GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *47
TO BE ANSWERED ON: 26.7.2024

NEED FOR A NEW NATIONAL CYBERSECURITY POLICY

***47. SHRI S NIRANJAN REDDY:**

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

(a) whether Government has recognized the need for a new National Cybersecurity Policy/Strategy due to emerging technologies and evolving threats;

(b) the steps being taken to formulate and implement a new National Cybersecurity Policy/Strategy addressing current and future cybersecurity challenges, including Artificial Intelligence (AI) and other critical technologies;

(c) whether Government has considered revising such policies periodically to keep pace with the fast-evolving nature of technology; and

(d) the timeline for introducing and implementing a new National Cybersecurity Policy/Strategy, and the key areas it will focus on to ensure a secure digital environment in the country?

ANSWER

MINISTER OF 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. *47 FOR 26.7.2024, REGARDING NEED FOR A NEW NATIONAL CYBERSECURITY POLICY

(a) to (d): Yes, the Government is committed to ensure that the Internet in India is Open, Safe, Trusted and Accountable for its users, specially in view of the role of emerging technologies and evolving threats. 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 coordination amongst different agencies.
ii. 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.
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, and 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 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.

MeitY addresses key concerns in cybersecurity including those related to emerging and critical technologies, particularly in the field of AI, through a continuous process of research, analysis, formulation and issue of necessary instructions and guidelines based on emerging needs and challenges. The primary focus is on the three pillars of Securing national cyberspace, Strengthening existing structures comprising of people, processes and capabilities and Synergise resources for their optimal utilization to protect the Digital Environment in the country and to ensure secure and resilient cyberspace for all citizens.

****