Registry No. DL- 33004/99

REGD.No.DL-33004/99

भारत का राजपत्र
The Gazette of India

CG-DL-A-29082024-256727
xxxGIDHxxx
CG-DL-E-29082024-256727
xxxORDExxx

Extraordinary
EXTRAORDINARY

Part II—Section 3—Sub-Section **(i)**
PART II—Section 3—Sub-section (i)

published with authority
PUBLISHED BY AUTHORITY

[No. **481]** New Delhi, Wednesday, August **28, 2024/** Bhadra **6, 1946**

No. 481] NEW DELHI, WEDNESDAY, AUGUST 28, 2024/ BHADRA 6, 1946

Ministry of Communications

(Department of

Telecommunications) NOTIFICATION New Delhi, the 28th August, 2024

G.S.R. 520(E).—The following draft rules which the Central Government proposes to make in exercise of the powers conferred by sub-section (1) of section 22 read with clause (v) of sub-section (2) of section 56 of the Telecommunication Act, 2023 (44 of 2023) are hereby published for the information of all the persons affected thereby and notice is hereby given that the said draft rules will be taken into consideration after the expiry of a period of thirty days from the date on which copies of this notification, as published in the Official Gazette, are made available to the general public;

If there are any objections or suggestions, please contact Joint Secretary (Telecom), Department of Telecommunication, Ministry of Communications, India may be sent to Govt., Sanchar Bhawan, 20, Ashok Road, New Delhi- 110001;

Any objections or suggestions received from any person with respect to the said draft rules before the expiry of the aforesaid period will be considered by the Central Government.

1. Short title, commencement and scope (1) These

rules may be called the Telecommunications (Telecommunication Cyber Security) Rules, 2024.

(2) These shall come into force from the date of their publication in the Official Gazette.

(3) These rules shall supersede the Prevention of Tampering of Mobile Device Equipment Identification Number Rules, 2017 and the Mobile Device Equipment Identification Number (Amendment) Rules, 2022 under the Indian Telegraph Act, 1885 (13 of 1885) but shall not affect the terms and conditions of action taken under those rules including registrations made under those rules.

2. Definitions

(1) In these rules, unless the context otherwise requires,

(a) “Act” means the Telecommunications Act, 2023 (44 of 2023);

(b) “Chief Telecom Security Officer” means a designated employee of a telecom entity appointed under rule 6 of these regulations. (c) “cyber

security of telecom networks and telecom services” or “telecom cyber security” means tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, assurances and technologies that can be used to protect telecom networks and telecom services as well as assets of persons including individuals from cyber threats; (d) “rules” means the Telecommunications (Telecommunication Cyber Security) Rules, 2024; (e) “security incident” means an event that has an actual or potential adverse effect on telecommunication cyber security; (f)

“telecommunication entity” means any entity authorized under sub-section (1) of

section 3 of this Act.

Authorised company means any person providing telecommunication services or establishing, operating, maintaining or expanding a telecommunication network, including a person exempted from the requirement of authorisation under sub-section (3) of section 3 of this Act.

(g) “telecommunications equipment identification number” means a telecommunications identifier consisting of one or more of the following

characteristics: i) International Mobile Equipment Identity (IMEI)

number; or ii) Electronic Serial Number

(ESN); or iii) any other number or symbol that identifies a unique telecommunications device.

(b) “linear data” means any data generated, transmitted, received or stored over a telecommunications network, including data related to the type, routing, duration or timing of the telecommunications.

(2) Words and expressions used in these rules and not defined

But things which are defined in the Act shall have meanings not specified in the Act.

Has gone.

3. Data collection, metering and analysis (1)

The Central Government or any agency authorised by the Central Government in this behalf may, for security purposes and for telecommunication

in order to ensure cyber security; (a)

requisition radar data and any other data from the telecom entity in such form and manner as may be notified by the Central Government for this purpose; or

(b) direct any telecom entity to collect and make available such data from a specified point and to establish necessary infrastructure and equipment to enable its processing and storage.

"(2) The data collected under sub-rule (1) may be analysed for taking measures to enhance telecom cyber security and if the Central Government determines to do so for security purposes and to ensure telecom cyber security, it may, by notification, take such measures as may be specified in the Government of India Act, 1961."

