Technology Law Analysis

May 06, 2022

CYBER SECURITY: INDIA REVAMPS RULES ON MANDATORY INCIDENT REPORTING & ALLIED COMPLIANCES

- The Indian Computer Emergency Response Team ("**CERT-In**") has issued a direction to expand the scope of mandatorily reportable cyber security incidents.
- Breach reporting within 6 hours of receiving knowledge of such incident. Failure to report could result in imprisonment and/or fine.
- Additional compliance requirements including data localization, conducting KYC of clients, data storage, appointing point of contact for cybersecurity incidents, etc.
- The Direction will be enforced from June 28, 2022.
- Direction is applicable to service providers, intermediaries, data centres, body corporate and Government organisations. Some specific compliances are applicable to virtual private server (VPS) providers, cloud service providers and virtual private network service (VPN Service) providers and entities in the virtual assets ecosystem.

BACKGROUND

On 28 April 2022, CERT-In issued a direction relating to "information security practices, procedures, prevention, response, and reporting of cyber incidents for Safe & Trusted Internet" (**"Direction"**).[1] The Direction has been issued under Section 70B(6) of the Information Technology Act, 2000 ("**IT Act**"). A summary of the provisions of the Direction is provided in Annexure A below.

The Direction has significantly widened the types of cyber security incidents that must be mandatorily reported to CERT-In. The Direction also imposes a strict timeline of 6 hours after notice of the incident for reporting such incidents to CERT-In and introduces several compliance requirements for different types of entities, including intermediaries, service providers, data centres, virtual private network service providers, cloud service providers, as also other entities such as "virtual asset service providers" and "virtual asset exchange providers". The key compliances are discussed below.

Considering the wide wording of the Direction, it is likely to be applicable to almost each and every type of business operating within India. The Direction will be effective from June 28, 2022 and may require businesses to rethink and overhaul their cyber security practices and processes.

NDA is organising a webinar to further discuss the key aspects of the Direction and their impact on businesses in India on Wednesday, May 11, 2022. You may register for the webinar at this link.

We have discussed some key aspects of the Direction below.

EARLIER REQUIREMENTS

*Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**CERT-In Rules**")[2] issued under Section 70B(5) of the IT Act.*

The CERT-In Rules required mandatory reporting of identified cyber security incidents (See Annexure B), while other cyber security incidents could be reported voluntarily. By way of the Direction, CERT-In has in a way amended several provisions of the CERT-In Rules.

KEY PROVISIONS OF THE DIRECTION AND CONCERNS

1. Reporting
   - *Mandatory reporting requirements:* The list of cyber security incidents which are mandatorily reportable has been expanded (see Annexure B). Now, essentially any and all types of cyber breaches are mandatorily reportable, irrespective of the severity of the incident.
   - *Who should report*: Service providers, intermediaries, data centres, body corporates and Government organisations (hereafter "**Identified Entities**")
   - *Timeline for reporting*: Incidents have to be reported by the Identified Entity within 6 hours of noticing such incident or being brought to notice about such incidents. The details regarding methods and formats of

Research Papers

Clinical Trials and Biomedical Research in India
April 22, 2025

Structuring Platform Investments in India For Foreign Investors
March 31, 2025

India's Oil & Gas Sector– at a Glance
March 27, 2025

Research Articles

2025 Watchlist: Life Sciences Sector India
April 04, 2025

Re-Evaluating Press Note 3 Of 2020: Should India's Land Borders Still Define Foreign Investment Boundaries?
February 04, 2025

INDIA 2025: The Emerging Powerhouse for Private Equity and M&A Deals
January 15, 2025

Audio

CCI's Deal Value Test
February 22, 2025

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

Vyapak Desai speaking on the danger of deepfakes | Legally Speaking with Tarun Nangia |

reporting cyber security incidents is also published on the website of CERT-In.[3] The information that CERT-In seeks in its prescribed format, in all likelihood may not be available within timeline of 6 hours. Such a timeline could be sufficient only for providing unconfirmed information, and raw data dumps. CERT-In should therefore allow entities to update the information they provide once they have more concrete information about an incident. It may be noted that the Joint Parliamentary Committee's report on Data Protection Bill, 2019 also recommends a 72-hour window for reporting data breaches.[4]

The legislature could consider bringing in criticality thresholds for mandatory reporting of cyber security breaches. Rule 11(1)(c) of the CERT-In Rules provide the list of priorities in which CERT-In allots resources for providing assistance in cyber security incidents. Such a threshold-based approach could be adopted for reporting as well so that minor or one-off incidents are not required to be escalated to CERT-In.

