Luthra and Luthra

LAW OFFICES INDIA

TMT NEWSLETTER

July – September 2025

Luthra and Luthra
LAW OFFICES INDIA

INSIDE

TELECOMMUNICATION

1. Ministry of Communications ("MoC") proposes rules for authorisations under the Telecommunications Act, 2023 ("Telecom Act")

The Telecom Act received presidential assent on December 24, 2023 marking a regulatory shift in the Indian telecommunication sector. The Telecom Act proposed an authorisation-based regime replacing the erstwhile license framework of the Indian Telegraph Act, 1885. While the key provision Section 3, which delineates the authorisation framework is yet to be enforced, there has been an ongoing consultation between Telecom Regulatory Authority of India **("TRAI")** and the MoC on the specific rules to regulate the various types of telecommunication services.

Telecommunication services have been broadly categorised into (a) main telecommunication services, (b) miscellaneous telecommunication services, (c) captive telecommunication service, and (d) broadcasting services.

So far, the Telecommunications (Authorisation for Provision of Main Telecommunication Services) Rules, 2025, ("**MTS Rules**"), Telecommunications (Authorisation for Captive Telecommunication Services) Rules, 2025 ("**Captive Rules**") and Telecommunications (Authorisation for Provision of Miscellaneous Telecommunication Services) Rules, 2025 ("**Miscellaneous Rules**") have been proposed on September 5, 10 and 9, 2025 respectively while the rules to regulate broadcasting services are still awaited.

These draft rules regulate the establishment, operation, maintenance and expansion of the aforesaid telecommunication services. The proposed rules prescribe the general terms and conditions such as manner of application, service area of authorisation, term and renewal of authorisation, eligibility criteria, disclosure and reporting obligations, penalties for violation of general terms and conditions and also include a format of authorisation for telecommunication services. Additionally, terms and conditions relating to key authorisations proposed under the above rules are discussed in detail below:

A. CAPTIVE RULES

These services are set up for the internal use of specific organisations, industries, or enterprises. The Captive Rules recognise captive telecommunication services to include - Captive Mobile Radio Trunking Services **("CMRTS")**, Captive Non-Public Networks **("CNPNs")**, Captive VSAT Services, and Captive General Services.

An application for captive authorisation is to be submitted via an online portal notified by the Central Government, accompanied by prescribed fees and supporting documentation. For certain categories, a "letter of intent" will precede the final grant, requiring fulfilment of conditions such as entry fees and performance guarantees. These authorisations will be valid for twenty years, with provision for renewal up to another twenty years.

The Captive Rules impose compliance obligations on authorised entities, requiring adherence to the provisions of the Telecom Act, TRAI regulations, and directions related to national security, lawful interception, and cyber security. Transfers or assignments of authorisation are prohibited without prior

approval. The Central Government also reserves the power to suspend or revoke an authorisation in the interest of national security, public interest, or for failure to meet statutory obligations.

Critically, the grant of authorisation for provision of captive services does not automatically confer spectrum rights, which remain subject to separate assignment and allocation processes.

B. MISCELLANEOUS RULES

The proposed framework recognises miscellaneous telecommunication services to include - public mobile radio trunking service **("PMRTS")**, enterprise communication service, machine to machine **("M2M")** service, PM-WANI, in-flight maritime connectivity **("IFMC")**, aeronautical data communication service and International SIM service.

While the general terms and conditions related to eligibility, application, term, renewal, compliance and conduct are akin to that of Captive Rules certain additional obligations are applicable on entities offering miscellaneous telecommunication services. For instance, (a) in case where renewal of authorisation is rejected, the provider of miscellaneous telecommunication services must also notify all its users of options available to them at least thirty-days prior to the termination of services, (b) an express undertaking from the authorised entity confirming compliance with applicable laws on data privacy and confidentiality of user information, (c) additional verification and KYC obligations for onboarding users and maintaining traceable records of such users.

