Indian Telecom Security Assurance Requirements (ITSAR) – India’s Proposed Smartphone Security Regime

January 12, 2026 • vajiramandravi.com

ITSAR Latest News

- The Union Government is considering legally enforcing Indian Telecom Security Assurance Requirements (ITSAR) for smartphones, involving 83 security standards, including **source code disclosure**, software controls, and user-permission restrictions.
- This has triggered **strong resistance** from global smartphone makers like Apple (5% market share in India), Samsung (15%), Google, and Xiaomi (19%), who argue that many provisions lack global precedent and threaten proprietary technologies.

Background

- India is the world’s **second-largest** smartphone market with nearly 750 million users.
- **Rising online fraud**, cybercrime, and data breaches have prompted the government to strengthen device-level security.

- The proposals align with the Indian PM's broader push for digital security and data sovereignty.
- Similar tensions have emerged earlier over mandatory cyber safety apps (later revoked), and stringent testing norms for security cameras due to national security concerns.

Key Features of the Proposed Security Standards

- **Source code disclosure:**
  - Manufacturers must submit proprietary source code for review and vulnerability analysis by government-designated labs.
  - **Objective**: Detect backdoors and systemic vulnerabilities.
  - **Industry response:**
    - The Manufacturers' Association for Information Technology (MAIT) calls it "not possible" due to corporate secrecy and privacy norms.
    - No such requirement exists in the EU, North America, Australia, or Africa.
- **Background permission restrictions:**
  - Apps cannot access camera, microphone, or location in the background. Mandatory continuous status-bar alerts when permissions are active.
  - **Concern**: No global precedent or standardized testing method.
- **Permission review alerts:** Devices must periodically prompt users to review app permissions. Industry wants alerts limited to "highly critical" permissions to avoid user fatigue.
- **One-year log retention:**
  - Phones must store security audit logs (logins, app installs) for 12 months.
  - **Industry concern:** Consumer devices lack sufficient storage capacity.
- **Periodic malware scanning:** Mandatory automatic malware scans. **Concerns**: Battery drain, slower device performance, etc.
- **Removal of pre-installed apps:** All non-essential pre-installed apps must be removable. Companies argue many apps are integral system components.
- **Mandatory notification of software updates:**
  - Manufacturers must inform the National Centre for Communication Security before releasing major updates or patches.
  - **Industry view:** This will be impractical during zero-day vulnerabilities. Delays may increase user exposure to active cyber threats.
- **Tamper detection (Rooting/Jailbreaking):** Devices must detect tampering and show persistent warnings. **Industry response:** No reliable universal detection mechanism exists.
- **Anti-rollback protection:** Blocking installation of older software versions, even if manufacturer-signed.
- **Concern**: No global standard; may restrict legitimate use cases.

Key Challenges and Way Ahead

- **Data Security vs proprietary rights**: Risk of exposing trade secrets. Risk-based regulation focusing on critical vulnerabilities rather than blanket controls.

- **Lack of global precedent**: Potential regulatory overreach. Adopt global best practices aligned with **OECD** and EU cybersecurity norms.
- **Ease of doing business**: Compliance costs may deter investment. Ensure time-bound clearance mechanisms for security updates. Strengthen user-level security **awareness** alongside device-level controls.
- **Operational practicality**: Update delays, battery drain, storage constraints. Explore independent third-party audits instead of direct source code disclosure.
- **Innovation chill**: Excessive regulation may impact R&D. Maintain a balance between national security, privacy, and innovation.

Conclusion

- India's proposed smartphone security framework (ITSAR) reflects legitimate concerns over cybersecurity, data protection, and national security in a rapidly digitising economy.
- However, enforcing intrusive measures like source code disclosure without global precedent risks undermining innovation, trust, and market competitiveness.
- A **consultative, proportionate**, and globally harmonised approach is essential to safeguard users while preserving India's attractiveness as a major digital and manufacturing hub.

Source: TH | ET
