Draft Rules under section 69B of the Information Technology (Amendment) Act, 2008

Ministry of Communications and Information Technology
(Department of Information Technology)
New Delhi , Dated ------

G.S.R ---- In exercise of the powers conferred by clause (za) of sub-section (2) of section 87, read with sub-section (3) of section 69B of the Information Technology Act 2000, as amended by the Information Technology (Amendment) Act, 2008 (10 of 2009), the Central Government hereby makes the following rules, namely:

1. (1) These rules may be called the Information Technology (Monitoring and Collecting Traffic Data or information) Rules, 2009

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

2. Definitions. – In these Rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act 2000, as amended by the Information Technology (Amendment) Act, 2008;

(b) "Computer resource" means computer resource as defined in section 2(1)(k) of the Information Technology Act, 2000;

(c) "Cyber security incidents" means any real or suspected adverse event in relation to cyber security and incidents, an act of violating explicitly or implied security policy resulting in unauthorized access, denial of service/ disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization;

(d) "Cyber security breaches" means unauthorized acquisition by a person of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

(e) "Information" means information as defined in section 2(1)(v) of the Information Technology Act, 2000;

(f) "Information security practices" means implementation of security policies and standards in order to minimize the cyber security incidents and breaches;

(g) "Intermediary" means an intermediary as defined in section 2(1)(w) of the Information Technology (Amendment) Act, 2008;

(h) "Monitor" with its grammatical variations and cognate expressions, includes to view or inspect or record or collect traffic data or information by means of a monitoring device;

(i) “Monitoring device” means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or inspect or record or collect traffic data or information;

(j) “Port” or “Application Port” means a set of software rules which identifies and permits communication between application to application(s), network to network(s), computer to computer(s), computer system to computer system(s);

(k) “Review Committee” means a Review Committee as constituted in Rule 419A of Indian Telegraph (Amendment) Rules, 2007;

(l) “Traffic data” means traffic data as defined in *Explanation (ii)* attached to section 69B of the Information Technology (Amendment) Act, 2008.

3. Directions for monitoring and collecting traffic data or information generated, transmitted, received or stored in any computer resource under sub-section (3) of section 69B of the Information Technology (Amendment) Act, 2008 (hereinafter referred to as the said Act) shall not be issued except by an order made by the competent authority, who is, Secretary to the Government of India in the Department of Information Technology, Ministry of Communications & Information Technology.

4. The competent authority may issue directions for monitoring and collection of traffic data or information generated, transmitted, received or stored in any computer resource for any or all of the following purposes related to cyber security:

(a) forecasting of imminent cyber incidents;

(b) monitoring network application with traffic data or information on computer resource;

(c) identification and determination of viruses/computer contaminant;

(d) tracking cyber security breaches or cyber security incidents;

(e) tracking computer resource breaching cyber security or spreading virus/computer contaminants;

(f) identifying or tracking of any person who has contravened, or is suspected of having contravened or being likely to contravene cyber security;

(g) undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resource;

(h) accessing a stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;

(i) any other matter relating to cyber security.

5. The competent authority may authorize any agency of the government for monitoring and collection of traffic data or information generated, transmitted, received or stored in any computer resource.

6. No direction for monitoring and collection of traffic data or information generated, transmitted, received or stored in any computer resource shall be given for purposes other than those specified in Rule (4).

7. Any direction issued by the concerned competent authority under Rule (3) shall contain reasons for such direction and a copy of such direction shall be forwarded to the Review Committee within a period of seven working days.

8. The agency authorized by the competent authority under Rule (5) shall designate one or more nodal officers not below the rank of Deputy Secretary to the Government of India to authenticate and send the requisition conveying direction issued under Rule (5) to monitor and to collect traffic data or information to the designated officers of the concerned intermediaries or person in-charge of computer resources.

9. The monitoring and collection of traffic data or information so directed shall be the monitoring and collection of traffic data or information as is sent to or from any person or class of persons or relating to any particular subject whether such traffic data or information, or class of traffic data or information, are received with one or more computer resources specified in the direction, being a computer resource likely to be used for the generation, transmission, receiving, storing of traffic data or information from or to one particular person specified or described in the direction or one or many set of premises, specified or described in the direction.

10. The requisition shall specify the name and designation of the officer or the authority to whom the monitored or collected traffic data or information is to be disclosed.

11. The intermediaries or person in-charge of computer resource shall designate officers to receive requisition and to handle such requisition from the nodal officer for monitoring or collection of traffic data or information.

12. The requisition conveying directions for monitoring or collection of traffic data or information shall be conveyed to the designated officers of intermediaries or person in-charge of computer resources, in writing by the nodal officer designated under Rule (8) and delivered by an officer not below the rank of Under Secretary or officer of the equivalent rank.

