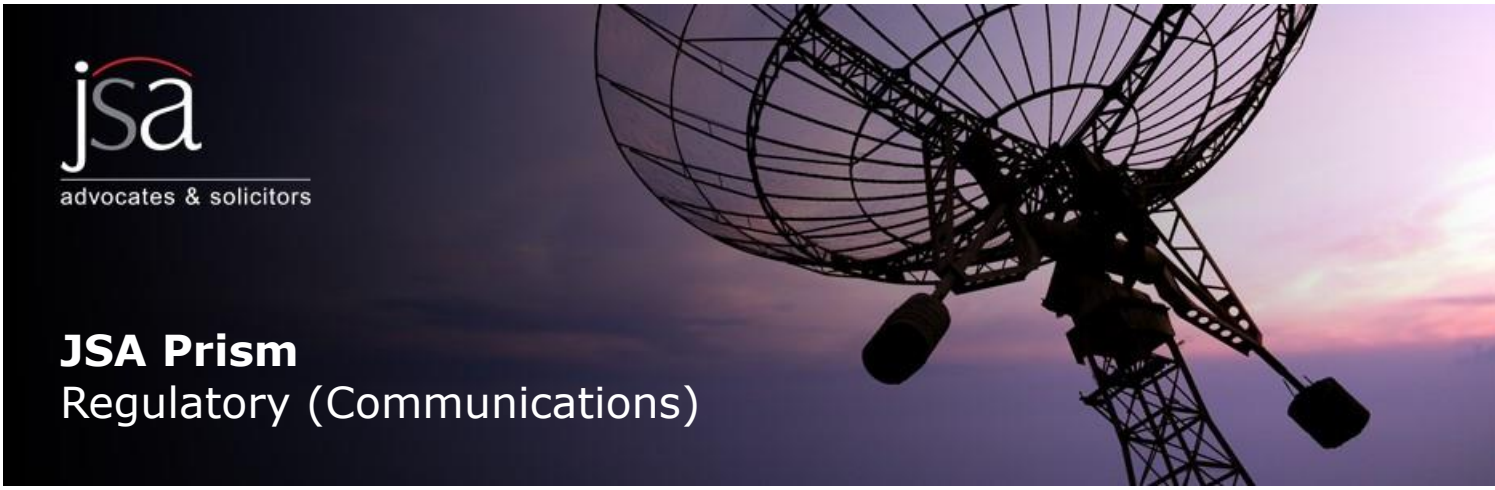

May 2022

FAQs on Cyber Security Directions, 2022

The Indian computer emergency response team ("**CERT-In**") has issued the frequently asked questions ("**FAQs**") dated May 18, 2022, in response to the various queries received from the stakeholders in relation to the cyber-security, breach reporting, and record maintenance requirements introduced vide its new Cyber Security Directions dated April 28, 2022 ("**2022 Directions**"). It may be noted that the FAQs are not to be considered as a legal document and that they do not replace, amend or alter any part of the Information Technology Act, 2000 ("**IT Act**") and/or the Information Technology (CERT-In and manner of performing functions and duties) Rules, 2013 ("**CERT-In Rules**").

The primary clarifications provided in the FAQs are as below:

Applicability: The obligation to report cyber security incidents applies to any entity which notices the cyber security incident, and the obligation is neither transferrable nor indemnified or be dispensed with. The FAQs also specifically state that such obligation to report cyber incidents extends to any entity whatsoever, in the matter of cyber incidents and cyber security incidents including Indian companies and foreign firms that serve Indian customers.

Incidents: The cyber incidents as well as cyber security issue as mentioned in the incidents must be reported to CERT-In. The FAQs also state that it is imperative to report cyber security incidents which are not mentioned in annexures of the CERT-In Rules or in the 2022 Directions.

Confidentiality: Reporting of cyber security incidents to CERT-In is enshrined in Section 70B of the IT Act read with the CERT-In Rules and hence, it is statutory in nature and overrides any confidentiality obligation that an entity has with other parties or its clients.

Timeline: In the event all the information as per the CERT-In incident reporting form is not available with an entity, the entity may provide information to the extent available at the time of reporting. Any additional information may be reported later within reasonable time to CERT-In.

Network Time Protocol Servers: CERT-In has clarified that Information and Communications Technology ("**ICT**") system clocks can be synchronised by configuring Network Time Protocol ("**NTP**") servers of the National Informatics Centre ("**NIC**") or National Physical Laboratory ("**NPL**") as a time source in the enterprise NTP Server (or on the device being used as NTP Server/s for the enterprise). Additionally, it has been clarified that the requirement of synchronising time is stipulated to ensure that only standard time facilities are used across all entities. Entities are permitted to use accurate and standard time source other than NPL and NIC as long as the accuracy of time is maintained by ensuring that the time source that is used conforms to the time provided by NTP Servers of NPL and NIC. The FAQs also clarify that (i) there is no need to mandatorily set their ICT systems clocks in Indian Standard Time (IST); and that (ii) cloud ICT infrastructures that span multiple geographies may setup their own NTP servers, as the 2022 Directions only require that the uniform time synchronisation across all ICT systems irrespective of time zone.

Further, customers in cloud environments have the option to either use native time services offered by the cloud to synchronize their clock or set up their own NTP server within their cloud environment. However, it is to be ensured that time source other than NIC/NPL, if used, shall not deviate from NPL and NIC.

If the service providers have ICT system across different geographies, then accurate and standard time source other than NPL and NIC is to be used while ensuring that their time source does not deviate from NPL and NIC.

ICT Systems Logs: The logs may be stored outside India also as long as the obligation to produce logs to CERT-In is adhered to by the entities in a reasonable time. An officer of CERT-In may seek the logs at any time. Any service provider offering services to the users in the country needs to enable and maintain logs and records of financial transactions in Indian jurisdiction.

Maintaining Information: FAQs have clarified that basic information of the customers/subscribers, which may consist of an individual, partnership, association, company etc., with brief particulars about their key management is to be maintained. No further clarifications or explanations in this regard has been provided.

Reporting: If reporting remains undetected for a long time, an analysis of the reported incident will be undertaken to detect gaps in security practices which will be analysed to mitigate the incidents in a timely manner. The details regarding methods and formats of reporting cyber security incidents is published on the CERT-In website. The service providers, intermediaries, data centres and body corporate offering services to the users in India are required to a Point of Contact to liaise with CERT-In.

Implications of Non-Compliance: The penalties prescribed under section 70B of the IT Act which includes imprisonment for a term that may extend to one year or fine up to INR one lakh or both will be applicable for non-compliance of the 2022 Directions.

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi

