications Infrastructure Act (PSTI Act) which mandates basic security features for consumer connectable products. Such laws might extend to requirements on how data is handled. A device that streams audio or video to a foreign server via an embedded SIM could raise red flags. Expect regulations (or at least strong guidelines) that **manufacturers be transparent about where data goes and obtain user consent for cross-border data flows**. There may also be import restrictions on products that don't meet security standards (for example, requiring certification labels for IoT cybersecurity). A foreign SIM product might need a local representative to be accountable for compliance, under laws similar to how EU requires an "authorized representative" for product compliance.

- **Network Interference and Spectrum:** Consumer devices with cellular capability must comply with telecom regulations like any mobile phone would (spectrum use, network access rules). If a foreign SIM device isn't homologated for local networks, it could cause interference or just fail to work properly. Regulators will ensure such devices are tested for network compatibility. Also, some countries limit the types of services a SIM can be used for – for instance, a device with a foreign SIM should not be used to offer unauthorized telecom services (like a Wi-Fi hotspot selling bandwidth, which could verge into telecom operator territory without a license).
- **The Risk of Botnets and DDoS:** On the cybersecurity front, poorly secured consumer IoT devices have been hijacked for botnets (e.g. Mirai botnet). If many devices have foreign SIMs, an attacker could potentially coordinate them via channels outside of local internet service providers' view. This makes it harder for local authorities to detect or mitigate large-scale attacks originating from these devices.

Regulators might respond by imposing **compliance audits** – requiring vendors to ensure their devices meet certain cyber hygiene if they want to enable an always-connected SIM. We might also see **mandatory kill-switches or emergency update mechanisms**: regulators could insist that manufacturers be able to remotely disable or patch a fleet of devices if they are compromised, which entails maintaining robust connectivity management (ironic if that connectivity is reliant on a foreign SIM that might be blocked – it underscores the need for pre-arranged local fallback connectivity in emergencies).

- **Cross-border Usage and "Permanent Tourists":** Many consumer devices are portable (think: a smartwatch or a pet tracker sold in Country A that a user might take and use in Country B). If these come with an included global SIM plan, they will effectively roam. While travel with personal devices is normal (and usually within roaming policies), regulators may look at large deployments. For example, if a certain popular gadget from country X floods a local network with thousands of roaming SIMs, local operators might enforce their own limits. This means consumer device makers need to work closely with connectivity providers to ensure their global SIM can actually operate in all target markets without violation – often via **commercial agreements for permanent roaming or local profile provisioning in each region**. The complexity of that can be high, and failure leads to devices losing connectivity in certain regions, which could result in consumer complaints or legal liability for advertised features not working.

Overall, in consumer IoT, **regulatory attention is intensifying around security, privacy, and network resilience**. Devices are smaller and cheaper, but regulators will not give them a free pass – indeed, insecure consumer devices have been identified as national cybersecurity risks. Therefore, using foreign SIMs in them must be balanced with rigorous compliance measures.

Future Technologies and Emerging Risks

Looking ahead, several technological developments will shape regulatory challenges for IoT connectivity in the next five years:

AI-Enabled IoT Devices

As artificial intelligence gets embedded into IoT devices ("AIoT"), devices will make more autonomous decisions and handle more sensitive data (e.g. facial recognition on smart cameras, predictive health diagnostics on wearables). AI algorithms often require large datasets and constant updates. **Regulatory implications:**

- **AI Regulation Intersection:** Regions like the EU are introducing AI-specific regulations (e.g. the EU AI Act) that will classify certain AI uses as high-risk, requiring transparency and risk mitigation. An AI-enabled IoT device (say an autonomous drone using AI for navigation) could fall under such rules. If that device uses a foreign SIM, compliance oversight is harder – authorities may worry that the AI model or decisions could be influenced or controlled remotely over a channel they can't easily monitor. Regulators might require that **AI functions remain operable even if connectivity is lost or compromised**, to avoid dangerous failures. Additionally, training data or telemetry from AIoT devices might be subject to data export controls if it contains personal information.

