Date: 27 September, 2024

To:
Shri Devendra Kumar Rai,
Joint Secretary (Telecom),
Department of Telecommunications,
Ministry of Communications,
Government of India

Sanchar Bhawan, 20, Ashoka Road,
New Delhi - 110001
jst-dot@gov.in

Access Now's Suggestions on the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024

We thank the Department of Telecommunications ("DoT") for the opportunity to submit suggestions with respect to the draft Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024 ("the Rules") under the Telecommunications Act, 2023 ("the Act").

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence and expertise based in over 20 countries across six continents, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights.[1]

Access Now engages with a global community of individuals from over 162 countries in our annual RightsCon summit series, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We helped found the Computer Incident Response Center for Civil Society (CiviCERT) network and are a member of the Forum for Incident Response (FIRST).[2] We have special consultative status at the United Nations.

In India and globally, Access Now has consistently engaged with stakeholders including governments and regulatory authorities on matters pertaining to digital rights,[3] including

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] CiviCERT, *About CiviCERT*, https://www.civicert.org/about/; Forum for Incident Response, *Vision and Mission Statement*, https://www.first.org/about/mission.
[3] Access Now, *No liberty, no safety: Sri Lanka must withdraw the Online Safety Bill*, https://www.accessnow.org/press-release/sri-lanka-must-withdraw-the-online-safety-bill/.

data protection,[4] cybersecurity,[5] content governance,[6] internet shutdowns,[7] surveillance and digital security.

Introduction

At the outset, we welcome the DoT's initiative to identify "critical" parts of telecommunications infrastructure which require a higher degree of monitoring and oversight. Threats to people's safety and security through targeting communications networks are growing given their increased importance in people's lives. At the same time, the contours of any powers relating to critical telecommunication infrastructure should be clear to prevent misuse and abuse and their relevance for security must not be used to evade accountability.

Access Now advocates for universal access to consistent, affordable, open, and secure internet worldwide.[8] Ensuring secure and stable telecommunications infrastructure promotes the goal of enabling access for all, at all times. Any disruption to networks is problematic, whether by state actors[9] or in the form of cyber attacks by unknown parties.[10] Vulnerabilities in telecommunications infrastructures can impact people's protected rights, including the right to freedom of speech and expression through safe and secure channels and the right to privacy. Governments must ensure that people are able to trust the services they are using and have access to secure communications networks.

Given the importance of these rules, we welcome this consultation process and recommend that DoT continue to embrace this open, participatory, multi-stakeholder

---

[4] Access Now, *Joint submission on the Bangladesh Draft Data Protection Act 2023,* https://www.accessnow.org/wp-content/uploads/2023/10/Submission-on-the-Bangladesh-Data-Protection-Act-2023-Access-Now-and-Tech-Global-Institute.pdf.

[5] Access Now, *Discussion Paper on International Cybersecurity Norms* for the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, https://www.accessnow.org/to-keep-us-safe-global-cybersecurity-norms-must-be-human-centered-and-protect-rights/.

[6] Access Now, *Submission on the draft Broadcasting Services (Regulation) Bill, 2023,* https://www.accessnow.org/wp-content/uploads/2024/01/Access-Now-Submission_Broadcasting-Services-Bill_January-2024.pdf.

[7] Access Now, *Shrinking democracy, growing violence: Internet shutdowns in 2023*, https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf.

[8] Access Now, *More than 3.5 billion left in the dark: why we're still fighting to reach U.N. targets for internet access*, https://www.accessnow.org/internet-access/.

[9] Access Now, *What they did in the shadows: Internet shutdowns and atrocities in Ukraine*, https://www.accessnow.org/internet-shutdowns-and-atrocities-in-ukraine/.

[10] Access Now, *Defending users at risk from DDoS attacks: An evolving challenge*, https://www.accessnow.org/defending-users-at-risk-from-ddos-attacks-an-evolving-challenge/.

process and also ensure that once finalised, the Rules are placed before Parliament in accordance with Section 56(3) of the Act.

Recommendations

1. **Designation of critical telecommunication infrastructure — Lack of certainty and transparency in decision-making.**

The Central Government has a discretionary power to declare any telecommunication network as "Critical Telecommunication Infrastructure" (CTI) under Section 22(3) of the Act. The section states that in order to be declared as CTI, the network must be one which, if disrupted, would have a "debilitating impact on national security, economy, public health or safety."

There is no procedure laid out in the Act or the rules as to the process which the Central Government must follow to arrive at its determination, and the specific grounds that must be met. There is also no scope for people, who will face the impact of any disruption, to request consideration of a network as CTI or to provide feedback on any proposal to declare a network as CTI. It is unclear as to which body within the Central Government is empowered to make such a declaration.

Omitting to declare a certain network as CTI may have a devastating effect on people's lives. On the other hand, given the significant compliance requirements for any network declared as a CTI, an inappropriate declaration will impose a burden on such a network or service provider.

The centralisation and opacity in decision-making at this level is not desirable, as it leads to uncertainty and undermines public trust in policy processes. Policies should be people-centric and anchored in plural democratic processes, rather than promoting *ad hoc* decision-making controlled by unspecified and inaccessible officials. The process should also not be disproportionately focused on networks relevant for security of the state or the military. The impact of security, or the lack thereof, of important telecommunications networks and services will be felt by people. It is therefore essential to involve them in the decision-making process, understand how and when they use these systems and when their data may be at risk, in order to effectively protect relevant networks.