(a) disseminate it to any agency of the Central Government involved in law enforcement and security-related activities; and

(b) may be shared with telecommunications entities or users;

(3) The Central Government and any agency authorised by the Central Government to collect data under these regulations as well as the persons with whom such data is shared under sub-rule (2) shall implement adequate security measures, including any specific security measures as notified by the Central Government, for the purpose of preventing any unauthorised access to such data.

(4) The data collected under these regulations shall be used or disclosed for the purpose of ensuring telecom cyber security.

1. No such use shall be made for any other purpose other than this.

4. Obligations relating to telecommunications cyber security

(1) No person shall endanger telecommunication cyber security. (2) No message

shall be sent using a telecommunication network or telecommunication service which is a breach of telecommunication cyber security. would have an adverse effect on safety.

(3) Without prejudice to the generality of sub-rules (1) and (2), no person shall use any telecommunication equipment or telecommunication identifier or telecommunication network or telecommunication services for the purpose of--(a) for fraud, cheating or impersonation;

(b) transmit any message which is based on

fraud;

(c) shall not cause or intend to cause any security event, or (d) shall not be used for any other use which is contrary to

any provision of any law for the time being in force.

(4) The Central Government may, from time to time, issue directions and standards for preventing misuse of telecom identity cards or telecom networks or telecom services in order to ensure telecom cyber security, which shall be binding on all persons to whom it is applicable.

(5) Every telecom company shall comply with the following measures to ensure telecom cyber security, namely:-

(a) adopt a telecom

cyber security policy, which shall include the following aspects:

(i) Security measures, risk management approaches, practices, training, best practices and technologies for enhancing telecom cyber security;

(ii) telecommunication network testing, including hardening, vulnerability assessment and penetration testing;

(iii) risk assessment, identification and prevention of security incidents; (iv)

rapid action systems to deal with security incidents, including mitigation measures to limit the impact of such incidents;

(v) Forensic analysis of security incidents to ensure learnings from such incidents and to further strengthen telecom cyber security;

(b) recommend to the Central Government the adoption of such policy under sub-section (a) as may be specified for the purpose;

(c) Identifying and mitigating the risks of security incidents and ensuring timely response to such incidents;

(d) take appropriate action to resolve security incidents, and minimise their impact;

(e) ensure implementation of guidelines and standards issued by the Central Government;

(f) conduct periodic telecom cyber security audits to assess the resilience of telecom cyber security to threats, both through its own mechanism and through a certified agency designated by the Central Government for the purpose;

(g) giving timely information to the Central Government or any officer authorised by the Central Government in this behalf, of any security incident, and the steps taken to deal with such incidents, in the manner specified in rule 7;

(b) establish facilities like Security Operations Centre (SOC) by the Central Government, either on its own or in collaboration with other telecom companies, within a specified time frame to address the following: to do

(i) Telecom cyber security incidents, attempts, intrusions, breaches and disruptions in telecom service or Monitoring misuse of telecom networks;

(ii) maintain records of threat actors affecting its telecommunications service, or telecommunications network; (iii) maintain operation and maintenance command logs;

(iv) maintaining logs of the SOC (firewall, intrusion detection system (IDS) or intrusion prevention system (IPS), or security information and event management (SIEM) or other such solutions);

(v) maintaining logs of telecommunication services or elements comprising the telecommunication network or any other element necessary for the security of the telecommunication service or the telecommunication network Keep;

(vi) maintain all records, or logs, specified herein for such period as may be specified by the Central Government and make the same available to such agency or person as may be authorised by the Central Government;

(vii) Rendering necessary assistance to any agency or person authorised by the Central Government or law enforcement agencies for the purpose of investigation relating to security incidents.

5. Measures to protect and ensure telecom cyber security

(1) The Central Government may establish digital and other mechanisms as it may consider necessary to enable any person and other stakeholders to identify and report any activity that threatens telecom cyber security, including acts listed under sub-rule (3) of rule 4.

(2) The Central Government shall, after prima facie scrutiny of the information received under sub-rule (1), identify the telecom identifier whose use is alleged to have caused threat to telecom cyber security and identify the person to whom such telecom identifier has been issued by the telecom company and issue a notice to such person along with the details thereof.

