GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION. NO. *213
TO BE ANSWERED ON: 17.12.2021

NATIONWIDE INTEGRATED SYSTEM FOR DEALING WITH CYBER ATTACKS

***213. SHRI SAMIR ORAON:**

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

(a) whether a nationwide integrated or co-ordinating system of the concerned Departments/Ministries has been developed to deal with cyber-attacks;

(b) if not, whether the requirement of the same is being felt;

(c) whether an effective technology has been developed to ward off these attacks; and

(d) whether an effective technology has been developed by the Ministry to prevent frauds through mobile phones which would identify such portals/persons/organizations and investigate them properly and take action under appropriate laws/sections?

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 REPLY TO RAJYA SABHA STARRED QUESTION NO. *213 FOR 17.12.2021 REGARDING NATIONWIDE INTEGRATED SYSTEM FOR DEALING WITH CYBER ATTACKS

……….

(a) and (b): The Government has 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) coordinates with different agencies at the national level for cyber security matters.

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) is a multi-stakeholder project and is implemented by the Indian Computer Emergency Response Team (CERT-In) under the Ministry of Electronics and Information Technology (MeitY). NCCC scans the cyberspace in the country at meta-data level to generate near real-time macroscopic views of the cyber security threats. NCCC provides a structured system and facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate the cyber security threats. Phase-I of NCCC has been made functional since July, 2017.

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

v. 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.

vi. 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.

(c): Government has taken several measures and deployed systems to prevent cyber-attacks:

i. CERT-In is operating 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.

ii. Government is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing free tools developed in collaboration with industry and research institutions for detection and removal of malicious code and securing computers and mobile devices.

iii. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.

iv. CERT-In has empanelled 96 security auditing organisations to support and audit implementation of Information Security Best Practices.

v. Cyber security mock drills are conducted regularly in Government and critical sectors. So far 61 such drills have been conducted by CERT-In where 600 organisations from different States and sectors have participated.

vi. 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. 15 and 17 training programs have been conducted covering 708 and 4801 participants during the year 2020 and 2021 (till October 2021) respectively.

vii. CERT-In co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

viii. Security tips have been published by CERT-In to enable users to secure their mobile/smart phones.

ix. Ministry of Electronics & Information Technology (MEITY) regularly conducts programs 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 like “www.infosecawareness.in”, and “www.cyberswachhtakendra.gov.in”.

(d): “Police” and “Public Order” are State subjects. MHA has launched National Cybercrime reporting portal i.e. www.cybercrime.gov.in to enable citizens to report complaints online pertaining to all types of cybercrimes. Complaints reported on this portal are attended to by the respective Law Enforcement Agencies of States/UTs as per Law.

****