- **Real-time Decision and Latency:** Many AIoT and autonomous systems (discussed next) need low-latency connectivity (for example, a self-driving car coordinating with infrastructure). If such systems rely on roaming connectivity, latency could increase and reliability decrease. This technical challenge becomes a regulatory/safety issue – we could see rules mandating that critical real-time AI systems (like automated driving or robotic surgery devices) **use local (edge) connectivity** to guarantee performance. In essence, foreign SIM connectivity might be deemed unfit for ultra-critical applications due to the unpredictability of cross-border networks.
- **Security of AI Models:** AI on edge devices often needs model updates or data uploads for learning. A malicious actor could attempt to tamper with an AI model by intercepting these updates. If updates are delivered over a foreign network, it might bypass certain security filters. Regulations might hence require that **AI model updates be delivered via trusted channels**. We may even see certification requirements for AIoT devices to prove that their communication links (no matter through which SIM) meet high security standards (to prevent adversarial attacks on the AI, like feeding it wrong data).

In summary, AI integration will push regulators to demand more reliability and security from IoT connectivity. Foreign SIMs will be acceptable for AIoT only if they can match the assurances of local links. Expect cross-domain collaboration between telecom regulators and AI regulators to address these issues.

Autonomous Systems and Vehicles

Autonomous devices – whether self-driving cars, delivery drones, or industrial robots – rely heavily on connectivity for navigation updates, remote supervision, or V2X (vehicle-to-everything) communications. They also pose direct safety risks if something goes wrong. Key considerations:

- **Regulatory Safety Requirements:** Autonomous vehicles are being regulated carefully (e.g. requiring safety drivers, redundant systems). Connectivity is often considered part of the redundancy – for instance, a drone might be required to have a communication link to an operator or a geofencing system. If that link is via a foreign SIM, questions arise: what if the drone loses signal due to roaming issues? Therefore, regulators may mandate **multi-network capability**: an autonomous device must be able to switch to a local network or have a fallback method (perhaps even satellite connectivity) if its primary link fails. There could also be rules about *command and control links* – for national security, some countries might insist that any remote control of autonomous vehicles be done through local networks that authorities can potentially access or shut down if needed (e.g. to prevent misuse as weapons). A foreign SIM might not afford that level of control.
- **Geofencing and Location Tracking:** Many countries regulate drones and autonomous machines by requiring them to broadcast identification and location (e.g. Remote ID for drones). If the device's connectivity is through a foreign service, will local authorities be able to receive those signals or track the device? We anticipate that **traceability of autonomous devices** will be a legal requirement –

possibly needing registration of connectivity identifiers similar to aircraft. For cross-border movement of autonomous vehicles, regulators might even require a means to remotely disable or take over the device in emergencies. This is only feasible if the communication channel is known and secure. Thus, foreign connectivity providers will need to work on agreements that, for example, allow law enforcement in the device's country of operation to send a kill command or track signal via the foreign network in real time (a challenging but likely necessary safeguard).

- **Edge Computing & V2X Infrastructure:** Autonomous cars and smart infrastructure will use **edge computing and V2X communication** (e.g. cars talking to traffic lights). Regulators (and city authorities) want these systems to be reliable and typically favor **localized communication** (like direct short-range communication or using local 5G base stations). A car that tries to use a distant home server via roaming for split-second decisions is both technically and regulatorily disadvantaged. We may see de facto requirements that **autonomous systems operate on local telecom slices or dedicated networks** for safety, which again pressures the use of local SIM profiles or agreements. Over time, if autonomous vehicles become mainstream, countries might legislate that they must integrate with national connected vehicle services (for traffic management, etc.), effectively forcing any foreign connectivity to be switched upon entry.

Overall, autonomous tech will likely **limit the tolerance for foreign-managed connectivity** because of the critical safety and security aspects.

This doesn't mean foreign SIMs can't be used – but they must be coupled with strong guarantees (like local failover, regulatory access, etc.).