(3) The person to whom a notice is issued under sub-rule (2) shall, within seven (7) calendar days of the receipt of such notice, send a written reply to the Central Government and if within that period, any If no reply is received, the Central Government shall take action to issue an order under sub-rule (5).

(4) If a reply is received on the receipt of a notice under sub-rule (2) within the time specified therein, the Central Government shall, after giving such person a reasonable opportunity of being heard, pass such order as it may deem fit under sub-rule (5).

"(5) The Central Government shall, on the basis of its assessment of the facts and the submissions, if any, made by the person to whom notice has been issued under sub-rule (2), pass an order with reasons, which may include directions to the telecom company:

(K) temporarily suspend the use of the relevant telecom identifier for the purpose of providing telecom services in such manner and for such period as the Central Government may, specified by the Government, or

(b) may terminate the use of the relevant telecom identifier for providing telecom services.

(6) Notwithstanding anything contained in sub-rule (2), if the Central Government considers that immediate action under sub-rule (5) is necessary or expedient in the public interest, no notice shall be required and in such circumstances, it shall pass an order stating the reasons therefor giving appropriate directions to the telecom company to temporarily suspend the use of the relevant telecom identifier for the purpose of providing telecom services.

(7) A copy of the order under sub-rule (5) or sub-rule (6) shall be supplied to the person affected by such order and such person may, within a period of thirty (30) calendar days from the date of its issue, represent in writing to the Central Government the reasons why such action should not be taken. The Central Government may, after giving such person a reasonable opportunity of being heard, for reasons to be recorded in writing, grant leave to maintain or cancel the order passed under sub-rule (5) or sub-rule (6) Any amendment of the order under sub-rule (6) may also include an order directing the telecom company to cease the use of the relevant telecom identifier for the purpose of providing telecom services specified under clause (b) of sub-rule (5).

(8) Any order of suspension or termination of telecom service under sub-rule (5), sub-rule (6) and sub-rule (7) may also be applied to other telecom equipment or telecom identifier associated with the person whose telecom identifier has been identified under sub-rule (2) or to other telecom identifiers issued to the person identified under sub-rule (2).

(9) The Central Government may maintain repository of persons and telecom identifiers who have been taken action against pursuant to orders under sub-rule (5) or sub-rule (6) or sub-rule (7) or sub-rule (8) and direct telecom companies to prohibit or restrict access to telecom services to such persons for a period not exceeding three (3) years from the date of such order.

(10) The Central Government may, if it considers necessary, share the list of telecom identifiers taken action against pursuant to orders under sub-rule (5) or sub-rule (6) or sub-rule (7) or sub-rule (8) with other persons providing services using telecom identifiers and may also direct such persons to provide such information as may be required for identification of their subscribers or for their personal use.

Restrict or restrict the use of such telecom identifiers for delivery of services as may be specified.

(11) No telecom identifier which is the subject of suspension or termination of telecom service in accordance with this Act shall be re-assigned to another person for a period of one (1) year from the date of issue of such order which may be extended to three (3) years in exceptional cases.

6. Chief Telecom Security Officer

(1) Every telecom company shall appoint a Chief Telecom Security Officer whose details shall be provided to the Central Government in writing in such form as may be specified for the purpose. Any replacement or change in the position of such officer shall be immediately notified to the Central Government in such form as may be specified.

(2) The Chief Telecom Security Officer shall be a citizen and resident of India and shall be a Director of a telecom company.

The person responsible for this office shall be accountable to the Board or similar governing body.

(3) The Chief Telecom Security Officer shall be responsible for coordinating with the Central Government for the implementation of these rules, including compliance with the following:- Any reporting requirement under these rules including security incidents under rule 7.

7. Reporting of Security Incidents

(1) On the occurrence of a security incident affecting a telecommunication entity, such entity shall, within six (6) hours of such incident, make an application to the Central Government in the form and manner specified for the purpose, shall report this to the extent applicable, including providing the following information (a) the

number of users affected by the safety incident;

(b) the duration of the security incident;

(c) the geographical area affected by the security incident;

(d) the extent to which the functioning of the telecommunication network or telecommunication service is affected;

(e) the extent of impact on economic and social activities; and

(f) the corrective measures taken or proposed to be taken

(2) The Central Government may, where it determines that disclosure of a security incident is in the public interest, inform the public about such security incident or require the affected telecom company to do so.

(3) The Central Government may require a disbursed telecommunications company to provide:

(a) information necessary to assess the security of such telecom network and telecom services, including telecom cyber security measures;

(b) security audit by an agency certified by the Central Government, at the cost of such telecom company, in the manner specified for the purpose.

(4) The Central Government may issue directions containing measures necessary to avert a security incident or to prevent the occurrence of a significant threat when it is identified and specify time limits for implementation of such directions by the affected telecom entity.

8. Liability in respect of telecommunications identity card and telecommunications

equipment (1) The manufacturer of the equipment which has the Internet Mobile Identity (IMEI) number,
The IMEI number of such device manufactured in India shall be registered with the Central Government in the form specified for such purpose before the first sale of such device.

(2) The importer of telecommunication equipment having IMEI number, shall get the IMEI number of such equipment imported into India for sale, testing, research or any other purpose registered with the Central Government in the form specified for such purpose before import of such equipment into India.

(3) No person shall—

(a) intentionally deletes, freezes, alters or alters the Unique Telecommunications Equipment Identification Number; or

(b) does not knowingly use, produce, transport, control or possess or interfere with any telecom identity card or any hardware or software relating to the telecom equipment, knowing that it has been configured as specified above. (4) The Central Government may

issue directions to the manufacturers of telecom equipment having IMEI number to provide such assistance as may be required in respect of the imported telecom equipment or IMEI number.

(5) The Central Government may issue directions to telecom companies to stop the use of telecom equipment having impersonated IMEI numbers in the telecom network or while providing telecom services.

9. Digital implementation of these rules

The Central Government may specify appropriate means for digital implementation of these rules, including the following

(a) collection, sharing and analysis of linear data,

(b) Issue notice and submit response under Rule 5. (c) Maintain

repository of individuals and telecom identities of persons who have Any action has been taken under Rule 5 of the

(d) said Act. Issuing directions, standards for prevention of misuse of telecom identity or telecom network or telecom services.

(e) Submission of telecom cyber security policy by the telecom company to the Central Government.

(f) Reporting of security incidents by the telecom company, including providing any additional information.

(g) Registration of IMEI number of equipment manufactured in or imported into India and

(ÿ) prohibition of use of telecom equipment having foreign IMEI numbers.

[I.No. 24-05/2024-UBB]

Devendra Kumar Rai, Joint Secretary

MINISTRY OF COMMUNICATIONS

(Department of Telecommunications)

NOTIFICATION

New Delhi, the 28th August, 2024

G.S.R. 520(E).—The following draft rules, which the Central Government proposes to make in exercise of the powers conferred under sub-section (1) of section 22, read with clause (v) to sub-section (2) of section 56 of the Telecommunications Act, 2023 (44 of 2023), are hereby published for the information of all persons likely to be affected thereby and notice is hereby given that the said draft rules shall be taken into consideration after the expiry of

a period of thirty days from the date on which copies of this notification as published in the Official Gazette, are made available to the public;

Objections or suggestions, if any, may be addressed to the Joint Secretary (Telecom), Department of Telecommunications, Ministry of Communications, Government of India, Sanchar Bhawan, 20, Ashoka Road, New Delhi- 110001;

The objections or suggestions which may be received from any person with respect to the said draft rules before the expiry of the aforesaid period shall be taken into consideration by the Central Government.

1. Short title, commencement, and savings

These rules may be called the Telecommunications (Telecom Cyber Security) Rules, 2024.

(1) They shall come into force on the date of their publication in the Official Gazette.

(2) These rules shall be in supersession of the Prevention of Tampering of the Mobile Device Equipment Identification Number Rules, 2017 and the Mobile Device Equipment Identification Number (Amendment) Rules, 2022 under the Indian Telegraph Act, 1885 (13 of 1885), but shall not override the terms and conditions of actions taken under those rules, including registrations undertaken pursuant to those rules.

