# UPDATES

## New Cybersecurity Directions Issued

Juris Corp
advocates & solicitors

Under Section 70B(6) of the Information Technology Act, 2000 (**"Act"**), the Computer Emergency Response Team (**"CERT-In"**)[1] issued **"Directions"** on 28th April 2022 relating to information security practices, procedure, prevention, response and reporting of cyber security incidents[2] (**"CSI"**) for safe & trusted internet[3] to augment and strengthen the cyber security in India.

The Directions aim to lay-down the mechanism for collection of primary information to coordinate response and emergency measures for CSI, to seamlessly assist analysis, investigation, and coordination. The objective of the Directions is to secure information in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence using computer resource or for handling any CSI. The Directions will come into effect from the 60th day of its issuance and failure to furnish the information or non-compliance[4] may lead to punishment with imprisonment up to one year or with fine up to INR 1 lakh or with both.

| Relevant Party | Directions Issued |
|---|---|
| **Service providers, intermediaries[5], data centres, body corporate and government organisations** | • Connect to the Network Time Protocol (**"NTP"**) Server of National Informatics Centre (**"NIC"**) or National Physical Laboratory (**"NPL"**) or with NTP servers traceable to these NTP servers, for synchronisation of all ICT systems clocks to mandatorily report to CERT-In any CSI (from the ones listed in Annexure I to the Directions).<br>• Designate a Point of Contact to interface with CERT-In and send CSI in format specified in Annexure II to the Directions. CERT-In can send order/direction with a format and timeframe to act and provide information to CERT-In to mitigate CSI/risks and enhance CSI awareness. |

[1] CERT-In is the national agency for incident response in India within Ministry of Electronics and Information Technology.
[2] Under Rule 2(h) of the IT (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**CERT-In Rules**") means "*any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation.*"
[3] Link: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[4] Under section 70B(7) of the IT Act.
[5] Under Section 2(1)(w) of the IT Act means "*any person who on behalf of another person receives, stores, or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places, and cyber cafes.*"

| Relevant Party | Directions Issued |
|---|---|
| | • Mandatorily enable logs of all ICT systems and maintain them for 180 days in India so that any CSI can be reported to CERT-In. |
| **Data Centres, Virtual Private Server providers, Cloud Service providers and Virtual Private Network Service providers** | • Register the following information accurately for 5 years (*or longer as mandated under law after any cancellation or withdrawal of the registration*):<br>✓ validated names of subscribers/customers hiring the services;<br>✓ period of hire including dates;<br>✓ IPs allotted to / being used by the members;<br>✓ e-mail address, IP address and time stamp used at the time of registration / on-boarding;<br>✓ purpose for hiring services; and<br>✓ validated address, contact numbers and ownership pattern of the subscribers / customers hiring services. |
| **The virtual asset service providers, virtual asset exchange providers and custodian wallet providers** | • Mandatorily maintain all the information obtained as part of Know Your Customer (**"KYC"**) as per Annexure III to the Directions as well as records of financial transactions for 5 years to ensure cyber security in payments and financial markets for citizens, while protecting their data, fundamental rights and economic freedom in view of the growth of virtual assets.<br>• Accurate information for individual transactions be maintained so that they can be reconstructed with details: identity of parties, IP addresses, timestamps and time zones, transaction ID, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred.<br>• For KYC, the Reserve Bank of India Directions 2016 / Securities and Exchange Board of India circular dated 24th April 2020 / Department of Telecom notice 21st September 2021 mandated procedures as amended from time to time may be referred to as per Annexure III. |

## Our Comments

The Directions are applicable to service providers in telecom, network, cloud, internet, web hosting, wallets, crypto exchanges, intermediaries in social media platforms, search engines, e-commerce platforms, body corporates, data centres and government organisations. The key requirements are very basic in nature. The CERT-In Rules had prescribed reasonable timeframe to report CSI, which has now been fixed at 6 hours and such stringent timeline would require the applicable parties to engage trained personnel who are prompt in meeting compliance requirements. The data localisation requirement applies to even to cloud based or application layer service providers even if they do not have a physical presence in India. The KYC function was limited to banks, insurance, and securities and has now, with Directions, is applicable to virtual asset service providers, virtual asset exchange providers and custodian wallet providers as defined by Ministry of Finance; however, they have not yet provided guidance on these terms. As an attempt to be more inclusive or futuristic, while simultaneously going beyond the tenets of the CERT-In Rules, the list of CSIs to be reported has been widened to include attacks or incident affecting digital payment systems, unauthorised access to social media accounts, affecting cloud computing systems/servers/software/applications, or related to big data, block chain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D Printing, additive manufacturing, drones and related to artificial intelligence and machine learning.

# Contact us:


**MUMBAI OFFICES**

302, Century Bhavan, 3rd Floor,
Dr Annie Besant Road, Worli,
**Mumbai** - 400 030, India
Tel: +91 22 6720 5555 / +91 22 4057 5555
Fax: +91 22 2421 2547

**Dispute Resolution Office**

148, Jolly Maker Chamber II, 14th Floor,
Nariman Point, **Mumbai** - 400 021, India
Tel.: +91 22 4920 5555
Fax: +91 22 2204 3579

**NEW DELHI OFFICE**

502, 504 & 506, 5th Floor, Antriksh Bhawan,
Kasturba Gandhi Marg,
**New Delhi** - 110 001, India
Tel: +91 11 4175 1889
Fax: +91 11 4014 4122

**BENGALURU OFFICE**

Kheny Chambers, Upper Ground Floor,
4/2 Cunningham Road, **Bengaluru** - 560 052, India
Tel: +91 80 4669 8200
Fax: +91 80 2226 6990

Follow us -

Visit us at: http://www.jclex.com/