C. MTS RULES

The proposed framework recognises main telecommunication services to include unified service, access service, internet service, and long-distance service, covering both the NSO and VNO operations for the aforesaid services.

While the general terms and conditions related to eligibility, application, term, renewal, compliance and conduct are akin to that of Miscellaneous Rules certain additional obligations are applicable on applicants/entities authorised for main telecommunication services such as (a) minimum net worth and paid-up equity requirement, (b) restrictions on cross holding between authorised entities providing services within the same service area, (c) deployment of mechanisms for providing emergency response services, (d) physical verification of premises of business users as part of their onboarding and more.

Additionally, the MTS Rules also comprehensively cover provision of telecommunication services via satellite and prescribe definite eligibility criteria, technical and operating conditions, security conditions and further prescribe rollout conditions for operationalising satellite-based telecommunication services within twelve months from the date of assignment.

These draft rules are currently under consideration of MoC after public consultation. Once finalised, these rules will further the process of replacing the legacy licensing regime with the proposed authorisation framework, streamlining market entry, enhancing regulatory clarity, and fostering investment and innovation in India's telecommunication sector.

2. MoC notifies amendment to lawful interception rules, 2025

The MoC has notified the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Amendment Rules, 2025 **("LIM Amendment")**, which came into force on September 12, 2025. Issued under the Telecom Act, these amendments change the definition of the term "Competent Authority" and provides clarity on the officials empowered to authorize lawful interception in case of inter-state inception of messages. "Competent Authority" is expanded to include the Union Home Secretary as the Competent Authority, in case of a request from the Secretary in-charge of the Home Department of the State Government to the Central Government for interception by that State Government beyond its territorial jurisdiction.

This inclusion clarifies the situation where a State Government seeks monitoring beyond its territorial jurisdiction which was missing earlier.

The LIM Amendment also modifies the appointment of nodal officers, provisioning one or more officers instead of the earlier fixed limit of two. This change provides agencies with greater flexibility in coordinating and executing lawful interception operations while ensuring compliance with the procedural safeguards established under the Telecom Act.

The LIM amendment clarifies the responsibilities of Competent Authority, ensuring a streamlined process for cross-jurisdictional requests. The amendment enhances transparency and accountability in operational protocols.

3. MoC proposes Telecommunications (Migration) Rules, 2025

On September 19, 2025, the MoC issued a notification proposing the draft Telecommunications (Migration) Rules, 2025 **("Migration Rules")** under the Telecom Act. These rules are designed to facilitate the transition of telecom operators from legacy licenses issued under the Indian Telegraph Act, 1885 and the Indian Wireless Telegraphy Act, 1933, to the authorisation-based framework established by the Telecom Act.

The proposed rules apply to various categories of licenses, including Access Service, Internet Service, NLD/ILD, GMPCS, VSAT, VNO, M2M, PM-WANI, IP-I, and MNP. License holders must apply for migration at least 12 months before the expiry of their current license (or within 90 days if less than 12 months remain when the rules take effect) by paying a non-refundable processing fee. Migration requests must cover all licenses held by the applicant, and the applicant must meet eligibility conditions prescribed for the relevant authorisation, except the minimum net worth requirement.

Approval for migration will depend on the clearance of all pending dues, including license fees, spectrum usage charges, penalties, undertaking for payment of dues from any pending litigations including any penalty and interest.

The Central Government shall also levy any differential entry fee between the fee already paid by the applicant and the extant fee applicable on the authorisation to which the licensee is migrating into. However, no refunds will be provided if the original entry fee is higher.

Once migration is approved, the existing license will be cancelled and deemed subsumed within the new authorisation without affecting past liabilities, obligations, or spectrum rights, which remain valid for their original tenure (in case of administratively assigned spectrum for up to five years). This initiative aims to streamline the regulatory framework and ensure a smooth transition for existing players to the new authorisation regime.

