

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1342
TO BE ANSWERED ON: 06.12.2024

STREAMLINING OF CYBER SECURITY SETUP

1342. SHRI YERRAM VENKATA SUBBA REDDY:

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

- (a) whether it is a fact that Government has streamlined the cyber security set up;
- (b) if so, the details thereof; and
- (c) to what extent this will be helpful to contain cyber frauds in the country?

ANSWER

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

(a) to (c): The Government is committed to ensure that the Internet in India is Open, Safe, Trusted and Accountable for its users. 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 security matters 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.

(vii) Government has made following rules to amend the Allocation of Business Rules (AoBR) vide notification dated 27th September, 2024 in order to streamline Cyber Security setup:

- Matters related to “Cyber Security as assigned in the Information Technology Act 2000 (21 of 2000) (as amended time to time) and support to other Ministries/Departments on Cyber Security” are assigned to Ministry of Electronics and Information Technology (MeitY).
- Matters related to “security of telecom networks” are assigned to Department of Telecommunications (DoT).
- Matters related to “Cyber Crime” are assigned to Ministry of Home Affairs (MHA).
- Matters related to “providing overall coordination and strategic direction for Cyber Security” are assigned to National Security Council Secretariat (NSCS)

By clearly assigning the responsibilities to various government bodies in cybersecurity, these rules create a more structured and cohesive approach to enhance cyber security including detection and mitigation of cyber frauds.
