GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4342
TO BE ANSWERED ON: 26.03.2025

STRENGTHENING OF CYBER SECURITY LAWS

†4342. SMT. LOVELY ANAND:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the measures being taken by the Government to prevent cyber crimes;
(b) the number of villages provided with internet facility under the Digital India Campaign so far State-wise; and
(c) the steps taken by the Government strengthen cyber security laws?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (c):The policies of the Government are aimed at ensuring an open, safe, trusted and accountable Internet for its users. To help achieve this aim and to strengthen the mechanism to deal with cyber-crimes, including initiatives to strengthen cyber security infrastructure and laws in a comprehensive and coordinated manner, the Central Government has taken several steps: as following:

i. In the Government of India (Allocation of Business) Rules, 1961 (AoBR), Ministry of Electronics and Information Technology (MeitY) has been allocated the matters relating to Cyber Laws, administration of the Information Technology Act, 2000 (IT Act) and other IT related laws. Further, the AoBR has been amended on 27.09.2024 to streamline the cyber security posture of the country. Through this amendment, matters relating to security of telecom networks has been allocated to Department of Telecommunications (DoT), matters relating to Cyber Security as assigned in the Information Technology Act, and support to other Ministries / Departments on Cyber Security has been allocated to Ministry of Electronics and Information Technology (MeitY), matters related to cyber-crime has been allocated to Ministry of Home Affairs (MHA) and overall coordination and strategic direction for Cyber Security has been allocated to National Security Council Secretariat.

ii. In order to protect users in India and the Indian internet at large from the emerging harms, criminalities and such other associated risks posed by the misuse of technologies and to ensure accountability towards law of the land, MeitY constantly engages with and receives inputs from the public and stakeholders, including in respect of creation of new laws, strengthening & enforcement of existing laws and monitoring level of compliance. In this regard, the IT Act was notified in year 2000 and is being amended from time to time to safeguard users in the cyberspace. Further, the Digital Personal Data Protection Act, 2023 (DPDP Act) has been enacted which provides the framework for data protection.

iii. The IT Act defines several offences and provides for penalties and punishments for various cyber offences and data breaches such as penalty and compensation for damage to computer, computer system, etc., compensation for failure to protect data, punishment for tampering with computer source documents, punishment for computer related offences, punishment for identity theft, punishment for cheating by personation by using computer resource, cyber terrorism, and punishment for securing unauthorised access to protected system etc.

iv. The Indian Computer Emergency Response Team (CERT-In) has been established under IT Act as the Nodal Agency which perform functions in the area of cyber security such as collection, analysis and dissemination of information on cyber incidents, forecast and alerts of cyber security incidents, emergency measures for handling cyber security incidents, coordination of cyber incidents response activities, issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents for the incident response.

v. Additionally, CERT-In operates the Cyber Swachhta Kendra (CSK), a citizen-centric initiative to extend the vision of Swachh Bharat to the Cyber Space, providing botnet cleaning and malware analysis services. CSK helps detect malicious programs, provides free removal tools, and educates users on best cyber security practices. Furthermore, CERT-In runs an automated cyber threat intelligence exchange platform that proactively collects, analyzes, and shares tailored cyber threat alerts with organizations across sectors, enabling them to take preventive measures against emerging threats.

vi. The National Critical Information Infrastructure Protection Centre (NCIIPC) has been established under the IT Act as the national nodal agency in respect of Critical Information Infrastructure Protection. NCIIPC is responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

vii. With regard to the protection of personal data, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 has been notified prescribing reasonable security practices and procedures on the sensitive personal data or information. Further, the DPDP Act mandates Data Fiduciaries to implement security safeguards as well as robust technical and organisational measures while processing the digital personal data. It holds Data Fiduciaries accountable for any personal data breach or other violations of the law. The Data Protection Board ensures this accountability by adjudicating breaches and imposing financial penalties for non-compliance.

viii. Further, DoT has notified Telecommunications (Telecom Cyber Security) Rules, 2024 and Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024 under the Telecommunications Act, 2023, to provide for measures for addressing the cyber- attacks and ensuring cyber security of Telecom infrastructure.

ix. DoT has launched Sanchar Saathi portal as a citizen-centric initiative to empower mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives of the Government. The portal facilitates reporting of suspected fraud communications, requesting the blocking and tracing of stolen or lost mobile handsets, checking the genuineness of mobile handset, and reporting international calls that falsely display an Indian telephone number as calling line identification.

x. DoT has developed a system to detect fraudulent mobile connections obtained using fake or forged documents. Additionally, an online Digital Intelligence Platform (DIP) has been launched to facilitate the sharing of information related to the misuse of telecom resources and disconnected numbers with stakeholders to prevent cyber-crimes and financial frauds. To curb international spoofed calls falsely displaying Indian mobile numbers, DoT and TSPs have devised a system to identify and block such calls, which are often exploited by cyber-criminals for fraud and impersonation.

xi. MHA has set up the ‘Indian Cyber Crime Coordination Centre’ (I4C) as an attached office to deal with all types of cyber-crimes in the country. As part of I4C, the NCRP (https://cybercrime.gov.in) has been launched to enable the public to report cyber-crime incidents. As ‘Police’ and ‘Public Order’ are State subjects as per the Seventh Schedule of the Constitution of India, States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber-crime, through their Law Enforcement Agencies (LEAs).

xii. The Massive Open Online Courses (MOOC) platform, namely ‘CyTrain’ portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber-crime investigation, forensics, prosecution etc. Furthermore, I4C has launched a Suspect Registry of cyber criminals in collaboration with Banks and Financial Institutions, strengthening efforts to track and prevent cyber fraud.

xiii. The State-wise statistics on the number of villages with Mobile Internet coverage is at **Annexure-I.**

****

Annexure-I

State/UT wise Village Mobile Internet coverage Status as on 31-12-2024

Sr No	State / UT	Mobile Internet covered out of list 6,44,131 villages
1.	Andaman & Nicobar Islands	389
2.	Andhra Pradesh	16285
3.	Arunachal Pradesh	4141
4.	Assam	25969
5.	Bihar	44781
6.	Chandigarh	0
7.	Chhattisgarh	19123
8.	Dadra & Nagar Haveli and Daman & Diu	95
9.	Goa	344
10.	Gujarat	17932
11.	Haryana	6640
12.	Himachal Pradesh	20112
13.	Jammu and Kashmir	6062
14.	Jharkhand	31725
15.	Karnataka	29134
16.	Kerala	1438
17.	Laddakh	225
18.	Lakshadweep	23
19	Madhya Pradesh	53899
20.	Maharashtra	41570
21.	Manipur	2211
22.	Meghalaya	6324
23.	Mizoram	740
24.	Nagaland	1202
25.	NCT of Delhi	55
26.	Odisha	48573
27.	Puducherry	96
28.	Punjab	12532
29.	Rajasthan	44389
30.	Sikkim	441
31.	Tamil Nadu	16424
32.	Telangana	9964
33.	Tripura	702
34.	Uttar Pradesh	105461
35.	Uttarakhand	15901
36.	West Bengal	40951
Total		**625853**

******