2. Definitions

(1) In these rules, unless the context otherwise requires:

(a) **"Act"** means the Telecommunications Act, 2023 (44 of 2023);

(b) **"Chief Telecommunication Security Officer"** means the designated employee of a telecommunication entity, appointed under rule 6 of these rules;

(c) **"cyber security of telecommunication networks and telecommunication services"** or **"telecom cyber security"** refers to tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, assurance and technologies that can be used to safeguard telecommunication networks and telecommunication services, as well as assets of persons, including connected telecommunication equipment, telecommunication services, personnel, infrastructure, applications, and the totality of transmitted and/or stored information, against relevant security risks in the cyber environment;

(d) **"rules"** means the Telecommunications (Telecom Cyber Security) Rules, 2024;

(e) **"security incident"** means an event having actual or potential adverse effect on telecom cyber security;

(f) **"telecommunication entity"** means any person providing telecommunication services, or establishing, operating, maintaining, or expanding telecommunication network, including an authorised entity holding an authorisation under sub-section (1) of section 3 of the Act, or a person exempted from the requirement of authorisation under sub-section (3) of section 3 of the Act

(g) **"telecommunication equipment identification number"** means a telecommunication identifier bearing one or more of the following characteristics:

(i) international mobile equipment identity (IMEI) number; or

(ii) electronic serial number (ESN); or

(iii) any other number or signal that identifies a unique telecommunication equipment.

(h) **"traffic data"** means any data generated, transmitted, received or stored in telecommunication networks, including data relating to the type, routing, duration or time of a telecommunication.

(2) Words and expressions used in these rules and not defined herein but defined in the Act, shall have the meaning assigned to them in the Act.

3. Collection, sharing and analysis of data

(1) The Central Government, or any agency authorised in this behalf by the Central Government, may, for the purposes of protecting and ensuring telecom cyber security:

(a) seek from a telecommunication entity, traffic data and any other data in the form and manner as notified by the Central Government for this purpose; or

(b) direct a telecommunication entity to establish necessary infrastructure and equipment for collection and provision of such data from designated points to enable its processing and storage.

(2) The data collected under sub-rule (1) may be analysed for taking measures to enhance telecom cyber security, and may, if so determined by the Central Government as necessary for protecting and ensuring telecom cyber security, be:

(a) disseminated to any agency of the Central Government engaged in law enforcement and security related activities; and

(b) shared with telecommunication entities or users.

(3) The Central Government and any agency authorised by the Central Government to collect data under these rules, as well as persons with whom such data is shared under sub-rule (2), shall put in place adequate safeguards, including any specific safeguards as may be notified by the Central Government for this purpose, to prevent any unauthorised access to such data.

(4) The data collected under these rules shall not be used or disclosed for any other purpose, except for ensuring telecom cyber security.

4. Obligations relating to telecom cyber security

(1) No person shall endanger telecom cyber security.

(2) No message shall be sent using telecommunication network or telecommunication service which adversely affects telecom cyber security.

(3) Without prejudice to the generality of sub-rule (1) and sub-rule (2), no person shall use telecommunication equipment or telecommunication identifier or telecommunication network, or telecommunication services, including through:

(a) fraud, cheating or personation;

(b) transmitting any message which is fraudulent;

(c) committing or intending to commit any security incident; or

(d) engaging in any other use which is contrary to any provision of any law for the time being in force.

(4) The Central Government may, from time to time, issue directions and standards for the prevention of misuse of telecommunication identifiers or telecommunication network or telecommunication services for ensuring telecom cyber security, which shall be binding on all persons on which it is applicable.

(5) Each telecommunication entity shall ensure compliance with the following measures to ensure telecom cyber security:

(a) adopt a telecom cyber security policy, which shall include:

(i) security safeguards, risk management approaches, actions, training, best practices, and technologies, to enhance telecom cyber security;

(ii) telecommunication network testing, including hardening, vulnerability assessment and penetration testing;

(iii) risk assessment, identification, and prevention of security incidents;

(iv) rapid action system to deal with security incidents, including mitigation measures to limit the impact of such incidents;

(in) forensic analysis of security incidents, to ensure learnings from such incidents and further strengthening telecom cyber security;

(b) confirm to the Central Government on the adoption of such policy as outlined under sub-paragraph (a), in the manner as may be specified for this purpose;

(c) identify and reduce the risks of security incidents and ensure timely responses to such incidents;

(d) take appropriate action for addressing security incidents, and mitigate their impact;

(e) ensure implementation of directions and standards as issued by the Central Government;

(f) conduct periodic telecom cyber security audits through its own mechanisms to assess resilience to threats to telecom cyber security, and through the certified agency as specified by the Central Government for this purpose;

