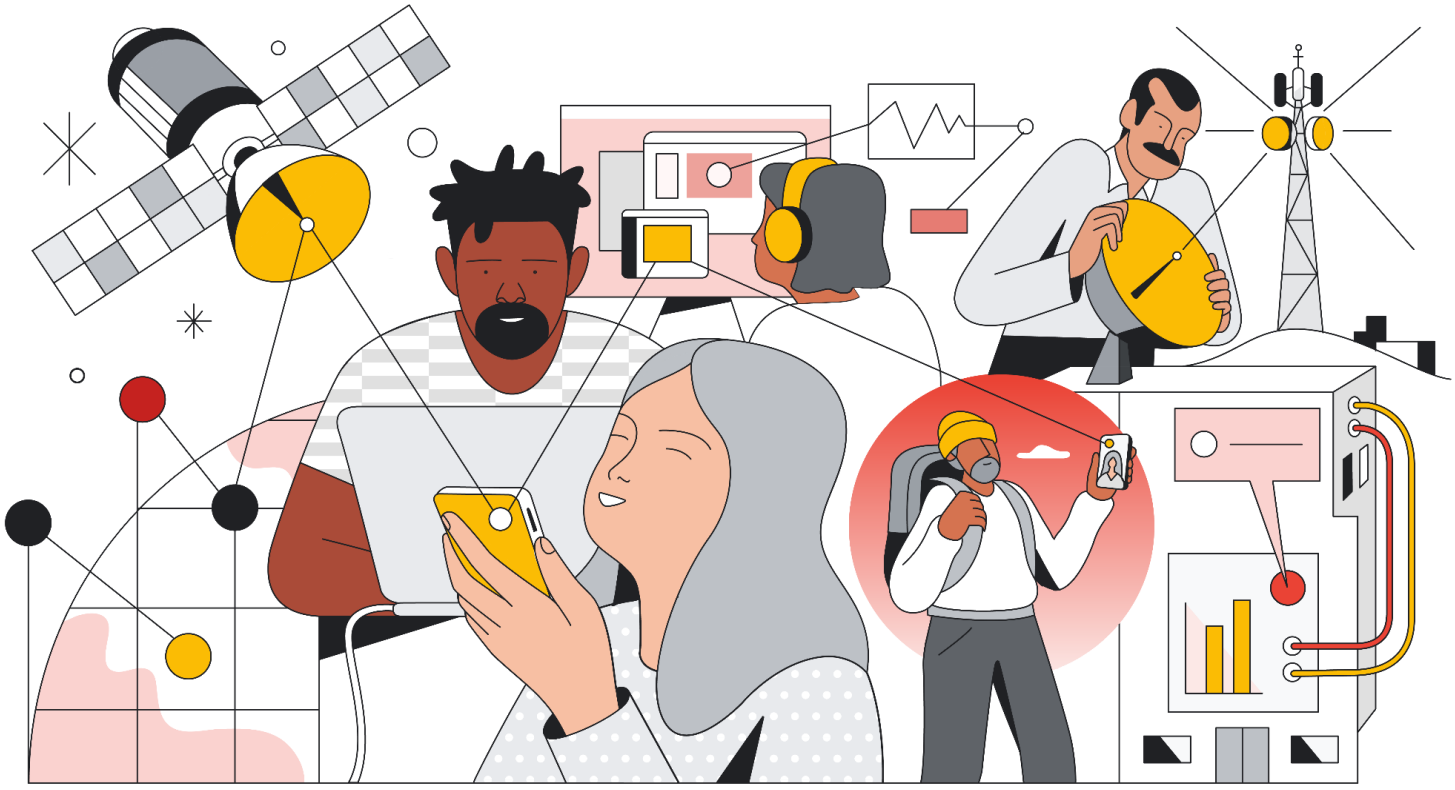
Google Cloud

Google Cloud Whitepaper
June 2023

Insights into Indian Telecoms Regulations



Insights into Indian Telecoms Regulations

Disclaimer

This whitepaper applies to Google Cloud products described in the Google Cloud Services Summary. The content contained herein is correct as of June 2023 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

Telecommunications is perhaps the most significant engine of world economic growth. Telecoms have powered social change and business expansion for almost 200 years, from telegraphs at the dawn of the Industrial Revolution to today's mobile apps, video, and data services. It's easy to see why: Communications Service Providers, as they are known today, connect people and their inventions, enabling new markets and innovations.

The industry, however, finds itself in the midst of epic disruption - facing low single-digit revenue growth[1], increasing CAPEX investments and demand on the network, and challenges in customer experience. Accordingly, the leaders of Communications Service Providers are looking for innovative ways to unlock new revenue streams, transform the end-to-end customer experience, handle explosive usage, effectively manage increasingly complex systems, unlock the full potential of their data, and deliver on sustainability objectives.

Underpinning these focus areas, Communications Service Providers in India are focused on ensuring they operate their critical infrastructure in line with ever-evolving regulatory, security, data privacy, and sovereignty requirements. As organisations accelerate their digital transformation journeys towards long-term growth - powered by cloud technology - there is a need to understand both the implications of these regulations for cloud and how the cloud can help Communications Service Providers to address these challenges.

This paper provides:

- An overview of the security-related regulations, guidelines, and standards that apply to Communications Service Providers within India
- Insight into the key themes and principles that emerge from the regulations
- Guidance on how Google Cloud can help Communications Service Providers meet their regulatory requirements

Regulatory themes

Telecom networks are critical in supporting economic development and national security within India. Communications Service Providers are also trusted with large amounts of sensitive customer information. Therefore, Communications Service Providers and the telecoms networks they operate are subject to many security and privacy-related regulations. In India's context, this includes both global security standards and national-level regulation and guidelines.

A survey of specific regulations affecting Communications Service Providers in India is included in the Appendix. In this section, we summarise the main themes emerging from these regulations and how Google Cloud can help.

[1] TM Forum, September 2022

Foundational security

Communications Service Providers are high-profile targets for cybersecurity attacks and require protection against cybersecurity risks, including state-level and state-sponsored attacks, insider threats, industrial espionage, and sabotage. Increasing cybersecurity concerns have led to governments and organisations to work together to shape cybersecurity requirements and frameworks, including global standards such as:

- ISO 27001
- ISO 27017,
- ISO 27018 and
- AICPA SOC2 (SSAE 18)

In India we see the Ministry of Electronics and Information Technology's (MeitY) Cloud Security Best Practices and the NCIIPC Guidelines for Protection of Critical Information Infrastructure as important guidance for Communications Service Providers (noting the IT Act, 2000 defines telecoms as Critical Information Infrastructure).

Security regulations and guidelines identify specific security measures and best practices across domains, such as physical security, network security, identity and access management, security incident management, and personnel security.

How we help: Google Cloud has comprehensive and in-depth security controls that we have deployed to help protect your data, summarised in this security overview paper. Other papers detail our security practices in specific areas, such as encryption at rest, encryption in transit, and infrastructure security. Google Cloud also publishes guidance on security best practices, use cases, and blueprints.

Google Cloud is registered with MeitY, meaning that Google Cloud can do business in India as per the MeitY Guidelines for Procurement of Cloud Services.

Google Cloud's security, third-party audits, and certifications help support customer's compliance. Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google Cloud undergoes several independent third-party audits regularly to provide this assurance. Customers can request reports via our Compliance Reports Manager.

Data privacy and communications confidentiality

With consumers entrusting Communications Service Providers with large volumes of sensitive customer data, including personally identifiable information and communications records, it's important that the consequences of data breaches be understood.

Protecting customer data privacy and confidentiality of communications are fundamental requirements for telecom operators. Unethical usage of customer data can lead to financial penalties (see below) and loss of customer trust.

Within India, the Unified Licensing Agreement includes requirements to ensure privacy of communication and to ensure that unauthorised interception of messages does not take place. The Sensitive Personal Data or Information (SPDI) rules under the IT Act of 2000 provides a further legal framework for data protection, including provision for financial penalties for negligence in protecting sensitive personal data. These protections are expected to be updated by the Digital Personal Data Protection Bill, which at the time of writing remains in draft and for review by India's Parliament.

How we help: Google Cloud's trust principles provide a starting point for our approach to data privacy.

Customers own their data, not Google. We want you to feel confident that taking advantage of Google Cloud doesn't require you to compromise on security or control of your business's data.. Google Cloud does not use customer data for advertising and we do not sell customer data to third parties. Our Cloud Data Processing Addendum for Google Cloud further describes our commitment to protecting your data.

Google Cloud is also compliant with international standards on data privacy, such as:

- ISO 27018 (Cloud Privacy)
- ISO 27701 (Privacy - Data Processor)

Additionally, Access Transparency for Google Cloud and Google Workspace supports this trust by providing logs of actions taken by Google staff and the reason for access including references to support tickets where relevant.

For more information, refer to our whitepaper on trusting your data with Google Cloud and to Google Cloud's Privacy Resource Center.

Data residency

When moving to a cloud environment, Communications Service Providers face the challenge of validating and controlling where their data resides. The importance of managing data residency is increasing as regulators push for more stringent requirements. For example, Communications Service Providers in India subject to the Unified Licence Agreement must ensure that certain data types (e.g., domestic telecoms traffic, domestic billing and domestic user information) remain within India.

How we help: Google Cloud services offer customers the ability to control where your data is stored via Data Residency. Google will store that customer data at rest only in the selected Region/Multi-Region in accordance with our Service Specific Terms.

Within India, customers can store data at rest exclusively within two cloud regions, Mumbai Region Data Center (asia-south1) and Delhi Region Data Center (asia-south2)

To assist customers in enforcing these controls, Google Cloud offers Organization Policy constraints which can be applied at the organisation, folder, or project level. You can limit the physical location of a new resource with the Organization Policy Service resource locations constraint.

Google Cloud customers can use VPC Service Controls to restrict the network locations from which users can access data, defining a service perimeter outside of which customer data cannot be accessed. This functionality allows customers to limit user access by IP address filtering, even if the user is otherwise authorised. Cloud Armor also allows customers to restrict locations from which traffic is allowed to their external load balancer.

Operational requirements

Should the availability of public communication services be impacted by a security incident, widespread disruption could occur. This has potential implications for both public safety and national security. Communications Service Providers could also face fines, reputational damage, and loss of business.

How we help: Communications Service Providers are responsible for ensuring they are designing for high availability (as well as security) when planning cloud solutions. Google Cloud publishes architecture guidelines to help customers achieve high availability at scale.

Google Cloud also supports customers with Backup and Disaster Recovery solutions. Communications Service Providers can use these solutions to design, build, and validate robust disaster recovery patterns that meet their specific recovery time objectives (RTOs) and recovery point objectives (RPOs).

To complement this, Google Cloud also has comprehensive internal plans and systems for its business continuity (refer to ISO 22301).

Google Cloud also offers customers the choice of manual or automated software updates, with the flexibility to control software update approvals and scheduling. Refer to OS Patch Management for an example.

Google Cloud security solutions

In addition to the security features and regulatory compliance already described, Google Cloud offers several Security solutions for a more comprehensive and holistic approach to security.

Communications Service Providers migrating to the cloud may not initially have the expertise to decide which security capabilities they need. Security solutions help customers identify those needs and rapidly roll out of relevant security functionality based on common blueprints and established best practices.

Security Foundations solution

As a starting point for customers who need clarification on their security needs, the Security Foundations solution includes a set of recommended products and security capabilities to help Communications Service Providers achieve a strong security posture within their Google Cloud environment.

This solution is based on the Security Foundations whitepaper and aligns with Google Cloud's security best practices.

Security and Resilience Framework (SRF) solution

Google Cloud can also support Communications Service Providers in carrying out a thorough review of their security practices.

The Security and Resilience Framework helps customers to establish or refresh their security program, founded on a risk-based assessment of the entire cybersecurity lifecycle (identify, protect, detect, respond, recover), utilising established industry frameworks.

The Discovery Platform supports the assessment and includes security maturity assessments across multiple domains. Google Cloud will provide a tailored set of recommendations around security best practices and recommended Google Cloud security products and solutions.

Web App and API Protection (WAAP) solution

The Web App and API Protection solution (WAAP) provides capabilities that protect applications, websites, and public APIs from internet-based threats, including DDOS, fraud, and botnet attacks.

