GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *304
TO BE ANSWERED ON: 28.03.2025

PROTECTING CRITICAL INFRASTRUCTURE AND PRIVATE DATA AGAINST CYBER ATTACKS

***304. DR. ASHOK KUMAR MITTAL:**

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

(a) whether Government is aware of the increasing frequency and sophistication of cyberattacks in the country, if so, the reasons for the inadequate cybersecurity infrastructure to address these threats;
(b) the details of cybersecurity incidents reported in the last three years and the extent of data breaches caused by these attacks;
(c) whether Government has formulated a robust national cybersecurity strategy, if so, the reasons as to why it remains unimplemented; and
(d) the steps being taken to ensure accountability for protecting critical infrastructure and private data against cyber threats?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (d): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *304 FOR 28.03.2025, REGARDING PROTECTINGCRITICAL INFRASTRUCTURE AND PRIVATE DATA AGAINST CYBER ATTACKS

…….

(a) to (d):Government is cognizant of the increasing frequency and sophistication ofcyberattacks in the country. Government has taken several legal, technical, and administrative policy measures for addressing cyber security challenges in the country.The Government has also institutionalised a nationwide integrated and coordinated system to deal with cyber-attacks in the country which, inter alia, includes:

i. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordinationamongst different agencies.
ii. Under the provisions of section 70B of the Information Technology (IT) Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents.
iii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.
iv. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same. It also provides cyber security tips and best practices for citizens and organisations.
v. Ministry of Home Affairs (MHA) has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.
vi. Under the provisions of section 70A of the ITAct, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.

As per the information reported to and tracked by CERT-In, the total number of cyber security incidents in the last three years are given below:

Year	Total number of cyber security incidents
2022	13,91,457
2023	15,92,917
2024	20,41,360

The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users.National Cyber Security Policy (NCSP)was published by the Government with the vision of building a secure and resilient cyberspace for citizens, businesses and Government and a mission to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

Government has taken following stepsfor protecting critical infrastructure and private data against cyber threats, which, inter-alia, includes:

i. NCIIPC provides threat intelligence,situational awareness, alerts & advisoriesand information on vulnerabilities toorganisations having Critical InformationInfrastructures (CIIs)/ Protected Systems(PSs) for taking preventive measures against cyber-attacks and cyber terrorism. It alsoprovides all cyber security related advice tothese organisations, whenever asked for.Further, it follows up with concernedorganisations for compliance of the IT(Information Security Practices

&Procedures for Protected Systems) Rules,2018to improve their cyber security posture.It also organises training/awarenesssessions for employees of entities havingCIIs/PSs.

ii. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 ("SPDI Rules") made under section 43A of the IT Act has prescribed reasonable security practices and procedures to protect sensitive personal data of users.

iii. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021")under the IT Act prescribes that the intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the SPDI Rules.

iv. The Digital Personal Data Protection Act, 2023 (DPDPA) provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect their personal data and processing of personal data of individuals for lawful purposes by the Data Fiduciaries.

v. CERT-In issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

vi. CERT-In issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

vii. CERT-In has issued an advisory to various Ministries in November 2023 outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.

viii. CERT-In operates an automated cyber threat intelligence exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

ix. CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.

x. CERT-In has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

xi. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations and enhance resilience in Government and critical sectors. 109 such drills have so far been conducted by CERT-In where 1438 organizations from different States and sectors participated.

xii. CERT-In has empanelled 200 security auditing organisations to support and audit implementation of Information Security Best Practices.

xiii. CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks. A total of 12,014 officials have been trained in 23 training programs in 2024.

xiv. CERT-In regularly conducts various activities for awareness and citizen sensitization with respect to cyber-attacks and cyber frauds.

xv. The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Awareness material in the form of handbooks, short videos, posters, brochures, cartoon stories for children, advisories, etc. on various aspects of cyber hygiene & cyber security including deepfakes are disseminated through portals such as www.staysafeonline.in,www.infosecawareness.in and www.csk.gov.in.

****