In addition to the change in the reporting requirements, the Direction introduces certain compliances that the relevant entities must adhere to. Some of the key compliances are discussed below:

2. *Specific orders/directions by CERT-In*: When CERT-In issues any order/directions to an Identified Entity, such entity must mandatorily take action or provide information or any assistance to CERT-In, as directed. This is an overarching provision as it allows CERT-In to seek information not only in case of an incident but also to take "protective and preventive actions". Further, there is no clarity on the sort of information that could be sought, and as per the Direction, Identified Entities are required to provide whatever information is sought. Moreover, if there is non-compliance with such order/direction, it will be treated as non-compliance with the Direction, which will have consequences, as discussed below.

   The scope of the orders / directions should be limited to providing such information and / or assistance as is *strictly* required for protective and preventive actions, so that entities are not required to provide information which may not relate to the incident.

3. *Synchronisation with NTP Server* – Identified Entities are required to 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 their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies are permitted to use accurate and standard time source other than NPL and NIC, however, they must ensure that their time source does not deviate from NPL and NIC. This provision could require several entities to undertake infrastructure changes for ensuring that there is no deviation from the NIC/NPL's NTP server. The purpose of such synchronization appears to be to ease analysis of cyber security incidents affecting multiple systems at the same time. Hence, we believe that even if there is slight deviation between NPL and NIC and other sources, so long as entities can maintain an authentic record of such difference, the same should satisfy the requirement.

4. *Maintenance and disclosure of logs*: Identified Entities must mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and these logs have to be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.

   This requirement does not specify the kinds of logs that must be maintained and provided to CERT-In. For e.g., would an entity providing e-mail services or search engine services to users be required to not only track but share all activities of the user, including their personal information? The current CERT-In Rules provides that CERT-In may collect and analyse information relating to cyber security incidents, however, the language in the Direction enables CERT-In to collect information even without occurrence of an incident. This can have a significant impact on privacy of users, and accordingly, this requirement would need to be evaluated against three-fold test of legality, legitimacy of aims, and proportionality prescribed in *K.S. Puttaswamy v. Union of India*.[5] It would be advisable to specify the kind of logs that should be maintained, and that may be required to be provided to CERT-In, such as specifying that only cybersecurity-related logs (such as those pertaining to firewalls, access to routers, administrative access to systems, etc.) would be covered under this provision.

5. *Recordal of data by certain entities*: Data centres, virtual private server (VPS) providers, cloud service providers and virtual private network service (VPN Service) providers are required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:

   - Validated names of subscribers/customers hiring the services
   - Period of hire including dates
   - IPs allotted to / being used by the members
   - Email address and IP address and time stamp used at the time of registration / on-boarding
   - Purpose for hiring services
   - Validated address and contact numbers
   - Ownership pattern of the subscribers / customers hiring services

   The language of the Direction imposes the burden to ensure accuracy of information on the service providers mentioned above by stating that "accurate information" must be maintained. Therefore, entities will now have to consider if manual intervention is required at the time of registration to ensure that accurate information is required. Some form of KYC process may need to be introduced to ensure accuracy. In relation to some of the items above, it is unclear how a service provider will ensure accuracy. For instance, the purpose of hiring services may change from time to time. Is it upon the service provider to ensure that the logs maintained record the change of purpose? The information sought required to be collected and maintained also seems excessive both in terms of scope and time.