This solution is relevant for all Communications Service Providers since DDOS attackers commonly target their infrastructure and systems, and unfortunately, the increased adoption of APIs by Communications Service Providers can expose their capabilities. In 2022, Google Cloud successfully identified and blocked the largest DDOS attack on record, demonstrating our ability to protect customers from internet-based attacks.

The WAAP solution includes the following products:

- Cloud Armor

- reCAPTCHA Enterprise
- Apigee API Management

Autonomic Security Operations (ASO) solution

Google Cloud's Autonomic Security Operations solution helps Communications Service Providers withstand security attacks through an adaptive, agile, and highly automated approach to threat management.

This solution is relevant for Providers that are interested in transforming their existing Security Operations Centre (SOC) or Security Incident and Event Management (SIEM) by increasing scale, automation, and the use of machine learning (ML) to keep up with a high volume of security incident data and deliver effective threat intelligence and incident response.

By leveraging the power of Chronicle and Mandiant, customers can transform their security operations and achieve a 10X increase in productivity, visibility and speed.

For more information, refer to our Autonomic Security Operations whitepaper.

Conclusion

Communications Service Providers in India are looking to transform and grow their business. Digital transformation initiatives include modernising core network and IT systems (including operations support system (OSS) and business support system (BSS)) via migration to the cloud and adopting cloud-native architectures. Communications Service Providers are also looking to improve customer experience and operational efficiency and monetise their data by adopting cloud-based analytics and ML to gain insights from their customer and network data.

Google Cloud is helping Communications Service Providers transition to the cloud while keeping in step with applicable laws, regulations, and guidance. Google Cloud continues to innovate in areas such as encryption, key management, auditability, transparency, and data residency to help Communications Service Providers meet their operational security, resilience, and data privacy needs.

Google Cloud is committed to keeping in step with telecom laws and regulations, to meet the evolving needs of Communications Service Providers and consumer demand in the telecommunications industry.

Appendix A: Regulations and Standards Impacting the Telecom Industry

As the industry broadens and new business lines are added, there is a shifting risk landscape for trust leaders in privacy, compliance, risk, and security. Narrowing the focus, let's review some of the top requirements impacting the telecom industry in India today.

Global Security Standards

The following global standards on Information Security are not specific to Telecoms but are widely accepted as a baseline for good security practices and provide a way to measure organisational compliance to internationally recognized security policies. MeitY's Cloud Security Best Practices recommends that Cloud Service Providers be certified against ISO 27001, ISO 27017, ISO 27018, and SSAE 16/SOC2.

Google Cloud supports compliance with the following standards:

- ISO 27001 outlines and provides the requirements for an information security management system, specifies a set of best practices and details the security controls that can help manage information risks
- ISO 27017 provides guidelines for information security controls applicable to the provision and use of cloud services
- ISO 27018 relates to one of the most critical components of cloud privacy - the protection of personally identifiable information (PII)
- AICPA SOC2 is based on the Statement of Standards for Attestation Engagements No.18 (SSAE 18), which extends the SSAE 16 standard recommended by MeitY.

Refer to the Google Cloud Compliance Resource Center for more information on the above standards, plus many more.

Unified Licensing Agreement

The National Telecom Policy (NTP) 2012 introduced the Unified Licensing Agreement after accepting Telecom Regulatory Authority of India (TRAI) recommendations. The guidelines for the Unified License Agreement states that one company can have only one Unified Licence. The Unified Licensing Agreement has been updated continuously since 2012 and provides an important reference for certain Telecom Service Providers operating in India.

The following Security Conditions (Chapter VI) are noted in relation to the use of Cloud services by Telecoms Service Providers:

- Requirement to ensure privacy of communication and ensure that unauthorised interception of messages does not take place. [39.4]

- Requirement to validate testing of network elements to relevant Indian or International Security Standards e.g. ISO 27000 series [39.7]
- Requirement to take appropriate security precautions to protect the network [39.8]
- Potential for fines to be imposed for security breaches [39.11]
- Requirement for domestic telecoms traffic to remain within India [39.23 (iii)]
- Requirement to retain billing information and domestic user information within India [39.23(vii)]

Information Technology Act, 2000 (IT Act)

The Information Technology Act, 2000 (IT Act) is the primary law in India dealing with cybercrime and electronic commerce. The IT Act provides a legal framework for electronic governance, defines cyber crimes and prescribes penalties against them. The IT Act aims to promote data protection in India via security practices and procedures to safeguard private and personal information. Companies that conduct business in India are now subject to new policies by the IT Act, such as adding specific company policies, adopting proactive data removal tools and implementing new notification procedures.

Per Section 39 (sub-section 39.1) of Licence Agreement for Provision of Unified Access and Services, strong encryption is restricted by the Unified Licence Agreement because internet service providers are not permitted to deploy “bulk encryption” on their networks in India. Users are restricted from using encryption with keys longer than 40 bits without prior permission. Moreover, the IT Act gives the central and state government the authority to direct any agency to intercept, monitor, or decrypt information transmitted, received, or stored through any computer resources.

The Sensitive Personal Data or Information (SPDI) rules under the IT Act 2000 also provide a set of minimum rules and regulations that must be followed by an organisation to safeguard personal and sensitive data.

Protection of Critical Information Infrastructure (CII)

The IT Act 2000 also defines Critical Information Infrastructure (CII) as resources that “shall have a debilitating impact on national security, economy, public health or safety” if incapacitated or destroyed. Telecoms is defined as Critical Infrastructure (along with other sectors such as Energy, Financial Services, Transport & Government).

Based on the IT Act, the National Critical Information Infrastructure Protection Centre (NCIIPC) was established to identify and protect CII across India. The NCIIPC has published Guidelines for Protection of Critical Information Infrastructure, containing recommended security controls (summarised in Figure 1 below). The recommended controls are similar to those contained in international standards such as the ISO 27000 series.