4. MoC proposes Telecommunications (User Identification) Rules, 2025

On September 19, 2025, the MoC issued a notification proposing the Telecommunications (User Identification) Rules, 2025 **("User Identification Rules")** under the Telecom Act. These draft rules provide for the mode and manner of user identification for telecommunication services notified by the Central Government under Section 3(7) of the Telecom Act.

The proposed rules mandate that all users of notified telecommunication services must be uniquely identified using government-approved identification methods before accessing such telecommunication services. This includes linking user identities to valid identification documents to ensure traceability and accountability.

The User Identification Rules propose an AADHAR based e-KYC for users of notified telecommunication services having a valid AADHAR as per the Aadhar (Authentication and Offline Verification) Regulations, 2021 and a digital KYC **("d-KYC")** for users with no AADHAR.

A d-KYC must be followed by a biometric identification of the user via biometric identity verification system **("BIVS")** via live photograph or any other biological attributes of an individual as may be specified. Every user biometrically identified shall be allotted a unique user-id for identification and subsequent revisions to the d-KYC as may be required. Lastly, any violation or non-compliance of these rules by an authorised entity, shall be subject to the provisions of the Telecommunications (Adjudication and Appeal) Rules, 2025.

5. DoT releases Draft National Telecom Policy 2025 ("NTP-25")

The DoT released the draft NTP-25 on July 24, 2025, outlining India's vision for its digital future. Building upon the National Digital Communications Policy 2018, NTP-25 aims to establish a resilient, secure, inclusive, and sustainable telecom ecosystem, keeping pace with emerging technologies such as 5G/6G, artificial intelligence, internet of things, quantum communications, satellite networks, and blockchain. NTP-25 is structured around six strategic missions: Universal and Meaningful Connectivity, Fostering Innovation, Promoting Domestic Manufacturing, Ensuring Secure and Trusted Networks, Enhancing Ease of Living and Doing Business, and Advancing Sustainable Development.

The NTP-25 proposes expanding network coverage through fiberisation, Bharat Net integration, satellite and non-terrestrial networks, and one million public Wi-Fi hotspots, ensuring connectivity in underserved areas. On the manufacturing front, NTP-25 promotes design-led domestic production, export growth, import substitution, and development of telecom manufacturing zones and research labs, enhancing self-reliance. The NTP-25 presents a transformative roadmap for India's telecom sector. By integrating digital inclusion, innovation, domestic manufacturing, cybersecurity, and sustainability, it is expected to accelerate

the deployment of advanced technologies like 5G/6G and satellite networks, enhance the quality of service, and expand coverage to rural and remote regions. The policy promotes investment and startup growth, thereby generating jobs and enhancing India's position in the global digital economy.

BROADCASTING

6. TRAI issues recommendations on reserve price for auction of FM Radio channels

TRAI on September 23, 2025 released its recommendations on the "Reserve Price for Auction of FM Radio Channels." Responding to a reference from the Ministry of Information and Broadcasting **("MIB")**, TRAI suggested reserve prices for Bilaspur (Chhattisgarh), Rourkela (Odisha), Rudrapur (Uttarakhand), and 18 towns in hilly regions of Himachal Pradesh, Uttarakhand, and Jammu & Kashmir.

TRAI has recommended delinking annual license fee from non-refundable one-time entry fee for all licensees to be calculated at 4 % of the adjusted gross revenue for the relevant financial year. It also endorsed the creation of a new "Category E" for hilly towns with populations below one lakh, with technical standards suited to their terrain. Alongside this, TRAI recommended measures such as allowing access to Prasar Bharati's tower and transmission infrastructure at concessional rates.

