

IMEI Tampering - Threat to Digital Sovereignty

Why in News?

Recently, the Department of Telecommunications (DoT) highlighted the growing threat of IMEI tampering under the Telecommunications Act, 2023, emphasizing the need for secure devices in India's expanding digital ecosystem.

The Big Picture - India's Growing Digital Ecosystem

- **Massive Subscriber Base** - Active wireless mobile subscriber base reached 1,204.01 million in July 2026.
- **Core Infrastructure** - Mobile networks and devices directly enable digital payments, online services, and citizen-centric governance.
- **Emerging Threat** - Misuse and unlawful tampering of the International Mobile Equipment Identity (IMEI) number.
- **Impact of Tampering** - Creates devices with altered identities, complicating tracking for law enforcement, threatening consumer safety, and weakening telecom security.

Understanding IMEI and Identifiers

- **What is an IMEI?** A unique 15-digit number that identifies a mobile device on a telecom network.
- **Type Allocation Code (TAC)** - The first 8 digits of an IMEI, which identify the specific device model or type.
- **Allocation Body** - Global System for Mobile Communications Association (GSMA) oversees global TAC allocation to manufacturers.
- **Dual-SIM Devices** - Feature two distinct IMEI numbers (one per SIM slot).
- **How to Check IMEI** - Dial *#06# on any mobile device.
- **Verification Tools** - Check via the Sanchar Saathi portal/app or send an SMS KYM.



What Constitutes Unlawful IMEI Tampering?

- It is illegal for any person to intentionally
- Remove, obliterate, change, or alter a device's unique IMEI number.
- Use, produce, traffic in, control, or possess hardware/software configured to alter IMEIs.

Lifecycle Accountability - Roles and Responsibilities

- **Manufacturers and Importers**
- **Pre-Registration Mandatory** - Must register IMEI numbers on the **Device Setu-ICDR** (Indian Counterfeited Device Restriction) portal prior to sale, testing, RandD, or import.
- **Authenticity** - Must ensure all devices carry valid, unique, and untampered IMEIs.
- **Retailers, Resellers and Brand Owners**
- **Retail and Resale Checks** - Resellers of used devices must verify IMEIs against the Central Government's blacklisted database (paying a nominal verification fee) before completing transactions.
- **Brand Compliance** - Brand owners must register on the Device Setu-ICDR portal and link brands to their relevant GSMA Type Allocation Codes (TAC).

What Citizens Should Avoid

- Procuring or using equipment (modems, SIM Boxes, modules) with configurable/tampered IMEIs.
- Procuring SIM cards using fraudulent documents or impersonation.
- Handing over or selling personal SIM cards to unauthorized third parties.
- Modifying Calling Line Identity (CLI) or caller ID using mobile apps or external websites.

Consumer Precautions and Lost/Stolen Device Protocol

- Buy handsets only from authorized sellers and verify IMEI via Sanchar Saathi.
- Use strong passwords, PINs, or biometrics to secure handsets.
- Repair devices exclusively at authorized service centers to prevent IMEI tampering.

Procedure for Lost or Stolen Handsets

- **Step 1** - File an immediate report with local police and retain a copy.
- **Step 2** - Obtain a duplicate SIM card from your telecom operator.
- **Step 3 (Wait Period)** - Wait 24 hours after SIM activation (per TRAI SMS restriction rules) to receive the OTP for verification.
- **Step 4** - Submit a blocking request on the Sanchar Saathi (CEIR) portal/app with the police complaint and valid ID to receive a unique Request ID.
- **Step 5 (If Recovered)** - Report recovery to local police first, then unblock the device via the CEIR portal using the Request ID.

Legal Framework and Safeguards (Telecommunications Act, 2023)

- **Prohibited Offenses** -
- **Section 42(3)(c)** - Prohibits tampering with telecommunication identifiers (IMEI).
- **Section 42(3)(e)** - Prohibits obtaining SIMs or identifiers through fraud or impersonation.
- **Penalties** - Up to 3 years imprisonment, a fine up to Rs.50 lakh, or both.
- **Offense Status** - Cognizable and Non-Bailable under Section 42(7).
- **Abetment** - Section 42(6) mandates the same punishment for anyone promoting or abetting IMEI tampering.

Reference

[PIB](#)