6. *Requirements for virtual asset ecosystem*: The Direction also applies to virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time), as

NewsX
April 01, 2025

Vaibhav Parikh, Partner, Nishith Desai Associate on Tech, M&A, and Ease of Doing Business
March 19, 2025

SIAC 2025 Rules: Key changes & Implications
February 18, 2025

set out in Annexure A. These entities are required to maintain all information obtained as part of KYC as well as records of financial transactions for a period of five years. Moreover, the information with respect to transaction records should be accurate and is required to be maintained in such a way that individual transaction can be reconstructed along with the relevant elements thereof such as parties to the transactions and IP addresses, nature, amount and date of transaction, etc. While the Income Tax Act, 1961 has recently been amended to include a definition for "Virtual Digital Assets" (**VDA**), it is unclear whether the Direction is referring to the same – and whether it seeks to enforce KYC norms vis-a-vis all services associated with VDA. The intent of the Direction appears to be directed at crypto-asset-based services and exchanges.

7. *Consequences of non-compliance:* When CERT-In issues any order/directions to a service provider/intermediary/data centre/body corporate, such entities must mandatorily take action or provide information or any such assistance to CERT-In. If the order/direction provide a format in which the information is required (up to and including near real-time), and a specified timeframe in which it is required, such directions must be complied with. Non-compliance will be treated as non-compliance with the Direction.

   The CERT-In Rules do not provide for any specific penalty for non-compliance with the reporting requirements thereunder. Hence, non-compliance with the CERT-In Rules would be penalized under Section 45 of the IT Act, which is the residuary penalty section and provides for a maximum penalty of INR 25,000. However, failure to provide information to CERT-In or to comply with the directions of CERT-In are punishable with imprisonment for a term of up to one year and / or with fine of up to one lakh rupees, as per Section 70B(7) (which is a non-cognizable offence). Hence, the penalty for non-compliance with reporting requirements has effectively been enhanced significantly by way of the Direction since now the Direction requires also mandates reporting. Therefore, if an entity fails to report a cyber security incident as per the procedure under the Direction, it may be liable under Section 70B(7).

   Importantly, entities do have a safeguard under Section 70B(8) which provides that no court will take cognizance of an offence under Section 70B, unless a complaint is made by a CERT-In officer. The CERT-In Rules provide the process to be followed before a complaint is made by a CERT-In officer. In cases of non-compliance, the concerned officer of CERT-In is required to submit a report of such non-compliance to the Director General providing details thereof.[6] All cases of non-compliance are submitted to a Review Committee constituted under Rule 19 of the CERT-In Rules.[7] Basis the direction of the Review Committee, the Director General can authorize an officer of CERT-In to file a complaint as provided under Section 70B.[8]

POWERS OF CERT-IN TO ISSUE SUCH DIRECTIONS

CERT-In has wide powers with respect to cyber security incidents under Section 70(B)(4) of the IT Act including issuing guidelines, advisories, etc. relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

While the IT Act gives CERT-In the power to issue directions, the Direction as issued contains provisions which effectively amend the CERT-In Rules (such as the nature of mandatorily reportable incidents and the timelines or reporting). It can be argued that such an amendment can only be carried out by the Central Government, under its rule-making powers under Section 87 of the IT Act. Further, as per Section 87(3), any rule made by the Central Government under the IT Act has to be tabled before each House of Parliament for discussion. Since this process has been entirely circumvented, it will have to be seen if the Direction can stand its ground in case of a judicial challenge. Similarly, it would need to be evaluated if Section 70B of the IT Act, which specifies the powers and functions of CERT-In, excessively delegates powers to the agency without effective guidelines and boundaries. It can also be argued that power under subsection (6) of Section 70B is limited to specific directions to be issued in relation to an incident and not a general direction in the nature of rules, the mandate for which is only with the Central Government and not CERT-In.

TAKEAWAY

The Direction does come as a surprise in terms of the broadly worded provisions. While the intention behind the Direction is laudable, the provisions of the Direction are overreaching and may not be the most efficient manner of dealing with cybersecurity threats. Considering that the Direction requires several technological changes, businesses must internally assess their practices and determine how and where changes are required. In some cases, constant manual intervention may also be required.

Considering that the Direction has far-reaching implications along with penal consequences, it would be helpful if CERT-In can provide a window seeking queries from industry participants and other stakeholders, subsequent to which requisite clarifications or amendments to the Direction can be issued.