FINTECH

7. Reserve Bank of India ("RBI") issues Master Directions on Regulation of Payment Aggregators, 2025

The RBI on September 15, 2025 issued the Reserve Bank of India (Regulation of Payment Aggregators) Directions, 2025 **("PA Directions")**, establishing a consolidated framework to strengthen oversight of payment aggregators, enhance consumer protection, and curb fraud. The PA Directions incorporate feedback on an earlier draft released on April 16, 2024 and also consolidate the Regulation of Payment Aggregator – Cross Border (PA - Cross Border) released on October 31, 2023 by the RBI. These master directions consolidate all regulations related to payment aggregators and creates a consolidated regulatory framework covering domestic and cross border payment aggregators. The PA Directions apply to all banks and non-bank entities undertaking the business of a payment aggregator and also apply to all authorised dealer banks and scheduled commercial banks which engage with entities undertaking the business of a payment aggregator.

The PA Directions defines payment aggregator as an entity that facilitates aggregation of payments made by customers to the merchants through one or more payment channels through the merchant's interface (physical/virtual) for purchase of goods, services or investment products, and subsequently settles the collected funds to such merchants. The PA Directions categorises payment aggregators as payment aggregator – physical, payment aggregator – online and payment aggregator – cross border basis the nature of operations undertaken by them.

Under the PA Directions, payment aggregators are required to maintain a minimum net worth of ₹15 crore, rising to ₹25 crore within three years, undertake KYC for merchants prior to onboarding, establish baseline measures for consumer protection and preventing fraud including a board approved information security policy, compliance with data storage requirements akin to that of payment systems operators and annually

have their cyber security measures audited by CERT-In empanelled auditors. Further payment aggregators must also ensure continued compliance with the RBI Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators. Lastly, payment aggregators must also disclose comprehensive information regarding its merchant policies, privacy policy and other terms and conditions.

8. RBI issues Reserve Bank of India (Know Your Customer (KYC)) (2nd Amendment) Directions, 2025.

The RBI on August 14, 2025, issued the Reserve Bank of India (Know Your Customer (KYC)) (2nd Amendment) Directions, 2025, amending the 2016 master directions on KYC. The amendments include publication of FAQs on KYC on the RBI website, ensuring that no onboarding or KYC updation application - including those of persons with disabilities is rejected without recorded reasons, and expanding KYC requirements beyond only being applicable at the time of onboarding to also include KYCs at the time of occasional transactions of ₹50,000 or above and on international money transfers.

These directions also recognise aadhaar face authentication as valid authentication and require that liveness checks be inclusive of persons with special needs. The amendments have come into effect on August 14, 2025.

These measures align with the principles of digital inclusion as highlighted by the Supreme Court in Pragya Prasun v. Union of India *W.P. (Civil) 289 of 2024*, which emphasised that digital KYC and other essential digital services must be accessible to persons with disabilities, including acid attack survivors and those with facial disfigurements, ensuring compliance with the Rights of Persons with Disabilities Act, 2016.

9. RBI publishes report on responsible and ethical enablement of artificial intelligence in the financial sector

The RBI committee on framework for responsible and ethical enablement of artificial intelligence **("Committee")** has published its report **("Report")** vide notification dated August 13, 2025, delineating foundational principles **("7 sutras")** and recommendations for the inclusion of Artificial Intelligence **("AI")** in the financial sector.

The foundational principles are as follows:

a) Trust is the foundation,

b) People first,

c) Innovation over restraint,

d) Fairness and equity,

e) Accountability,

f) Understandable by design, and

g) Safety, resilience, and sustainability.

These principles are aimed at guiding the development, deployment, and governance of AI in the financial sector.