We recommend that Section 22(3) of the Act be amended and include a clear mechanism, involving consultation, to notify any network as Critical Telecommunication Infrastructure; and specific grounds on which such a decision can be made. A draft amendment to this effect should be published for input and comments.

For smooth and comprehensive implementation, it would also be advisable to have clear guidance for all CTIs and any entities providing networks or services which may be notified as CTIs to understand the framework for compliance. This would greatly help service providers, new entrants to the market, and the public at large as to their obligations and protections. A comprehensive picture of security standards and measures required to be put in place, and by whom, would also aid research by independent security experts whose inputs can help strengthen protection of CTI.

We recommend that a Central Government authority specifically empowered under the Act publish an annual notification of all networks declared as Critical Telecommunication Infrastructure, and make available for access all of the measures that any such declared network must take under the Rules.

2. **The Rules must not permit access to people's personal data.**

People's personal data, which is protected under the Digital Personal Data Protection Act, 2023 (DPDPA), and other laws, must not be accessed by any entity including the Central Government through the data access provisions in the draft rules. General provisions for access to data must not be misused to bypass the rigour of procedures under other laws, including but not limited to the rules for interception under the Act.

Specifically, personal data must never be accessed through the following (not an exhaustive list):

- Rule 3(2) which requires telecommunication entities to provide the Central Government "details" of their networks;
- Rule 5(1) which permits the Central Government to "access and inspect hardware, software and data"; and
- Rule 6(h) which requires the CTI through its Chief Telecommunication Security Officer to provide "All logs relating to critical telecommunication infrastructure".

We recommend that the Rules clearly state that personal data as defined in the DPDPA will not be accessed through the Rules; and that a formal, transparent procedure be put in place to ensure any powers of access and inspection are exercised only through written requests.

3. **Obligations related to CTIs and additional obligations which can be included for greater transparency and security — Rule 7.**

We welcome the requirements in Rule 7, particularly the obligation to ensure that "vulnerability/ threat/ risk analysis for telecommunication network architecture" of CTIs is required annually or at a greater frequency. It is important to ensure that security researchers are not penalised for identifying and responsibly disclosing such vulnerabilities so that they can continue to provide important contributions to the overall security of networks in India.

We recommend that CTIs should have procedures in place for reporting and identifying vulnerabilities so that independent researchers and experts can responsibly disclose them as to possible threats with legal certainty that they would not be unjustly harassed with threats of liability under the Act or other laws. This will help with strengthening CTI and the overall cybersecurity infrastructure of the country.

Provisions for disclosure should be included so that in case of a security incident, there is clear guidance as to notification of the government as well as impacted persons. In some cases, notification of impacted individuals may be required after a vulnerability has been patched. We recommend that clear provisions for disclosure to the general public should be included, including for changes to CTIs of which people using them should be aware.

We recommend that the rules incorporate clear timelines and mandates for impacted individuals and the general public to be informed about security incidents and vulnerabilities relating to CTIs.

Summary of suggestions

We recognise that the Rules deal with technologies and standards which are subject to change and evolve, and therefore the consultation and open communication process must not end with the publication of these Rules. Sustained multi-stakeholder dialogues must

continue to evaluate the effectiveness, relevance, and necessary improvements of measures and standards under the Rules and the Act.

S. No.	Rule/ provision	Recommendation
1.	General recommendation	We recommend that Section 22(3) of the Act be amended and include a clear mechanism, involving consultation, to notify any network as Critical Telecommunication Infrastructure; and specific grounds on which such a decision can be made. A draft amendment to this effect should be published for input and comments.
2.	General recommendation	We recommend that a Central Government authority specifically empowered under the Act publish an annual notification of all networks declared as Critical Telecommunication Infrastructure, and make available for access all of the measures that any such declared network must take under the Rules.
3.	Rule 3(2), Rule 5(1), Rule 6(h), and generally applicable	We recommend that the Rules clearly state that personal data as defined in the DPDPA will not be accessed through the Rules; and that a formal, transparent procedure be put in place to ensure any powers of access and inspection are exercised only through written requests.
4.	Rule 7 - obligations relating to critical telecommunication infrastructure.	We recommend that CTIs should have procedures in place for reporting and identifying vulnerabilities so that independent researchers and experts can responsibly disclose them as to possible threats with legal certainty that they would not be unjustly harassed with threats of liability under the Act or other laws. This will help with strengthening CTI and the overall cybersecurity infrastructure of the country.

S. No.	Rule/ provision	Recommendation
5.	Rule 7 - obligations relating to critical telecommunication infrastructure.	We recommend that the rules incorporate clear timelines and mandates for impacted individuals and the general public to be informed about security incidents and vulnerabilities relating to CTIs.

We thank you for the opportunity to participate in this consultation. We hope that the Ministry will undertake further public consultation after review of initial comments from all stakeholders, including through public meetings. We remain available for any clarification or queries in relation to this feedback, and any other further assistance.

Yours sincerely,

Shruti Narayan
Asia Pacific Policy Counsel
shruti@accessnow.org

Namrata Maheshwari
Senior Policy Counsel and Encryption Policy Lead
namrata@accessnow.org

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org

Access Now | https://www.accessnow.org