Technology Law Analysis

July 21, 2023

CYBERSECURITY GUIDELINES FOR GOVERNMENT – HOW ARE PRIVATE ENTITIES AFFECTED?

The Indian Computer Emergency Response Team ("**CERT-In**") and Ministry of Electronics and Information Technology ("**MeitY**") have issued detailed Guidelines on Information Security Practices for Government Entities ("**Guidelines**")[1] in furtherance of the objective of creating a safe and trusted internet. This follows the broader directions on cybersecurity which were issued by CERT-In in April 2022 ("**Directions**")[2] (applicable to all service providers, intermediaries, data centres, body corporate and Government organisations), and the CERT-In Rules from 2013.[3]

Notably, the Guidelines are only applicable to Central government organisations and their associated organisations including all Ministries, Departments, Secretariats and Offices[4], their attached and subordinate offices, all government institutions, public sector enterprises and other government agencies under their administrative purview ("**Government Entities**"). There are wide-ranging guidelines which have been prescribed for Government Entities ranging from measures to be taken for network and infrastructure security, identity and access management, securing cloud services, and user awareness and training.

IMPACT ON PRIVATE PARTIES WHILE CONTRACTING WITH GOVERNMENT ENTITIES

While the Guidelines apply primarily to Government Entities, they can have a considerable, although indirect, impact on private entities which contract with any Government Entities. The section on third party access and outsourcing are especially noteworthy. The key guidelines under this section are as follows:

- The Government Entity should ensure restricted access to information for third party service providers, and should share such information only after executing a non-disclosure agreement.
- The agreement must specify information security requirements to be complied with by such service provider, including at least:
  - General policy on information security;
  - Procedures to protect organisational assets;
  - Restrictions on copying / disclosure;
  - Controls to ensure return of information/assets in the vendor's possession after termination / expiry of the contract;
  - Right to audit contractual responsibilities either by itself or through third parties;
  - The right to monitor and the right to terminate services in the event of a security incident; and
  - Arrangements for reporting, notification and investigation of security incidents and breaches.
- The service provider must also provide:
  - their information security audit report to the Government Entity on a periodic basis or on request.
  - detailed list of all components of the software (including open source) / solution in the form of Software Bill of Material (SBOM).
  - Information on any identified vulnerabilities in the system to the Government Entity within a reasonable time period.
- The service provider must ensure protection and confidentiality of the data collected and processed by it, and should ensure that it is not shared with any third parties in the absence of express consent or an agreement with the Government Entity. Such data should also be provided to the Government Entity as and when required.
- Personnel of the service provider should also be required to comply with the information security policies, processes and procedures of the Government Entity.

Notably, the Guidelines require that in case of violation of the above obligations, the Government Entity should terminate the contract with the service provider, and the service provider would separately be liable under any laws which apply to such violation.

KEY TAKEAWAYS

In light of the increase in cybersecurity attacks and incidents in the past few years, it is imperative that all

Research Papers

FAQs on Setting Up of Offices in India
December 13, 2024

FAQs on Downstream Investment
December 13, 2024

Gaming Law 2024
December 12, 2024

Research Articles

The Revolution Realized: Bitcoin's Triumph
December 05, 2024

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 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 FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs

organisations, whether a Government Entity or not, enhance their cybersecurity infrastructure and processes. The Guidelines in effect make many compliances indirectly applicable to private entities, by virtue of their contracts with Government Entities. Organisations which typically contract with such entities, or intend to contract with the Government in the future would need to closely assess these Guidelines and take necessary steps towards implementation. Such measures would include not only network and infrastructural ones, but even internal policy measures, with respect to data access and responsibilities.

On the flip side, given that Government Entities will have the right to ask for and access extensive data of their vendors, the agreements should also contain adequate obligations for the Government Entity to protect such data. Hence, the obligations towards data protection and cybersecurity would need to be mutually imposed and enforced, although, it may be argued that the Government Entity would anyway be subject to such obligations by virtue of the Guidelines.

Provisions such as the right to terminate in case of a cybersecurity incident are quite radical, and will affect contractual negotiations with Government Entities significantly. Private service providers would need to consider how best to protect their interest, e.g. by negotiating clauses such that termination is permitted only in case of negligence in implementing security procedures.

Additionally, other measures to be taken by Government Entities may also have an impact on obligations of service providers. For e.g., the Guidelines restrict connections with third parties through ports, services, protocols, etc. and also require monitoring of all traffic to and from third party networks and systems. Hence, it is advisable for private entities to take stock of potential obligations which may be imposed on them as a result of these Guidelines and take steps towards preparation.

– Aniruddha Majumdar & Aparna Gaur

You can direct your queries or comments to the authors.

[1]Available at: https://ww w.cert-i n.org.in /PDF/gui delinesg ovtenti ties.pdf (Last visited on July 21, 2023).

[2]Available at: https:/ /www.ce rt-in.or g.in/D irecti ons70B .jsp (Last visited on July 21, 2023). Our analysis of the directions is available at: https:/ /www.da taguida nce.com /opinio n/india -strict er-cybe rsecuri ty-norm s-and-re porting.

[3]I.e., the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

[4]As specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961

September 26, 2024

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996

September 22, 2024