

Technology Law Analysis

May 25, 2022

CERT-IN RELEASES FAQs EXPLAINING THE DIRECTION ON CYBERSECURITY

On 28 April 2022, the Indian Computer Emergency Response Team (“**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 was issued under Section 70B(6) of the Information Technology Act, 2000 (“**IT Act**”). Our analysis of the Direction is available [here](#). The Ministry of Electronics and Information Technology (“**MeitY**”) has now issued a list of frequently asked questions (“**FAQs**”) on the Direction in an attempt to resolve some industry concerns and clarify the intent and expectations of CERT-In.

A press conference was also organized with the Minister of State for Electronics and Information Technology, Mr. Rajeev Chandrasekhar on May 18, 2022 wherein he answered queries from the media regarding the Direction.² In the conference, Mr. Chandrasekhar emphasized that CERT-In’s role is to protect safety and security of the internet.

The FAQs clarify that they are not meant to replace/amend or alter any part of the IT Act, 2000 and/or the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties)

Rules, 2013 (“**CERT-In Rules**”).³ It is also stated that the FAQs are an evolving document which may undergo changes. Thus, the question whether a legislation or a Direction as issued by CERT-In can be clarified by way of FAQs remains open. In order to provide a consolidated understanding of the compliance requirements of an entity, we have analysed the relevant provisions under the CERT-In Rules and the Direction, read with the FAQs.

1. Mandatory reporting of incidents:

- **Timeline for reporting:** As per the Direction, Identified Entities are required to report the specified incidents within 6 hours of “noticing such incident or being brought to notice about such incidents”. We had recommended in our hotline (available [here](#)) that CERT-In should allow entities to update the information they provide once they have more concrete information about an incident. The FAQs clarify this point and provide that the Identified Entities may provide information to the extent available at the time of reporting and additional information may be reported later within a reasonable time to CERT-In.⁴ However, the FAQs also provide that if an incident covered in Annexure I of the Direction also meets certain criteria⁵ such as data breaches or incidents impacting human safety, such incidents should be reported within 6 hours. It is unclear what the intent behind identifying these specific incidents is and this aspect needs further clarity.

Additionally, FAQs state that Identified Entities also need to deploy appropriate security controls and follow reasonable security practices to detect and prevent cyber security incidents. This is not provided for in the Direction, but Section 43A of the IT Act requires a body corporate, possessing, dealing or handling any sensitive personal data or information (“**SPDI**”) in a computer resource which it owns, controls or operates, to implement and maintain reasonable security practices and procedures. It is unclear if by virtue of this clarification, all entities, whether or not they possess, deal with or handle any SPDI, are liable to be penalized if CERT-In establishes that such entities lack appropriate security controls and do not follow reasonable security practices.

- **Types of incidents:** The Direction expanded the list of cyber security incidents which are mandatorily reportable (see Annexure B), as compared to the CERT-In Rules. The method and format of reporting cyber security incidents is published on the website of CERT-In.⁶ Annexure I of the FAQs contains descriptions of the types of incidents covered, to provide further clarity. Several concerns have rightly been raised regarding the expansive nature of the Annexure to the Direction for mandatorily reportable incidents. CERT-In should, however, clarify that determination of whether an incident is mandatorily reportable is a two-step analysis. First, it must be considered whether the incident falls within the definition of “cyber security incident” as defined under the CERT-In Rules. If yes, it must be considered if such incident falls within the scope of any entries under the Annexure to the Direction. The industry has also been requesting for materiality thresholds for incidents in order for them to be mandatorily reported.
- **Entity which needs to report:** The Direction specifies that service providers, intermediaries, data centres, body corporates and Government organisations are covered under this reporting obligation (hereafter “**Identified Entities**”). The FAQs clarify that individuals are not meant to be covered under the Direction.⁷ In cases where multiple entities are affected by an incident, whether directly or indirectly, the FAQs provide that the entity which notices the cyber security incident is required to report to CERT-In.⁸ Further, the FAQs state that the obligation of reporting cyber incidents is not transferrable and cannot be “indemnified or dispense[d] with”. However, it is unclear why an entity cannot be indemnified by another entity when, for instance, the latter fails to report an

Research Papers

Compendium of Research Papers

January 11, 2025

FAQs on Setting Up of Offices in India

December 13, 2024

FAQs on Downstream Investment

December 13, 2024

Research Articles

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

January 15, 2025

Key changes to Model Concession Agreements in the Road Sector

January 03, 2025

The Revolution Realized: Bitcoin's Triumph

December 05, 2024

Audio

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

Renewable Roadmap: Budget 2024 and Beyond - Part I

August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

[Click here to view Hotline archives.](#)

Video

“Investment return is not enough” Nishith Desai with Nikunj Dalmia (ET Now) at FIIB event in Riyadh

October 31, 2024

Analysing SEBI's Consultation Paper

incident.

