

India Tightens Security Rules for Satellite Communication Service Providers

May 7, 2025 • vajiramandravi.com



What's in Today's Article?

- India Satellite Communication Guidelines Latest News
- Key Compliance Requirements for Satcom Companies in India
- Current Regulatory Landscape
- India Satellite Communication Guidelines FAQs

India Satellite Communication Guidelines Latest News

- India's Department of Telecommunications (DoT) has issued stricter security guidelines for satellite communication (satcom) services.
- It added new conditions related to data localization, website blocking, metadata collection, and the integration of the indigenous NavIC (Navigation with Indian Constellation) positioning system.

Key Compliance Requirements for Satcom Companies in India

- The Department of Telecommunications (DoT) has issued a set of security and operational guidelines for satellite communication firms such as **Starlink** (Elon Musk), Amazon's Kuiper, Eutelsat OneWeb, and Jio.

Key Compliance Requirements

- **Local Manufacturing**
 - Companies must submit a year-wise phased manufacturing plan, aiming to indigenise at least 20% of the ground segment within five years of starting commercial operations.
- **Data Localisation**
 - All satellite communication-related data must be stored within India.
- **Domestic Navigation System Integration**
 - Mandatory integration of NavIC, India's regional navigation system, in user terminals on a best-effort basis, with full transition required by 2029.
- **Website Blocking Mechanism**
 - Firms must enable systems to block government-identified websites.
- **Cooperation with Law Enforcement**
 - Companies are required to collect and share metadata with security agencies when requested.

Enhanced Data Localisation Requirements

- **No Routing Through Foreign Gateways**
 - Satcom operators must ensure that user traffic originating from or destined for India is not routed through any foreign gateway, Point of Presence (PoP), or space system not part of the designated satellite constellation.
- **No Data Mirroring Abroad**
 - Operators are prohibited from mirroring Indian user traffic to any server/system located outside India.
- **Decryption Ban Outside India**
 - Companies must undertake not to copy or decrypt Indian telecom data outside the country.
- **India-Based Infrastructure Mandate**
 - Data centres, DNS resolution systems, and lawful interception mechanisms must be located within India.
 - Network control, user terminal monitoring, and equipment control must also operate from within Indian territory.

National Security and Law Enforcement Cooperation

- **Service Restrictions During Emergencies**
 - Companies must be capable of restricting services to individuals, subscriber groups, or regions during periods of hostilities or national emergencies.
- **Clearances for Voice and Data Services**
 - Separate security clearances are required before launching voice or data communication services.

- **Special Monitoring Zones (SMZs)**

- Designated zones include areas within 50 km of international borders and coastal regions up to the Exclusive Economic Zone (200 nautical miles).
- These zones will be monitored by law enforcement and security agencies.

- **Real-Time User Terminal Tracking**

- Operators must provide real-time location data (latitude-longitude) of all user terminals, both fixed and mobile, upon request.
- They must also report foreign or unregistered terminals connecting from within Indian territory.

Strategic Intent

- These guidelines reflect India's push for:
 - Digital sovereignty
 - National security
 - Promotion of indigenous technologies like NavIC
 - Boosting local manufacturing in telecom infrastructure

Current Regulatory Landscape

- Starlink is currently undergoing security clearance to begin operations in India.
- It has already formed retail partnerships with Airtel and Jio.
- The Telecom Regulatory Authority of India (TRAI) is finalising the **satellite spectrum allocation** framework, which will impact how these companies operate.

India Satellite Communication Guidelines FAQs

Q1. What is NavIC and why must satcom firms use it?

Ans. NavIC is India's regional navigation system; satcom firms must integrate it for better national security and self-reliance.

Q2. What are India's new data localisation rules for satellite firms?

Ans. Firms must store all user data in India and avoid routing or mirroring traffic through foreign servers or systems.

Q3. Which companies are affected by these new DoT guidelines?

Ans. Starlink, Amazon Kuiper, Eutelsat OneWeb, and Jio must follow India's new rules to operate satellite communication services.

Q4. What infrastructure must satcom companies locate within India?

Ans. Data centers, DNS resolution, lawful interception, and user monitoring systems must be physically based within Indian territory.

Q5. How must firms cooperate with Indian law enforcement?

Ans. They must provide real-time user tracking, metadata, and block access in sensitive zones when requested by authorities.

Source: [IE](#) | [LM](#) | [TR](#)

Source: <https://vajiramandravi.com/current-affairs/india-tightens-security-rules-for-satellite-communication-service-providers/>

© Vajiram & Ravi. For personal use only.