13. The nodal officer issuing the requisition conveying directions for monitoring or collection of traffic data or information under Rule (5) shall also make a request in writing to the designated officers of intermediaries or person in-charge of computer resource for monitoring and collection of traffic data or information as per the format indicated in the requisition and report the same to the officer designated under Rule (10).

14. The nodal officer shall also make a request to the officers of intermediaries or person in-charge of computer resource designated under Rule (11) to extend all facilities, co-operation and assistance in installation, removal and testing of equipment and also enable online access or to secure and provide online access to the computer resource for monitoring and collecting traffic data or information mentioned in the directions.

15. On receipt of requisition conveying direction issued under Rule (3), the designated officer of the intermediaries or person in-charge of computer resources designated under Rule (11) shall acknowledge the requisition by way of letter/fax/ electronically signed email to nodal officer within two hours.

16. The officer of the intermediaries or person in-charge of computer resource designated under Rule (11) shall maintain proper records of the requisitions received by him.

17. The designated officers of the intermediaries or person in-charge of computer resources shall forward every fifteen days a list of requisition conveying direction for monitoring or collection of traffic data or information to the nodal officer. The list should include details such as the reference and date of requisition conveying direction of the concerned competent authority.

18. The intermediaries or person in-charge of computer resources shall put in place adequate and effective internal checks to ensure that unauthorised monitoring or collection of traffic data or information does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of monitoring or collection of traffic data or information as it affects privacy of citizens and also that this matter is handled only by the designated officers of the intermediary.

19. The intermediaries or person in-charge of computer resources are responsible for their respective actions of their employees also. In case of established violations

pertaining to maintenance of secrecy and confidentiality of information and unauthorised monitoring or collection of traffic data or information, action shall be taken against the intermediaries or person in-charge of computer resources under the relevant provisions of the laws of the country.

20. The Review Committee shall meet at least once in two months and record its findings whether the directions issued under Rule (5) are in accordance with the provisions of sub-section (3) of section 69B of the Act. When the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and order for destruction of the copies, including corresponding electronic record of the monitored or collected traffic data or information.

21. Records, including electronic records pertaining to such directions for monitoring and/or collection of traffic data shall be destroyed by designated officer after the expiry of nine months from receipt of direction or creation of record, whichever is later, unless these are, or likely to be, required for functional requirements.

22. The intermediaries or the person in-charge of computer resource shall destroy records pertaining to directions for monitoring and/or collection of information within six months of discontinuance of the monitoring and/or collection of traffic data and in doing so they shall maintain extreme secrecy.

23. Any person who intentionally, without authorisation under Rule (3) and Rule (5), monitors or collects traffic data or information, or attempts to monitor or collect traffic data or information, or authorises or assists any other person to monitor or collect traffic data or information in the course of its occurrence or transmission at any place within India, shall be proceeded against under the relevant provisions of the Law.

24. Any monitoring or collection of traffic data or information in computer resource by the employee of an intermediary or person in-charge of computer resource or a person duly authorised by the intermediary, undertaken in course of his duty relating to the services provided by that intermediary, shall not be unlawful, if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices, in connection with :

i) installation of computer resource or any equipment to be used with computer resource; or

ii) operation or maintenance of computer resource; or

iii) installation of any communication link or code either at the end of the intermediary or subscriber, or installation of user account on the computer resource of intermediary and testing of the same for its functionality;

iv) accessing stored information from computer resource relating to the installation, connection or maintenance of equipment, computer resource or a communication link or code; or

v) accessing stored information from computer resource for the purpose of:

(a) implementing information security practices in the computer resource;

(b) determining any security breaches, computer contaminant or computer virus;

(c) undertaking forensic of the concerned computer resource as a part of investigation or internal audit; or

vi) accessing or analysing information from a computer resource for the purpose of tracing a computer resource or any person who has contravened, or is suspected of having contravened or being likely to contravene, any provision of the Act that is likely to have an adverse impact on the services provided by the intermediary.

25. The details of monitored or collected traffic data or information shall not be used or disclosed by intermediary or any of its employees or person in-charge of computer resource to any person other than the intended recipient of the said information under Rule (10). Any intermediary or its employees or person in-charge of computer resource who contravenes these provisions shall be proceeded against under the relevant provisions of the Act.

26. The details of monitored or collected traffic data or information shall not be used or disclosed by the agency authorised under Rule (5) for any other purpose, except for forecasting imminent cyber threats or general trend of port-wise traffic on Internet, or general analysis of cyber incidents, or for investigation or in judicial proceedings before the competent Indian court.

27. Save as otherwise provided in Rule (26), strict confidentiality shall be maintained in respect of direction for monitoring or collection of traffic data or information issued by concerned competent authority under Rule (3) and nodal officers under Rule (8).