With this clarification, the obligation to report is not only on just the entity which has suffered the incident but could also be on another entity which notices such breach. For instance, in cases where an entity is obtaining the services of another entity, and the recipient entity comes to know of an incident at the service entity's end, as per the clarification in the FAQs, the obligation to report could be on the recipient entity as well. This requirement will be tough to implement since an entity may not have control over the computer resources of a contracting entity and will not have the wherewithal or authorization to collect information regarding the incident. Hence, the onus of reporting an incident should only be on the entity which is in charge of the computer resource which has been impacted and has access to the information required to be reported. This would be consistent with the IT Act, which recognizes the concept of a "person in-charge of computer resource" under several provisions such as Section 69B(2).

- Reporting Obligation of Intermediaries: The FAQs state that it is imperative that intermediaries also report those types of cyber security incidents which are not mentioned either in the annexure of the CERT-In Rules or in the Direction considering the nature, severity and impact of the incident.⁹ This is a highly onerous requirement, given that the scope of mandatorily reportable incidents is already very wide.

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. The FAQs clarify that the Direction does not envisage seeking of information by CERT-In from any entity on a continuous basis as a standing arrangement. Information will be sought only if cyber security incidents and cyber incidents occur, and on a case to case basis. The purpose of seeking information will also be limited to discharge of statutory obligations to enhance cyber security in the country. From the FAQs, it appears that the intent of seeking information by CERT-In is limited. The Direction should therefore be expressly amended since the existing language in the Direction appears to be over-broad.
3. **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. As stated in our hotline, there is a concern that this can have a significant impact on privacy of users. 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*.¹⁰

As per the FAQs, the logs that should be maintained depend on the sector that the Identified Entity is in, such as firewall logs, intrusion prevention systems logs, SIEM logs, web / database/ mail / FTP / proxy server logs, event logs of critical systems, application logs, ATM switch logs, SSH logs, VPN logs, etc. This list of logs is not exhaustive and is merely illustrative, and the FAQs state that both successful as well as unsuccessful events are required to be recorded from an incident response and analysis perspective. The scope of logs to be maintained remains over-broad, and it should be restricted to such logs which are strictly necessary for analyzing a cyber security incident. CERT-In should finalise the scope of such logs taking into account industry feedback.

The Direction also provides that 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. It has been clarified that in addition to storing of logs in India, the logs may be stored outside India as long as the obligation to produce logs to CERT-In is adhered to by the entities in a reasonable time.¹¹ The FAQs also state that 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.¹² The requirement to maintain records of financial transactions in the Indian jurisdiction goes beyond the requirement under the Direction which (under (vi)) does not require localization. Extraterritorial application of the Direction must be interpreted in light of Section 75 (as also mentioned in Question 26 of the FAQs. We have discussed this in detail in point 6 below with respect to applicability to foreign entities.

4. **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.

The FAQs clarify that the term "VPN service provider" does not include enterprise and corporate VPNs but refers to an entity that provides "Internet proxy like services" through the use of VPN technologies, standard or proprietary, to general Internet subscribers/users.¹³ However, there is still no clarity on the kind of entities that would be covered under "cloud service providers" given the lack of definition in the Direction. For e.g., it is not clear if only such service providers should be covered which provide dedicated cloud services, or if service providers which use a cloud incidentally as part of their services would also be covered.

With respect to the requirement to maintain "Ownership pattern of the subscribers", the FAQs clarify that basic information about customers and subscribers who use their services must be maintained including nature of the

customer (individual, partnership, association, company etc.)¹⁴ The particulars to be maintained should also include brief particulars of key management - this requirement was not present in the Direction and has been added in the FAQs. This may be difficult to maintain for all customers / subscribers since key management may change frequently and customers may not want to disclose such details.

5. **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. The FAQs specify that there is no need to mandatorily set system clocks in Indian Standard Time (IST), and that the Direction mandates uniform time synchronisation across all ICT systems irrespective of time zone.¹⁵ Specifically in case of cloud ICT infrastructures, the FAQs clarify that customers in cloud environments have an option to use the native time services offered by the cloud to synchronize their clock. They can also set up their own NTP server within their cloud environment. Accordingly, entities which rely on the native time services offered as part of the cloud may continue to use the same. For entities which synchronise with time sources other than the native cloud time services, they may use the NTP Servers of NPL, NIC or other accurate and standard time sources as long as the accuracy of time is maintained.

The FAQs clarify that an accurate time stamp is required to re-create the accurate sequence of events for a cyber incident, especially when multiple computer systems across entities are involved.¹⁶ Further, *“security technologies also rely heavily on specific patterns and correlation rules that are often based on time parameter, and unsynchronized clocks across systems could result in failure of security systems as well as an entity’s ability to act on proactive alerting/advisory of CERT-In as well as other agencies”*. Indeed, having synchronized time across systems helps the incident response team with immediate reporting and monitoring when it comes to cybersecurity. Cyber attackers typically attempt to cover the pathway through which they have broken inside a system for which they may compromise the system clocks. This causes all logs to go haywire, and without proper records, doing any forensic investigation becomes very difficult. Moreover, if the system clocks are not synchronized, it could result in the complete failure of the security systems to maintain accurate logs.