(g) promptly report any security incident to the Central Government, or any officer authorised on this behalf by the Central Government, and measures taken to address such incidents in the manner specified in rule 7;

(h) establish facilities such as Security Operations Centre (SOC), by itself or in collaboration with other telecommunication entities, within the time period as specified by the Central Government, to address the following:

(i) monitor telecom cyber security incidents, attempts, intrusions, breaches and misuse of telecommunication service or telecommunication network;

(ii) maintain details of threat actors impacting its telecommunication service, or telecommunication network;

(iii) maintain command logs of operation and maintenance;

(iv) maintain logs of SOC (firewall, Intrusion Detection System (IDS) or Intrusion Prevention System (IPS), or Security Information and Event Management (SIEM) or other such solution);

(v) maintain logs of elements involved in telecommunication services, or telecommunication network or any other element required for security of telecommunications service or telecommunications network;

(vi) maintain all records or logs specified herein, for a period as specified by the Central Government and make available to the agency or person authorized by the Central Government;

(vii) provide necessary support to the agency or person authorized by the Central Government or the law enforcement agencies for the purpose of investigation related to security incidents.

5. Measures to protect and ensure telecom cyber security

(1) The Central Government may put in place digital and other mechanisms as it may consider necessary to identify, or for enabling any person and other stakeholders to identify and report any act that endangers telecom cyber security, including through actions listed under sub-rule (3) of rule 4.

(2) The Central Government shall, after a prima facie examination of the information received under sub-rule (1), identify the telecommunication identifier, the use of which is alleged to have endangered telecom cyber security and the person to whom such telecommunication identifier has been issued by the telecommunication entity, and issue a notice to such person, with details thereof.

(3) The person to whom notice is issued under sub-rule (2), shall send a written response to the Central Government, within seven (7) calendar days of receipt of such notice, and if no response is received within such period, the Central Government shall proceed to issue an order under sub-rule (5).

(4) If a response is received from the recipient of the notice under sub-rule (2) within the time specified therein, the Central Government shall, after giving such person a reasonable opportunity of being heard, make an order thereon as it thinks fit under sub-rule (5).

(5) The Central Government shall, based on its assessment of facts and submissions, if any, made by the person to whom notice is issued under sub-rule (2), pass an order, with reasons, which may include directions to the telecommunication entity to:

(a) temporarily suspend use of the relevant telecommunication identifier for the purpose of providing telecommunication services, in the manner and for a duration as may be specified by the Central Government, or

(b) terminate the use of the relevant telecommunication identifier for providing telecommunication services.

(6) Notwithstanding anything stated in sub-rule (2), no notice shall be required if the Central Government considers that immediate action under sub-rule (5) is necessary or expedient in the public interest, and in such circumstances, it shall pass an order recording the reasons therefor, with appropriate directions to the telecommunication entity to temporarily suspend use of the relevant telecommunication identifier for the purpose of providing telecommunication services.

(7) The copy of the order under sub-rule (5) or sub-rule (6) shall be provided to the person affected by such order, and such person, may, within a period of thirty (30) calendar days from the date of issuance thereof, represent to the Central Government in writing, with reasons why such action should not be

taken. The Central Government shall, after giving such person a reasonable opportunity of being heard, pass an order, either upholding or modifying or revoking the order passed under sub-rule (5) or sub-rule (6), for reasons to be recorded in writing. Any modification of the order under sub-rule (6) may also include an order directing the telecommunication entity to terminate the use of the relevant telecommunication identifier for the purpose of providing telecommunication services as specified under clause (b) of sub-rule (5).

(8) Any order of suspension or termination of telecommunication service under sub-rule (5), sub-rule (6) and sub rule (7) may also be extended to the other telecommunication equipment or telecommunication identifier linked to the person whose telecommunication identifier has been identified under sub-rule (2) or other telecommunication identifier issued to the person identified under sub-rule (2).

(9) The Central Government may maintain a repository of persons and telecommunication identifiers which have been acted upon pursuant to the orders under sub-rule (5) or sub-rule (6) or sub-rule (7) or sub-rule (8), and may direct telecommunication entities, to prohibit or limit the access to telecommunication services to such persons for a period not exceeding three (3) years from the date of such order.

