KNOWLEDGE BANK™

Always stay curious

MCO LEGALS

12th July, 2022

CYBER LAW: ISSUE 9

NEW CERT-IN GUIDELINES 2022 - A WAY AHEAD TO A STRONG CYBER SECURITY MECHANISM IN INDIA

Introduction

On 28th April 2022, the Indian Computer Emergency Response Team (hereinafter referred to as CERT-In) issued directions under section 70B (6) of the Information Technology Act, 2000 (hereinafter referred to as IT Act, 2000) relating to information security practices, procedures, prevention, response, and reporting of cyber incidents for Safe & Trusted internet. These guidelines shall become effective after 60 days from the date of its notification. CERT-In is the nodal agency established under section 70B of the IT Act, 2000 for performing various functions in the area of cyber security. It is working since January 2004. Its major functioning revolves around the collection, analysis, and dissemination of information on cyber security incidents.

Major Directions

Following are the few significant guidelines issued under the CERT-IN Directions, 2022 –

- Connecting to the Network Time Protocol (NTP) server – As per the CERT-in Directions, all the service providers, intermediaries, data centres, body corporate and government organizations shall connect to the Network Time Protocol (NTP) Server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronization of all their ICT (Information and Communication Technology) systems clocks. It is also an additional requirement for the entities having ICT infrastructure which spans multiple geographies to use accurate and standard time sources other than NPL and NIC, and it is to be ensured that their time source shall not deviate from NPL and NIC.
- Reporting of Cyber Incidents – It is mandatory for all the service providers, intermediaries, data centres, body corporates, and government organizations to report any cyber incident within six hours of being notified that such cyber incident has happened or on becoming aware of such incident themselves. All the details regarding methods and format of reporting cyber security incidents are published on the official website of CERT-in. Few of the cyber security incidents to be reported mandatorily, as mentioned in Annexure I of the CERT-In Directions are - Targeted scanning/probing of critical networks/system, Compromise of critical systems/information, Compromise of critical systems/information, Data Breach, Data Leak, Fake mobile apps, Malicious code attacks such as spreading of virus/worm/Trojan/Bots/ Spyware/Ransomware/Cryptominers,Unauthorised access to social media accounts etc.
- Providing assistance to CERT-In in case of a cyber-security incident – It is mandatory for all the service providers/intermediary/data centre/body corporate to take action or provide information or any such assistance to CERT-In, for the purpose of cyber incident response, protective and preventive actions related to cyber incidents. The support provided by them may contribute toward cyber security mitigation actions and enhanced cyber security situational awareness. The information or assistance shall be provided only on the direction or order issued by the CERT-In. The order/direction so issued may contain the format of the information that is required, a specified timeframe in which it is required, which should be adhered to and compliance provided to CERT-In. In case the service provider/intermediary/ data centre/body corporate fails to adhere to such order/direction, it will be treated as non-compliance on their part.
- Designated Point of Contact – There shall be a designated Point of Contact appointed by the service providers, intermediaries, data centres, body corporate and Government organisations to interface with CERT-In. It is also required on part of these entities to send the information of the Point of contact in the desired format by the CERT-In. All communications for compliance shall be sent to the said Point-.

Amit Meharia

Managing Partner, MCO Legals
LLB (Hons) King's College
London, Solicitor
(Supreme Court of England & Wales)

amit.m@mcolegals.co.in

Expertise:

Corporate Due Diligence &
Corporate/Commercial Arbitration

Bhavna Sharma

Research Partner

B.Sc., LLM,
Jamia Millia Islamia

of Contact.

- ICT Systems Logs – CERT-IN directions have imposed a mandatory duty of all the service providers, intermediaries, data centres, body corporate and Government organisations to enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. All this information should be provided to CERT-In along with reporting of any incident or when ordered/directed by CERT-In.
- Registration and Maintenance of certain information – The CERT-In directions demand that all the Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register certain information such as validated names of subscribers/customers hiring services, period of hire, IPs allotted to or being used by the members, the purpose of hiring service, email addresses and IP address and time stamp used at the time of registration/on-boarding, validated address and contact number, and ownership pattern of the subscribers/ customer hiring services and maintain the same for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration.
- Preservation of KYC and financial information – The Directions also require virtual asset service providers, virtual asset exchange providers and custodian wallet providers to compulsorily maintain all information obtained under Know Your Customer (KYC) and records of financial transactions for a period of five years so as to ensure cyber security in the area of payments and financial markets for citizens while protecting their data, fundamental rights and economic freedom in view of the growth of virtual assets.

Conclusion

It is a welcoming step on part of the government of India to come up with updated CERT-In directions, however, there lay some ambiguities in the directions which resulted in doubting the applicability and implementation of the directions in practical. A few of them are – the term 'ICT system' is not defined in the directions. This might lead to collecting more information than required and giving the government access to such a high amount of data. The list of cyber security incidences which must be reported is narrow and there are many other incidents which must be reported that are not mentioned in the list. Also, the terms like 'data breach', 'data leak', and 'fake mobile apps' are not defined and hence can be interpreted differently and the scope can be broadened or narrowed which might result in arbitrariness. The directions required that the data must be maintained for a period of 180 days by the entities which is an excessive timeline. The reason behind such direction is not conveyed by the government. This might lead to exposing the data making it prone to leaks and cyberattacks as for the protection and right preservation of the data, the entities have to create additional infrastructure for retaining and storing such data. The data localization as demanded in the directions may also affect the easy flow of data across nations and act as a barrier for foreign services providers to enter in the Indian market. Another issue that prevails with the directions is that the Virtual Private Network (VPN) services providers have to maintain the information provided by the customers for 5 years even after they have cancelled their registration. This might impact the basic essence of VPN services i.e. "encryption" and in turn hit the digital privacy of the user.

Having said that, it can't be denied that the Govt. of India has taken timely active precautionary measures to prevent the incidents of cyber-attacks which was the need of the hour. The directions are made strict and tight bound looking at the number of cyber security incidents (48, 285) that occurred against the government authorities in 2021. It raised a serious concern about the cyber security of the nation which must be protected at the first sight as it was creating a culture of cyber-warfare among the nations. Non-compliance to these direction attracts criminal liabilities. The purpose of these directions itself was to augment and strengthen cyber security in India. Hence realising the need of controlling the increased rate of cyber-attacks, the government coming up with such close-fitted and impervious directions is justified in prioritizing the interest of the nation.