The Committee has also proposed a governance framework covering the following aspects:

a) **Measures for enabling innovation:** Creation of an AI innovation sandbox for the financial sector; establishment of a robust data infrastructure; incentives and funding for smaller entities and development of sector specific indigenous AI models to foster innovation and leverage AI.
b) **Affirmative policy framework:** Creating an AI standing committee; graded liability framework for entities using AI tools and enhanced disclosure requirements. The Committee believes that such disclosures will help build public trust and assure stakeholders by providing transparency into how AI is being governed and whether their concerns are being acknowledged and addressed.
c) **Governance structure:** Ground up governance for AI based tools within regulated entities **("REs")**, and fintechs via measures such as a board approved AI policy; data lifecycle governance; model documentation; validation, and ongoing monitoring; mechanisms to detect and address model drift and degradation followed by a robust product approval process.
d) **Consumer protection framework:** Measures for enhancing stakeholder accountability and consumer protection including adoption of AI-specific cybersecurity measures such as dynamic threat detection; red teaming; business continuity plans and incident reporting obligations; followed by a robust grievance redressal framework based on transparency, fairness and accessibility.
e) **Risk mitigation measures:** Apart from the incident specific measures discussed in the paragraph above, the Report also recommends comprehensive sector risk mitigation measures including maintaining a comprehensive depository of models; periodic multi-staged audits and an SRO-driven AI toolkit where the REs could benchmark their compliance with key responsible AI principles such as fairness, transparency, accountability, and robustness.

The RBI via this report has proposed an 'innovate with guardrails' approach towards AI in the financial sector. The Report balances incentives for using AI-aided technologies while simultaneously establishing governance and compliance baselines.

ONLINE GAMING

10. Ministry of Electronics and Information Technology ("MeitY") enacts the Promotion and Regulation of Online Gaming Act, 2025 and releases Draft Online Gaming Rules, 2025 for consultation

The Parliament enacted the Promotion and Regulation of Online Gaming Act **("PROGA")**, 2025, with presidential assent on August 22, 2025, establishing a uniform national framework that promotes e-sports and online social games while prohibiting online money games offered in India. PROGA defines three buckets of online games, e-sports, online social games, and online money games, and creates the Online Gaming Authority of India to classify games, register permissible titles, maintain a national registry, enforce compliance, and adjudicate suspensions or cancellations. Online money games, its advertisements and any assistance to online money games in relation to transfer of funds has been prohibited under PROGA. Fines up to ₹ 1 crore and imprisonment up to three years has been prescribed for contravention of the provisions of PROGA.

MeitY has also issued the draft Promotion and Regulation of Online Gaming Rules, 2025 under Section 19 of the PROGA. The draft rules set out procedures for classification and registration of permissible games (with up to five-year validity), disclosure of material changes, notice-and-hearing safeguards before adverse actions, time-bound decision cycles, penalty mechanisms, and coordination protocols with sector ministries, while enabling the Online Gaming Authority of India to function digitally-by-default for streamlined compliance and rapid blocking of illegal money games. Pending finalization, these Rules complement PROGA's establishment of a national registry for online games, advertising restrictions, fund-transfer prohibitions for online money games, and enforcement architecture. The draft rules are currently under consideration of MeitY after public consultation.

PROGA was challenged in September 2025, with respect to the complete ban on online money games before Delhi, Karnataka, and Madhya Pradesh High Courts. The Supreme Court allowed the Union's transfer petitions in Head Digital Works Private Limited & Anr. v. Union of India *Transfer Case (Civil) No(s). 133/2025* and directed that all writs challenging PROGA pending before different High Courts to be transferred to the Supreme Court; any similar petitions in other High Courts also stand transferred. Centralization removes the risk of conflicting High Court orders and ensures a single authoritative ruling on core issues raised by gaming companies, including legislative competence vis-à-vis Entry 34 (State List) of Constitution, the ban's impact on Article 19(1)(g) with respect to rights for skill-based games, Article 14 arbitrariness given the skill/chance distinction, and the allegation of legislative overruling on settled precedents where online games of skill have been provided protection.

PROGA provides legitimacy to e-sports and online social game operators who will gain a central licensing pathway and a clear compliance checklist that can unlock investment and distribution, whereas real-money gaming businesses face nationwide prohibition and heightened enforcement risk. Concurrently, the Supreme Court has centralized all constitutional challenges to the PROGA and will adjudicate the validity of the ban that eliminates the traditional skill-versus-chance distinction for money games, creating near-term legal uncertainty for online real money gaming models but leaving the statutory and rulemaking timelines under PROGA intact, unless stayed. Until the Supreme Court rules or grants interim relief, PROGA remains a valid law which shall be enforceable upon notification by the Central Government.

INFORMATION TECHNOLOGY AND DATA PROTECTION

11. Indian Computer Emergency Response Team ("CERT-In") releases elemental cybers defence controls for Micro, Small, and Medium Enterprises (MSME) Cybersecurity

CERT-In, under the MeitY, released Version 1.0 of the "15 Elemental Cyber Defence Controls" on September 1, 2025 to provide MSMEs with a minimum, practical baseline to mitigate risks to sensitive data, financial transactions, and operational continuity. The controls are designed to uplift cyber hygiene across MSMEs as they scale their digital operations amid rising threat activity.

The framework identifies 15 critical control areas covering asset management, network and email security, endpoint protection, secure configuration, patch management, incident management, logging and monitoring, data protection, risk management, access control, among others, and translates them into 45 actionable recommendations to help MSMEs benchmark their posture and prioritise remediation. These measures are intended to be implementable with modest resources while offering high risk-reduction value.

Implementation pathways include integrating the controls into existing policies, conducting baseline audits through CERT-In empanelled auditing organisations, and instituting periodic reviews. Practical steps highlighted include centralised asset inventories, secure network configurations, deployment of endpoint protection, timely patching, resilient data backups, multi-factor authentication, and workforce cybersecurity training. Together, these measures offer a pragmatic roadmap for MSMEs to strengthen defences and improve resilience.

12. CERT-In issues Technical Guidelines v2.0 on SBOM, QBOM/CBOM, AIBOM and HBOM to strengthen supply chain cybersecurity

On July 9, 2025, CERT-In released Version 2.0 of its Technical Guidelines covering Software Bill of Materials **("SBOM")**, Quantum and Cryptographic BOMs **("QBOM/CBOM")**, Artificial Intelligence BOM **("AIBOM")**, and Hardware BOM **("HBOM")**, establishing standardized frameworks to track, manage, and secure software and hardware components across their lifecycles. A BOM (Bill of Materials) is a structured inventory of all components, sub-components, and associated metadata that make up a product or system. In cybersecurity and supply-chain contexts, BOMs provide transparency into what's inside the software and hardware so organizations can manage vulnerabilities, compliance, and supplier risk.

For SBOM, the Guidelines define minimum elements that should be captured for each component (e.g., name, version, supplier, license, dependencies, vulnerabilities, patch status, and integrity data), and emphasize machine-readable, automatable practices so SBOMs can be generated and consumed at scale. They recommend the use of standard formats like, SPDX and CycloneDX, and describe how automation integrates SBOMs into development, vulnerability management, and audit workflows.

Beyond SBOM, the suite covers CBOM and QBOM to inventory cryptographic assets and document quantum-readiness, AIBOM to make AI systems transparent and governable through model, data, and dependency inventories, and HBOM to ensure traceability and integrity of physical components across the hardware supply chain. Together, these BOMs provide full-stack visibility and a common language for managing risk across software, cryptography, AI, and hardware layers.

13. CERT-In Issues Comprehensive Cyber Security Audit Guidelines for Indian Enterprises

On July 25, 2025, the CERT-In, exercising its statutory authority under Section 70B of the Information Technology Act, 2000 **("IT Act")** issued Version 1.0 of the Comprehensive Cyber Security Audit Policy Guidelines to standardise how Indian organisations plan, conduct, and close cybersecurity audits. These guidelines are intended for CERT-In empanelled auditors and organizations in both the public and private sectors that are required to or are seeking to evaluate their cyber security posture, identify vulnerabilities, assess risks, and ensure compliance with applicable regulatory standards and industry best practices. The Guidelines set a minimum cadence of at least one comprehensive audit per year with sectoral regulators free to require more and emphasise risk-based scoping that covers the organisation's ICT estate end-to-end.