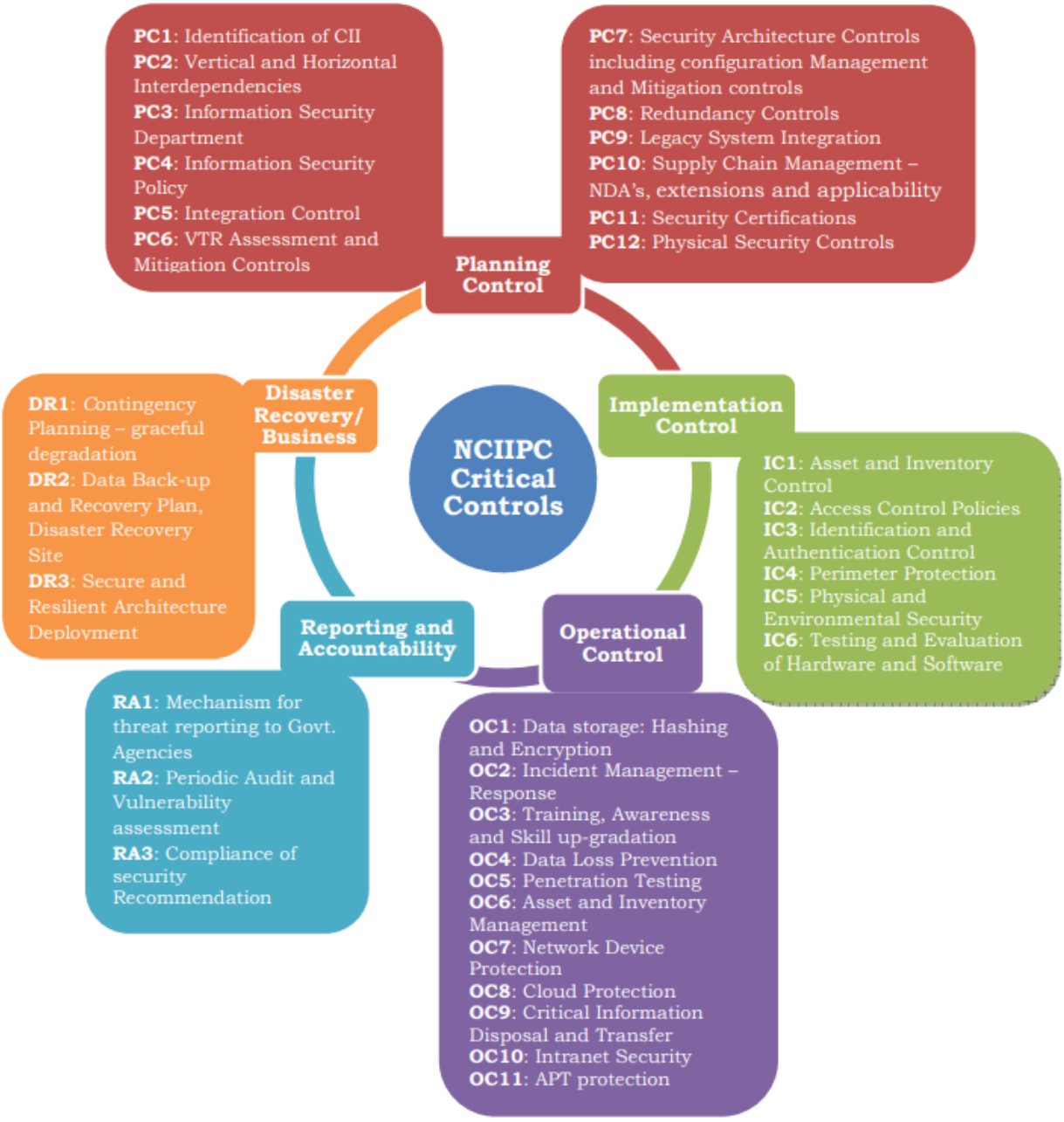


Figure 1: NCIIPC Best Practices Security Framework[2]

[2] Guidelines for Protection of Critical Information Infrastructure, January 2015

Ministry of Electronics and Information Technology (MeitY)

The Ministry of Electronics and Information Technology (MeitY) is a government agency providing policies and guidelines to the electronics and information technology sector. Their main objective is to promote the growth of electronics and IT industries by promoting R&D and innovation while emphasising efficiency in digital spaces.

Procurement of Cloud Services

MeitY provides the requirements and guidelines for Cloud Service Providers to empanel (register) their products and services with the Government of India. MeitY dictates a set of mandatory and optional categories of services to be offered by Cloud Service Providers. Google Cloud is empanelled by MeitY, meaning that Google Cloud can do business in India as per the MeitY Guidelines for Procurement of Cloud Services.

Cloud Security Best Practices

In 2020, MeitY published its advisory document connected to the MeghRaj (Government of India Cloud) initiative,Cloud Security Best Practices. This document is not specific to telecoms or binding for Communication Service Providers.

Personal Data Protection Bill

In November 2022, MeitY published a draft Digital Personal Data Protection Bill (DPDB Bill) to govern the processing of digital personal data within India.

Under this DPDB Bill, personal data may be processed only for a lawful purpose for which an individual has given consent. Certain rights would be granted to individuals, including the right to obtain information, seek correction and erasure, and address grievances. The DPDP Bill also limits cross-border transfers of personal data to jurisdictions that the government will notify and such transfers will need to fulfil terms and conditions that will be prescribed by the government. This Bill calls for the establishment of a Data Protection Board of India to adjudicate non-compliance with the provisions of the Bill.

At the time of writing, the Personal Data Protection Bill had not passed into law. It is likely that the bill is tabled for enactment by the Indian Parliament in the second half of this year.

India CERT-In Cybersecurity Directions 2022

India CERT-In Cybersecurity Directions 2022 (Cert-In) are directions issued under Section 70 B, sub-section (6) of the IT Act. CERT-In provides guidance for the types of incidents that must be mandatorily reported and imposes notification requirements for such incidents to CERT-In 6 hours after notice of the incident. These Directions apply to all entities, including foreign

companies that provide services to the citizens of India.

Additional regulations for consideration

Other relevant legislation for Indian Communication Service Providers includes:

- The Indian Telegraph Act, 1885
- The Indian Wireless Telegraphy Act, 1933
- The Telegraph Wires (Unlawful Possession) Act, 1950

A Draft Telecommunication Bill was released in 2022 by the Ministry of Communications, with the intention of updating the regulations mentioned above, but at the time of writing, this act had not been approved.