Well-Intended, But at What Cost?
BIF Raises Concerns on SIM-Binding Directions to Select Apps Issued under the Guise of Telecom Cyber Security Amendment Rules

New Delhi, 02 December 2025 — BIF expresses serious concern over the *Directions for SIM Binding* issued by the Department of Telecommunications (DoT) on 28 November 2025, mandating that app-based communication services remain continuously linked to the specific SIM card installed in the user's device and forcing periodic six-hour logouts for web/desktop versions.

While well-intentioned in their stated goal of curbing cyber-fraud originating from abroad, the directions raise significant questions of jurisdiction, proportionality, and consumer impact, and risk creating obligations that extend far beyond the mandate of the Telecom Act or the purpose of the Telecom Cyber Security Rules. It is disappointing that directions of such far-reaching operational impact have been issued with such short implementation timelines, without any form of public consultation or user-impact assessment.

1. **Jurisdictional and Regulatory Overreach**

A central concern which BIF had cautioned against during the public consultations on the Draft Telecom Cyber Security Amendments has materialized, i.e., the creation of the *Telecommunication Identifier User Entity (TIUE)* category is being misused to issue directions to OTT platforms and digital services, which are entities squarely governed under the IT Act and administered by MeitY.

The Telecommunications Act does not authorise the regulation of OTT communication platforms, nor does it provide the legislative basis to impose telecom-style operational mandates upon them. Yet, under the guise of the Telecom Cyber Security Amendment Rules and without any public consultation, the present SIM-binding directions extend precisely such obligations, that too on a select set of applications.

The directions go beyond the statutory remit, blur settled jurisdictional boundaries between the Telecom Act and the IT Act. This is a problematic instance of regulatory overreach by the executive without legislative sanction and unfortunately, any stakeholder engagement.

2. **Disproportionate Disruption for Genuine, Law-Abiding Users**

In their current form, the SIM-binding and forced periodic logout requirements could **impose material inconvenience and service disruption on ordinary users, while offering** limited incremental benefit against sophisticated fraud networks.

Ordinary use cases—such as travellers and NRIs who rely on Wi-Fi to use their Indian numbers abroad, professionals who depend on uninterrupted web-client access during an 8–10 hour workday, families and multi-SIM users who routinely separate their primary SIM from their messaging number, and elderly or low-literacy users who struggle with repeated re-authentication—stand to be disproportionately affected.

The result is a **consumer cost imposed in the absence of consultation, impact assessment, or proportionality**, and one that risks degrading user experience for compliant, law-abiding citizens.

3. **Selective Application**

The selective applicability of these directions creates clear avenues for **regulatory arbitrage**. By covering some services and excluding others that operate in an identical manner, the approach could have the effect of bad actors simply migrating to platforms not subject to these obligations. It also results in unequal treatment of similarly situated services, contrary to well-established equality principles, and may also lead to market distortions.

4. **Need for Consultation, Technical Feasibility Assessment, and Proportionate Measures**

The effectiveness of SIM-binding measures alone to address cyber-fraud is questionable, particularly when the dominant vectors of cyber-fraud such as the procurement of Indian SIM cards through mule networks, remote access of devices located within India, and well-documented domestic fraud clusters like Jamtara, are only marginally impacted, if at all, by such conditions.

At the same time, the proposed obligations raise serious questions of technical feasibility, given OS-level restrictions (particularly within iOS), dual-SIM and eSIM complexities, and the significant architectural redesign that TIUEs would be compelled to undertake.

A narrow SIM-binding requirement risks diverting attention from more impactful measures: strong SIM-KYC enforcement, and coordinated enforcement across telecom operators, financial intermediaries, and law-enforcement agencies.

In this backdrop, it becomes imperative that DoT pause the current implementation timelines, open a formal stakeholder consultation, constitute a technical working group of OS providers, TIUEs, licensees, and security experts, and ultimately adopt a risk-based and proportionate framework consistent with constitutional standards of necessity and least intrusive means.

Mr. T.V. Ramachandran, President, BIF said: "BIF stands ready to work constructively with the Government to strengthen India's telecom cybersecurity architecture. However, the apprehension during earlier consultations that digital and OTT services may inadvertently be brought under telecom-style obligations now stands visibly manifest in the present directions. This makes it all the more essential that any measure of this magnitude must be backed by legislative sanction, and respect jurisdictional boundaries and undergo transparent, consultative scrutiny so it causes minimal disruption for millions of genuine users and businesses."