(10) The Central Government may, if it considers necessary, share the list of telecommunication identifiers that have been acted upon pursuant to orders under sub-rule (5) or sub-rule (6) or sub-rule (7) or sub-rule (8), with other persons providing services using the telecommunication identifiers and direct such persons also to prohibit or circumscribe the use of such telecommunication identifiers for identification of their customers or for delivery of their services, in the manner as may be specified.

(11) Any telecommunication identifier which is the subject of suspension or termination of the telecommunication service pursuant this rule, shall not be reallocated to any other person for a period of one (1) year from the date of issuance of such order which may be extended upto three (3) years in specific cases.

6. Chief Telecommunication Security Officer

(1) Each telecommunication entity shall appoint a Chief Telecommunication Security Officer, whose details shall be provided in writing to the Central Government in the form as may be specified for this purpose.
Any replacement or change of such officer shall be promptly notified to the Central Government, in such form as may be specified.

(2) The Chief Telecommunication Security Officer shall be a citizen and resident of India, and responsible to the Board of Directors or similar governing body of the telecommunication entity.

(3) The Chief Telecommunication Security Officer shall be responsible for coordinating with the Central Government for the implementation of these rules, including compliance with any reporting requirements under these rules, including of security incidents under rule 7.

7. Reporting of security incidents

(1) On the occurrence of any security incident affecting a telecommunication entity, such entity shall report the same to the Central Government within six (6) hours of such occurrence in the form and manner specified for this purpose, including the furnishing of the following information as applicable:

(a) the number of users affected by the security incident;

(b) the duration of the security incident;

(c) the geographical area affected by the security incident;

(d) the extent to which the functioning of the telecommunication network or telecommunication service is affected;

(and) the extent of impact on economic and societal activities; and

(f) the remedial measures taken or proposed to be taken.

(2) The Central Government may, where it determines that disclosure of the security incident is in the public interest, inform the public of such security incident, or require the affected telecommunication entity to do so.

(3) The Central Government may require the affected telecommunication entity to:

(a) provide information needed to assess the security of such telecommunication network and telecommunication services, including telecom cyber security measures;

(b) carryout security audit by a certified agency as specified by the Central Government at the cost of such telecommunication entity, in the manner specified for this purpose.

(4) The Central Government may issue directions including for the measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and may specify the time-limits for implementation of such directions to the affected telecommunication entity.

8. Obligations relating to telecommunication identifier and telecommunication equipment

(1) A manufacturer of equipment that has international mobile equipment identity (IMEI) number, shall register such IMEI number of such equipment manufactured in India with the Central Government, prior to the first sale of such equipment, in the form as may be specified for such purpose.

(2) An importer of equipment that has an IMEI number, shall register such IMEI number of such equipment imported in India for sale, testing, research or any other purpose with the Central Government, prior to the import of such equipment into India, in the form as may be specified for such purpose.

(3) No person shall:

(a) intentionally remove, obliterate, change, or alter unique telecommunication equipment identification number; or

(b) intentionally use, produce, traffic in, have control or custody of, or possess hardware or software related to the telecommunication identifier or telecommunication equipment, knowing it has been configured as specified above.

(4) The Central Government may issue directions to manufacturers of telecommunication equipment bearing IMEI number to provide assistance as required in relation to tampered telecommunication equipment or IMEI number.

(5) The Central Government may issue directions to telecommunication entities to block the use of telecommunication equipment with tampered IMEI number in telecommunication networks or providing telecommunication services.

9. Digital implementation of these rules

The Central Government may specify appropriate means for the digital implementation of these rules, including for:

(a) collection, sharing and analysis of traffic data;

(b) issuance of notice and submission of response under rule 5;

(c) maintaining repository of persons and telecommunication identifiers against which any action has been taken under rule 5;

(d) issuance of directions and standards, for the prevention of misuse of telecommunication identifiers or telecommunication network or telecommunication services;

(e) submission of telecom cyber security policy by the telecommunication entity to the Central Government;

(f) reporting of security incidents by the telecommunication entity including any additional information to be provided;

(g) registration of IMEI number of equipment manufactured or imported in India; and

(h) blocking the use of telecommunication equipment with tampered IMEI numbers.

[F. No. 24-05/2024-UBB]

DEVENDRA KUMAR RAI, Jt. Secy.

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.