Edge Computing and 5G Networks

Edge computing – processing data closer to where it's generated – and advanced 5G networks are transforming IoT deployments. They aim to reduce latency, preserve data sovereignty, and increase reliability. Regulatory angles include:

- **Data Localization via Edge:** As mentioned earlier, many data sovereignty laws can be satisfied by processing and storing data locally. Edge computing enables a device with a foreign SIM to still comply by, for instance, using a local edge node for storage and only sending non-sensitive results back abroad. Regulators might encourage or require certain IoT services to use **local edge clouds**. For example, smart city sensors could be mandated to connect to an edge computing center operated by a local entity. If those sensors have foreign SIMs, their traffic might need to be routed (perhaps via a local breakout gateway) to the local edge. This could lead to technical regulations: e.g. requiring that foreign connectivity providers establish local **points-of-presence (PoPs)** or edge servers such that IoT traffic doesn't all backhaul to the home country. Indeed, some IoT connectivity providers already deploy distributed core network nodes worldwide to meet such requirements.
- **5G Slicing and Private Networks:** With 5G, companies can have private network slices or dedicate bandwidth for critical IoT. Regulators are supportive of private networks for industries (some

countries auction localized spectrum for this). If an exported device is intended to join a private 5G network at its destination (say, an industrial robot joining a factory's local 5G), having a pre-provisioned foreign SIM might complicate that – it may need a SIM provisioned to the local network slice. Regulations (or industry standards) might evolve that devices in certain sectors be **"slice-ready"** – meaning they can accept a local network profile easily. Also, roaming on 5G slices may not be straightforward technically or legally, further pushing local provisioning.

- **Resilience and Outages:** One driver for edge computing is resilience – if internet links fail, local processing can continue. Regulators, especially for critical infrastructure IoT, will value resilience. A device solely dependent on a foreign SIM and a distant cloud is seen as less resilient (since international links or remote servers could fail or be cut off). Therefore, expect regulations or guidelines emphasizing **redundancy**: e.g. if a foreign SIM is used, there should be local storage of critical data and perhaps an alternate connectivity path for emergencies.
- **Emerging Technologies:** Looking beyond 5G, developments like **6G** (which might deeply integrate AI and edge) and **LEO satellite IoT networks** could alter the landscape. If satellite IoT (Starlink-type or others) becomes common, devices might bypass terrestrial SIMs altogether. But that raises a similar question: using foreign satellite service might trigger regulatory responses (some countries already require licenses for using satellite terminals). In five years, regulators will likely also be grappling with how to incorporate these new connectivity modes into their frameworks. The common theme

remains: any communication channel a device uses must either be **visible and controllable** to some extent by the host nation or meet certain trust criteria.

In conclusion, **future tech trends push for more local, intelligent networking**, which paradoxically might conflict with the idea of a single global SIM service. Regulatory frameworks will push IoT solutions to be adaptable: leveraging local edges, complying with AI rules, and ensuring autonomous devices behave safely under local oversight. Manufacturers and connectivity providers will need to stay agile to integrate these requirements.

Recommendations:

Regulatory Precautions and Safeguards

To ensure security, compliance, and traceability in the use of foreign SIM/eSIMs for IoT, a comprehensive regulatory framework should implement multiple layers of precaution. Below is a set of recommended safeguards and best practices for regulators, IoT manufacturers, and connectivity providers:

- **1. Specialized Licensing & Oversight:** Establish a **special authorization category** for foreign IoT SIM service providers. Providers must register with the regulator and obtain a license or NOC, agreeing to comply with local laws (lawful intercept, data requests). Regulators should have the power to **audit operations** (including data centers, interfaces) used to provide connectivity in their jurisdiction, and to suspend or revoke authorization swiftly if national security or compliance is threatened.

- **2. Strict KYC and User Verification:** Enforce stringent **Know-Your-Customer** requirements for any foreign SIMs provided. The manufacturer or exporter using the SIMs should be verified as the customer and accountable. Each SIM/eSIM must be associated with a specific device (IMEI or serial number) and end-use. Maintain a **registry mapping SIM ICCIDs ↔ device IDs ↔ export destinations**. This ensures that if a SIM is found operating domestically or in illicit use, authorities can trace it back to the source. Regular reporting to security agencies should be mandated, listing active SIMs, their assigned devices, and usage periods.
- **3. Domestic Use Prevention Measures:** To prevent unauthorized local use of foreign SIMs, require technical safeguards such as **geo-fencing or network locks**. For example, foreign SIMs intended for export devices should be **programmed to not register on domestic networks** of the exporting country, or to automatically deactivate if they do. Likewise, enforce time limits if a device re-enters and stays in the home country (to avoid clandestine local usage). Regulators can work with operators to block foreign M2M SIMs that violate these terms, as a backstop.
- **4. Local Profile Availability (eSIM Localization):** Mandate that any IoT device with a foreign eSIM **supports remote provisioning of local operator profiles**. The device maker should pre-arrange at least one local profile in each target country or region (either via roaming partners or eSIM profile downloads) to ensure compliance with any permanent roaming restrictions. In high-restriction countries,