6. **Applicability to foreign entities**: One major concern with the Direction is its applicability to foreign service providers who are catering to users in India. The FAQs provide some guidance on this aspect stating that with respect to applicability of the Direction to foreign entities, the provisions of the IT Act should be referred to, specifically Section 1 and Section 75.¹⁷ Section 1(2) of the IT Act provides that the IT Act *“shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.”* Further, Section 75 provides that the provisions of the IT Act shall also apply to *“any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.”*

In case a foreign entity is non-compliant with any provision of the Direction with respect to a computer, computer system or computer network located in India, it could be considered to be in contravention of Section 70B of the IT Act. Since the contravention would involve a computer, computer system or computer network located in India, it can be argued that Section 75 should accordingly apply to such foreign entity, although the contravention has been committed outside India. Hence, based on the FAQs, it appears that the intent of the Direction is to only cover such foreign entities which have a computer, computer system or computer network in India. If the technological infrastructure of a foreign entity is not within India, it may not be subject to the Direction.

Nevertheless, with respect to similar questions on applicability of the Direction (including its compliance requirements) to entities outside India, the responses under the FAQs are largely unclear.¹⁸ Further, all entities operating in India are required to maintain such data in a safe and secure manner. Therefore, it should be specifically clarified in the Direction that only such entities which have computer infrastructure in India would be within the ambit of the Direction, and this interpretation would be in line with the provisions of the IT Act as well.

7. **Requirements for virtual asset ecosystem**: The Direction 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 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.

Notably, the Central Board of Direct Taxes is still in the process of finalizing the scope of definition of “virtual digital assets” under the Income Tax Act, 1961. Till the time there is clarity on the scope of the definitions, these obligations should be kept in abeyance.

8. **Consequences for non-compliance**: If there is non-compliance with any order/direction of CERT-In, it will be treated as non-compliance with the Direction. 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) of the IT Act (which is a non-cognizable offence). 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). We have discussed the procedure with respect to Section 70B(7) in our hotline (available [here](#)). Nevertheless, MeitY has clarified that the power under Section 70B(6) *will be exercised reasonably and on occasions when the non-compliance is deliberate.*¹⁹

There still exist numerous concerns with the Direction, and a lack of clarity with respect to many provisions remain, despite the FAQs. Industry bodies continue to make representations before the relevant authorities and it is likely that further clarifications will be provided.

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 23, 2022).

² Available at: <https://www.youtube.com/watch?v=In8PUveB-wk> (Last visited on May 23, 2022).

³ Our analysis of the Cert-In Rules is available at

<https://www.natlawreview.com/article/reporting-cybersecurity-breaches-india-it-time-to-overhaul-law>.

⁴ Question 30 of FAQs.

⁵ Question 30 of the FAQ provides that "Any incident as stated in Annexure-I of the Cyber Security Directions of 28.04.2022 and meeting the following criteria should be reported within the stipulated 6 hour time:

- cyber incidents and cyber security incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant including Ransomware) on any part of the public information infrastructure including backbone network infrastructure

- Data Breaches or Data Leaks

- large-scale or most frequent incidents such as intrusion into computer resource, websites etc.

- cyber incidents impacting safety of human beings".

⁶ See www.cert-in.org.in (Last visited on May 23, 2022).

⁷ Question 7 of FAQs.

⁸ Question 13 of FAQs.

⁹ Question 10 of FAQs.

¹⁰ 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](https://www.nishithdesai.com/SectionCategory/33/Technology-Law/Analysis/12/60/TechnologyLawAnalysis/5028/3.html).

¹¹ Question 35 of FAQs.

¹² Question 36 of FAQs.

¹³ Question 34 of FAQs.

¹⁴ Question 33 of FAQs.

¹⁵ Question 40 of FAQs.

¹⁶ Question 39 of FAQs.

¹⁷ Question 26 of FAQs.

¹⁸ See, for e.g., Question 27 and 28 of FAQs.

¹⁹ Question 23 of FAQs.

DISCLAIMER

The contents of this hotline should not be construed as legal opinion. View detailed disclaimer.

This Hotline provides general information existing at the time of preparation. The Hotline is intended as a news update and Nishith Desai Associates neither assumes nor accepts any responsibility for any loss arising to any person acting or refraining from acting as a result of any material contained in this Hotline. It is recommended that professional advice be taken based on the specific facts and circumstances. This Hotline does not substitute the need to refer to the original pronouncements.

This is not a Spam mail. You have received this mail because you have either requested for it or someone must have suggested your name. Since India has no anti-spamming law, we refer to the US directive, which states that a mail cannot be considered Spam if it contains the sender's contact information, which this mail does. In case this mail doesn't concern you, please unsubscribe from mailing list.