– Aniruddha Majumdar, Aparna Gaur, Huzefa Tavawalla & Gowree Gokhale

You can direct your queries or comments to the authors

---

[1] Available at: https://www.cert-in.org.in/Directions70B.jsp (Last visited on May 4, 2022).

[2] Our analysis of the Cert-In Rules is available at https://www.natlawreview.com/article/reporting-cybersecurity-breaches-india-it-time-to-overhaul-law.

[3] See www.cert-in.org.in (Last visited on May 4, 2022).

[4] See http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf (pg. 17) (Last visited on May 4, 2022).

[5] Puttaswamy v Union of India, (2017) 10 SCC 1; Our analysis of the judgement is available at: https://www.nishithdesai.com/SectionCategory/33/Technology-Law-Analysis/12/60/TechnologyLawAnalysis/5028/3.html (Last visited on May 4, 2022).

[6] Rule 16 of the CERT-In Rules.

[7] Rule 18 of the CERT-In Rules.

[8] Rule 20 of the CERT-In Rules.

ANNEXURE A

Summary of the Direction

1. The list of cyber security incidents that must be mandatorily reported by service provider, intermediary, data centre, body corporate and Government organisation has been amended and several additional types of cyber security incidents have been added (see Annexure I of the Direction). Such incidents have to be mandatorily reported by the organisation within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in

2. When CERT-In issues any order/directions to a service provider/intermediary/data centre/body corporate, such entities must mandatorily take action or provide information or any such assistance to CERT-In. If the order/direction provides a format in which the information is required (up to and including near real-time), and a specified timeframe in which it is required, such directions must be complied with.

3. The Direction provides several compliance requirements for different types of entities:

a. Service providers, intermediaries, data centres, body corporate and Government organisations are required to:

- 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 their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies can use accurate and standard time source other than NPL and NIC, however they must ensure that their time source does not deviate from NPL and NIC.
- Designate a Point of Contact to interface with CERT-In. This requirement already exits under Rule 17 of the CERT-In Rules. However, the Direction adds the format in which information relating to a Point of Contact has to be sent to CERT-In (See Annexure II of the Direction).
- Mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and these logs have to be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.

b. Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers are required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:

- Validated names of subscribers/customers hiring the services
- Period of hire including dates
- IPs allotted to / being used by the members
- Email address and IP address and time stamp used at the time of registration / on-boarding
- Purpose for hiring services
- Validated address and contact numbers
- Ownership pattern of the subscribers / customers hiring services

c. Virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) are required to:

- Maintain all information obtained as part of Know Your Customer (KYC) in accordance with the Direction and records of financial transactions for a period of 5 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.
- With respect to transaction records, accurate information has to be maintained in such a way that individual transactions can be reconstructed along with the relevant elements comprising of, but not limited to, information relating to the identification of the relevant parties including IP addresses along with 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.

ANNEXURE B

The new additions to types of mandatorily reportable cyber security incidents inserted by way of the Direction are underlined:

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorized access of IT systems/data
- Defacement of website or intrusion into a website and unathorised changes such as inserting malicious code, links to external websites, etc.

- Malicious code attacks such as spreading of virus/ worm/ trojan / bots/ spywares/ Ransomware/ Cryptominers
- Attacks on servers such as database, mail and DNS and network devices such as routers
- Identity Theft, spoofing, and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Services (DDoS) attacks
- Attacks on applications such as e-governance, e-commerce
- Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
- Data breach
- Data leak
- Attack on Internet of Things (IoT) devices and associates systems, networks, software, servers
- Attacks on incident affecting Digital Payment Systems
- Attacks through Malicious mobile apps
- Fake mobile apps
- Unauthorized access to social media accounts
- Attacks on malicious/suspicious activities affecting cloud computing systems/servers/software/applications
- Attacks or malicious suspicious activities affecting systems/servers/networks/software/applications related to Big Data, Block Chain, Virtual Assets, Virtual Asset Exchanges, Custodian Wallets, Robotics, 3D and 4D printing, additive manufacturing, drones
- Attacks or malicious/suspicious activities affecting systems/servers/software/applications related to AI and Machine Learning