regulators could require proof that a local IMSI profile will be activated (for instance, a *"localization compliance certificate"* from a partner MNO) before the device is deployed. This way, even if the device starts with a foreign connection, it can seamlessly transition to a fully local service when required.

- **5. Data Localization and Routing Controls:** Implement **data governance rules** for IoT connectivity. Require that data collected in-country by the device be either stored locally or routed in a way that complies with local privacy laws. For example, regulators can demand **IP localization** – local break-out of data traffic to a domestic internet gateway – so that device data doesn't all travel back to the foreign core network unmonitored. In cases where data must leave the country (e.g. to the manufacturer's cloud), enforce usage of **encryption and lawful access mechanisms**, and possibly **data export permits/assessments** for sensitive categories of information.
- **6. Cybersecurity Standards and Certification:** Integrate IoT-specific cybersecurity requirements into the regulatory framework. This includes mandating compliance with standards (such as the ISA/IEC 62443 or NIST IoT security guidelines) for devices using foreign SIMs. Key measures: **unique device identities and strong authentication** (no default passwords), **encryption of communications**, secure boot and update mechanisms, and **regular security testing/vulnerability disclosure**. Regulators should consider a **certification scheme or labelling program** – devices could be required to undergo a security assessment (and perhaps a penetration test focused on the SIM/network interface) before approval for import/export. Such

certification would assure that even if the connectivity is foreign, the device will not pose undue cyber risk.

- **7. Lawful Intercept and Emergency Access:** Ensure that agreements are in place for **lawful interception** of IoT communications when necessary. Foreign SIM providers should commit to cooperating with local law enforcement, either by providing an intercept capability in real-time or handing over relevant data logs upon lawful request (subject to privacy laws). Additionally, regulators should require an **emergency access mechanism** – e.g., the ability to send an emergency command to a device (to shut it down or alter its behavior) via the network. This might involve setting up local proxy gateways that can reach the device's SIM profile on the foreign network in critical situations. Testing of emergency calls (for systems like eCall) and emergency messaging on foreign SIMs should be part of compliance checks.
- **8. Geopolitical Risk Mitigation:** Regulators and industries should conduct **supply chain risk assessments** for connectivity. If a particular foreign SIM or service is deemed high-risk (due to geopolitical tensions or sanctions), precautions should include: diversification (using multiple connectivity providers so no single foreign entity has control), escrow arrangements for eSIM profiles (so a local neutral party could take over provisioning if needed), and **fail-safe modes**. For example, a national regulator might require that critical IoT devices have a way to **"fallback" to a local network or shut down gracefully** if the foreign network becomes unavailable or compromised. Policies could be drafted to restrict use of foreign SIMs

from adversary nations in critical infrastructure outright, while allowing them in low-risk consumer devices – a risk-tiered approach.

- **9. Multi-Stakeholder Coordination:** The regulatory framework should be holistic – telecom regulators must coordinate with sectoral regulators (transport, health, consumer product safety, etc.). For instance, create **cross-sector task forces** to update automotive, healthcare, and consumer electronics regulations to account for connectivity issues. Guidelines for each industry (like a *"Connected Vehicle Telecom Compliance Guide"* or medical device connectivity guide) can help manufacturers understand and meet requirements. International cooperation is also key: share best practices through bodies like the **ITU or G20** for harmonizing approaches, and develop MoUs between countries for mutual recognition of IoT SIM compliance regimes or streamlined data-sharing for enforcement.
- **10. Traceability and Monitoring Systems:** Implement systems to continuously **monitor and audit IoT devices using foreign connectivity**. This could involve the use of an IoT device registry as mentioned, as well as technical monitoring at the network level – e.g., mobile operators could be mandated to flag unusual roaming patterns (a spike in foreign M2M SIM usage on local networks) to the regulator. Regulators might also require periodic **compliance reports** from SIM providers/manufacturers, including metrics like number of devices deployed per country, average roaming duration, any compliance incidents (devices blocked, etc.). By having ongoing visibility, regulators can dynamically adjust policies (for example, if devices are found not respecting the "export-only" rule, crackdowns can follow quickly).