For auditees, these Guidelines assign board-level oversight of programs and remedial actions, makes clear that maintaining a robust security posture is the organisation's responsibility (not the auditor's), and requires prompt remediation and follow-up audits after findings are closed. It also directs auditees to embed

secure-by-design practices, maintain asset inventories and patching, enforce least-privilege and multi factor authentications, and avoid using non-genuine or outdated software and protocols. For auditing organisations, the Guidelines define independence and competency requirements, mandate the use of declared personnel only, and impose stringent rules for handling audit data (including storage in India, encryption in use, secure disposal with certification, and report-signing workflows). Auditors must share audit metadata with CERT-In within five days of completion, enabling national-level visibility and quality benchmarking. Methodologically, audits must go beyond checklist testing by applying comprehensive standards and frameworks.

Practically, the Guidelines shift audits from a one-off compliance exercise to an operational risk program. Quality assurance is backed by CERT-In oversight and a graded "deter and punish" framework for substandard work or violations, ranging from warnings to suspension, de-empanelment, and penal/legal action. Taken together, these measures are intended to strengthen enterprise security posture, improve audit consistency and evidence quality, and enhance national cyber resilience—an intent the Guidelines state explicitly and that contemporary reporting also recognises as a pivot toward continuous threat preparedness.

14. X.509 Certificate Policy for India Public Key Infrastructure ("PKI")

The Controller of Certifying Authorities **("CCA")**, Government of India, has released Version 1.10 of the X.509 Certificate Policy **(CP)** for India PKI. The updated policy aims to enhance interoperability among subscribers (of digital certificates) and relying parties (that rely on the digital certificates of subscribers) to secure e-commerce and e-governance in India. India PKI, governed under the IT Act, 2000, operates on a hierarchical model with the Root Certifying Authority of India **(RCAI)** at its core. The revised CP is aligned with global best practices, consistent with the IETF PKIX RFC 3647 framework, and applies to all components of India PKI, including RCAI, CAs, Registration Authorities **(RAs)**, and repositories.

15. Certifying Authorities (CAs) Licensing Guidelines issued by CCA

The CCA regulates Digital Signature Certificates **("DSCs")** in India under the IT Act. To strengthen trust in digital transactions and support e-governance, the CCA has released updated licensing guidelines for CAs issuing DSCs under India PKI.

The updated framework emphasises financial stability, technical readiness, and compliance:

a) **Eligibility & Ownership:** Companies must have a minimum paid-up capital of ₹5 crore and a net worth of ₹50 crore, with foreign equity capped at 49%.

b) **Application Process:** Applicants must submit a business plan, demonstrate technical infrastructure readiness, and provide a Certification Practice Statement.

c) **Audit & Approval:** CCA-empanelled auditors will assess technical, physical, and procedural infrastructure, granting "in-principle" approval upon successful evaluation.

d) **Financial Requirements:** A non-refundable application fee of ₹25,000 (fresh licence) or ₹5,000 (renewal), plus a performance bond/bank guarantee of ₹50 lakh, ensures financial credibility.

Upon successful evaluation and audit, applicants will be issued a Public Key Certificate and Paper Licence, formalising their status as licensed Certifying Authorities. The details of approved CAs will be published on the CCA website to ensure transparency and public trust.

16. India Strengthens Digital Trust with Updated Audit Criteria for Certifying Authorities

On September 9, 2025, the CCA, MeitY, released the latest Audit Criteria for CAs (Version 1.7), aimed at enhancing the security, compliance, and operational integrity of digital signature services in India. Under the IT Act, CAs are licensed by the CCA to issue DSCs, which enable secure e-governance, e-commerce, and electronic authentication. Key highlights of the updated Audit Criteria include:

a) **Mandatory Annual Audit:** All CAs must undergo an annual audit by empanelled auditors to ensure compliance with security and operational standards.
b) **Half-Yearly and Quarterly Audits:** Half-yearly audits focus on security policies and operational planning, while quarterly audits cover repository management.
c) **eKYC Compliance:** Monthly auditing of 5% of eKYC-based certificate issuance samples is mandated.

