GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 688
TO BE ANSWERED ON: 06.12.2023

CYBER SECURITY AND DATA PROTECTION

688. SHRIMATI MANJULATA MANDAL:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) the measures taken by the Government to create awareness among the public and private sectors about the importance of cyber security and data protection;
(b) whether Government is facing any challenges and gaps in implementing these measures and if so, the details thereof;
(c) whether the Government has formulated policies to address the increasing cyber security threats in the country; and
(d) if so, the details thereof including the proposed structure of the agencies?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. The Internet technology and Internet used to be seen as force for good, but in recent years, technology is also exploited for causing user harms and criminality.Government has taken the following measures to enhance awareness among organisations and users for safe usage of digital technologies and prevent cyber attacks:

(i) MeitY is implementing 'Information Security Education and Awareness' (ISEA) programme, which envisions capacity building, promotion of formal/non-formal education, training and creation of mass awareness in the area of Information Security in the country. The academic activities of the project are implemented through a network of 52 academic and training institutions across the country. Mass awareness programmes are conducted across schools, colleges and for senior citizen, women, Government officials and general public.
(ii) MeitY initiated the Cyber Surakshit Bharat (CSB) programme in public-private partnership to educate & enable the Chief Information Security Officers (CISOs) & broader IT community in Central/State Governments, Banks, PSUs and Government organizations to address the challenges of cyber security. The training programmes are conducted in cities like Delhi, Gurgaon, Mumbai, Kolkata, Bangalore, Hyderabad, Chennai, Chandigarh, Bhopal, etc.
(iii) MeitY conducts online awareness level and advanced level training courses in cyber security for officials of Central Government Ministries/Departments to create awareness about cyber security in Government employees
(iv) MeitY launched G20-Stay Safe Online Campaign in December 2022 during G20 presidency of India with an objective to raise awareness among citizens to stay safe in online world on the widespread use of social media platforms and rapid adoption of digital payments. The target groups of users are Children/ Students, Women, Senior Citizens, Teachers/ Faculty, General Public, Specially-abled and Government officials.

(v) MeitY conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.inand www.csk.gov.in.

(vi) CERT-In has issued an advisory to various Ministries/Departments 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.

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

(viii) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

(ix) 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.

(x) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 86 such drills have so far been conducted by CERT-In where 1159 organizations from different States and sectors participated.

(xi) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. A total of 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022. In 2023, up to October, a total of 7007 officials from Government, critical sectors, public and private sector were trained in 21 training programs in the area of cyber security.

(xii) CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Safer Internet Day on 7.2.2023 and Cyber Security Awareness Month in October 2023, by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with Centre for Development of Advanced Computing, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices, etc., through videos and quizzes on the MyGov platform.

(xiii) CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.

(xiv) Advocacy and awareness of Data Protection bill, the rights of citizens and the obligations of data fiduciaries were put forth on various forums.

(c) and (d): The Government has taken the following measures to address the increasing cyber security threats in the country:

(i) The Digital Personal Data Protection Act, 2023 (DPDPA), enacted on 11th August 2023, 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 for the data fiduciaries the need to process such personal data for lawful purposes.

(ii) National Cyber Security Policy (NCSP) 2013 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.

(iii) Ministry of Home Affairs has issued National Information Security Policy and Guidelines (NISPG) to the Central Ministries as well as State Governments and Union territories with the aim of preventing information security breaches and cyber intrusions in the information and communication technology infrastructure.

(iv) CERT-In issued directions relating to information security practices in April 2022 in exercise of powers under section 70B(6) of the Information Technology Act, 2000. These directions aim to enhance overall cyber security posture and ensure Safe & Trusted Internet in the country.

(v) CERT-In has 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.

(vi) A comprehensive framework for cybersecurity of government websites and applications was laid down in the Guidelines for Indian Government Websites and applications (GIGW), which are required to be followed while developing and hosting such websites and applications, and audited and certified for compliance.

(vii) MeitY has issued Guidelines for Cybersecurity Audit that cover both comprehensive and limited audit on periodic basis by competent auditors with clear responsibilities for ensuring such audit regularly, inclusive of vulnerability assessment and penetration testing.

(viii) The Government has following existing institutionalized structure to address cyber security threats in the country:

a. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for cyber security matters.

b. Under the provisions of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents.National Cyber Coordination Centre (NCCC), a multi-stakeholder project implemented by CERT-In under the Ministry of Electronics and Information Technology (MeitY), scans the cyberspace in the country at meta-data level to generate near real-time macroscopic views of the cyber security threats.

c. Ministry of Home Affairs (MHA) has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.

d. Under the provisions of section 70A of the Information Technology (IT) Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. NCIIPC provides near real-time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

e. Department of Telecommunications (DoT) has established Telecom Security Operations Centre (TSOC) for effective management of security incidents including prevention, identification and response system for national telecom infrastructure.

****