- **11. Future-Proofing Provisions:** Given the fast pace of tech, the regulatory framework should be adaptive. Include clauses that allow regulators to **impose new conditions as needed** in the interest of security and public interest – for example, if AI in IoT becomes regulated or if new network tech (like 6G or satellite IoT) emerges, the telecom authority can swiftly mandate relevant changes (like requiring a new form of SIM authentication, or forbidding certain unsecure protocols). Regulators should also encourage **innovation sandboxes** – allowing IoT firms to pilot new connectivity approaches under supervision – which can inform better rules without stifling innovation.
- **12. Education and Support:** Finally, accompany regulations with guidance documents and support for compliance. Many IoT manufacturers (especially startups) may not be well-versed in telecom regulations. Regulators can publish clear guidelines, checklists, and even offer compliance workshops or portals. For example, a guideline on "Using eSIMs in Exported IoT Devices" could summarize the do's and don'ts for companies. This proactive approach helps industry comply willingly and effectively. Additionally, fostering standards (through GSMA, IEEE, etc.) for eSIM use in IoT can create a baseline that aligns with regulatory expectations, reducing friction.

By implementing these precautions, TRAI can create an environment where **global IoT deployments are feasible without sacrificing national security, user privacy, or regulatory control**. The goal is a balanced regime that permits manufacturers to leverage foreign connectivity solutions for convenience and scale, while ensuring that appropriate checks, local integrations, and fail-safes are in place. In essence, the framework should turn the foreign SIM from a potential risk into a transparently managed component of the IoT ecosystem.

Conclusion

The coming five years will be pivotal in shaping how the global IoT industry balances seamless connectivity with sovereign regulations. The use of foreign telecom SIM/eSIM cards in export-bound IoT/M2M devices offers tremendous advantages for global operation, but it intersects with a host of regulatory domains – telecommunications law, data privacy, cybersecurity, and sector-specific safety rules. **Regulatory issues such as permanent roaming restrictions, data localization demands, KYC and licensing requirements, and national security concerns are already prompting changes worldwide**. Industries like automotive, healthcare, and consumer tech illustrate that a one-size-fits-all approach won't work; regulations must account for different risk profiles and use cases. Meanwhile, emerging technologies – AI on the edge, autonomous machines, advanced 5G/6G networks – will introduce both solutions (e.g. better local processing) and new challenges (e.g. need for ultra-reliable links).

The analysis shows that regulators are moving toward a paradigm of **"local accountability"** for globally connected devices. Companies leveraging foreign SIMs will need to architect their connectivity with compliance in mind – using tools like eSIM for local network provisioning, encryption for data-in-transit, and partnerships with local operators or data centers to satisfy laws. On the regulatory side, a robust framework with the recommended safeguards can mitigate risks. Measures like specialized licensing, enforced localization capabilities, cybersecurity standards, and traceability mechanisms are instrumental in addressing the legal, technical, and geopolitical dimensions of the issue. When properly implemented, they ensure that even if a device connects via a foreign operator, it remains **visible, controllable, and secure** from the standpoint of the host nation.

Ultimately, international dialogue will be important – finding ways to allow IoT connectivity to flourish across borders while respecting each country's requirements. Regulatory bodies, industry alliances, and standards organizations should continue to collaborate on best practices and perhaps move toward mutual recognition of certain compliance measures (analogous to how telecom equipment certifications work). By anticipating the risks and acting proactively – as outlined in this report – stakeholders can avoid reactionary bans and instead enable a **future of globally connected, yet locally compliant, IoT deployments**. The balance of innovation and regulation is delicate, but with comprehensive safeguards and cooperative oversight, the benefits of IoT can be realized without compromising on security, privacy, or sovereignty.

Thanks.

Sincerely Yours,

(Prof. Dr.Kashyapnath)
President