Summary: DSCI's Submission on RBI's Draft Master Directions on Cyber Resilience and Digital Payment Security Controls for PSOs

The Data Security Council of India (DSCI) submitted its comments on the Reserve Bank of India's draft master directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators (PSOs). DSCI welcomes the RBI's continued efforts to strengthen India's digital payment ecosystem and appreciates the forward-looking provisions introduced in the draft.

DSCI acknowledges the draft guidelines as a step in the right direction for enhancing cybersecurity in the payments ecosystem. The directions aim to:

- Improve protection against cyber threats, data breaches, and financial fraud.
- Build greater consumer trust, supporting wider adoption of digital payments.
- Foster collaboration among PSOs to share cyber threat intelligence and best practices.
- Encourage adoption of emerging technologies and robust cybersecurity solutions, contributing to long-term digital resilience.

These measures are expected to not only enhance the security posture of payment system operators but also boost financial inclusion and innovation in the sector.

While supportive of the overall direction, DSCI highlighted a few concerns for RBI's consideration:

1. Applicability to Unregulated Entities

- Concern: Section 5 of the draft mandates PSOs to ensure unregulated entities they work with comply with the cyber security directions. However, PSOs may find it practically difficult to enforce compliance on entities they do not regulate or control.
- Recommendation: RBI could consider embedding these obligations through contractual arrangements between PSOs and unregulated entities, ensuring shared responsibility without burdening PSOs with disproportionate accountability.

2. Incident Reporting Requirements

- Concern: The requirement to report "any unusual incident" within 6 hours (including settlement delays and internal frauds) is overly broad and may dilute focus on actual cybersecurity-related incidents. Moreover, without access to Annexures referenced in the draft (Annex 1 and 2), the scope of reportable incidents remains unclear.

- Recommendation: RBI should consider streamlining and clarifying the reporting regime by:
    - Defining “unusual incidents” with precision.
    - Clearly distinguishing cybersecurity incidents from other operational issues.
    - Ensuring that only material incidents warrant urgent reporting to both RBI and CERT-In, to avoid reporting fatigue and operational disruptions.

Conclusion

DSCI’s submission underscores the importance of a balanced and pragmatic approach to cybersecurity regulation. It advocates for measures that uphold strong cyber resilience while enabling operational feasibility, sectoral innovation, and digital growth. With these refinements, the draft directions can serve as a critical foundation for a secure and trusted digital payment ecosystem in India.