The enhanced audit framework is expected to boost transparency, accountability, and confidence in India's digital signature ecosystem.

EMERGING TECHNOLOGIES

17. Ministry of Civil Aviation ("MOCA") notifies Draft Civil Drone (Promotion and Regulation) Bill, 2025

MOCA has released the Draft Civil Drone (Promotion and Regulation) Bill, 2025, **("Drone Bill")** that aims to establish a comprehensive legal framework for the operation, regulation, and promotion of unmanned aircraft systems in India and shifts from the regime of the Drone Rules, 2021 framed under the Aircraft Act, 1934. It is also pertinent to mention that the Aircraft Act, 1934 has itself been repealed by the Bharatiya Vayuyan Adhiniyam, 2024.

The Drone Bill shifts the regulatory landscape from a rules-based legislation to a standalone legislation with explicit carve outs for unmanned aircraft systems above 500 kg, lays down detailed provisions regarding registration, certification, operation, and maintenance of drones among other requirements. The Directorate General of Civil Aviation has been retained as a designated regulatory authority, empowered to enforce compliance through inspections, audits, and investigations. The Drone Bill introduces penalties for non-compliance, including fines up to ₹1 lakh and imprisonment of up to three years for unauthorised operations or failure to adhere to safety protocols.

The Drone Bill, is set to transform the Indian drone sector. A clear regulatory framework will make drones more accessible to businesses and consumers, encouraging their use in agriculture, logistics, surveillance, infrastructure inspection, and other sectors. By mandating registration, certification, and operational standards, the Drone Bill aims to enhance safety and accountability. Government has also been empowered with economic regulation of Unmanned Aircraft Systems Sector including determination of fare, fee, tariff and charge giving more clarity on the economic front of the drone sector.

Luthra and Luthra
LAW OFFICES INDIA

This newsletter is only for general informational purposes, and nothing in this edition of the newsletter could possibly constitute legal advice (which can only be given after being formally engaged and familiarizing ourselves with all the relevant facts). However, should you have any queries, require any assistance, or clarifications with regard to anything contained in this newsletter, please feel free to contact Vikash Kukreti, at the below mentioned coordinates.

KEY CONTACTS

VIKASH KUKRETI
Partner
Email - vkukreti@luthra.com

GAURAV TIWARI
Senior Associate
Email - Gtiwari@luthra.com

AKASH TAHENGURIA
Associate
Email - atahenguria@luthra.com

OFFICES

NEW DELHI
1st and 9th Floors, Ashoka Estate,
24 Barakhamba Road, New Delhi - 110 001
T: +91 11 4121 5100 F: +91 11 2372 3909
E: delhi@luthra.com

MUMBAI
20th Floor, Indiabulls Finance Center,
Tower 2 Unit A2, Elphinstone Road,
Senapati Bapat Marg, Mumbai - 400 013
T: +91 22 4354 7000
F: +91 22 6630 3700
E: mumbai@luthra.com

BENGALURU
3rd Floor, Onyx Centre, No. 5, Museum Road,
Bengaluru - 560 001
T: +91 80 4112 2800 / +91 80 4165 9245
F: +91 80 4112 2332
E: bengaluru@luthra.com

HYDERABAD
Serene Towers,
House No. 8-2-623/A,
Road No. 10, Banjara Hills,
Hyderabad, Telangana - 500034
T: +91 40 7969 6162
E: hyderabad@luthra.com

CHENNAI
Prestige Palladium Bayan,
8th Floor, Greams Road, Nungambakkam Division,
Egmore, Chennai - 600 006,
Tamil Nadu
T: +91 95604 88155
E: chennai@luthra.com