GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 2496
TO BE ANSWERED ON: 16.03.2022

EXPERTISE IN CYBER SECURITY

2496. SHRI SUMEDHANAND SARASWATI:
SHRIMATI RANJEETA KOLI:

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

(a) whether there is a lack of expertise in dealing with cyber security cases in the country and if so, the details thereof;
(b) the details of the steps taken by the Government to improve cyber security;
(c) whether our nuclear plants, space research centres and security installations are safe in respect of cyber security from cyber hackers, if so, the details thereof and if not, the results thereon;
(d) whether the Government has cooperated with other institutions to strengthen the Government cyber security and if so, the details thereof; and
(e) the details of the steps being taken by the Government to create awareness about cyber security in the country?

ANSWER

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

(a): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users.The Government is well aware of increasing demand of cyber security expertise as cyber security threats are increasing as the Internet expands and more & more Indians get connected and use Internet. Government offers various capacity building programmes such as Information Security Education and Awareness (ISEA), Cyber Surakshit Bharat (CSB) to create expertise to deal with cyber security cases in the country.

(b): Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

(i). 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.
(ii). 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.
(iii). Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(iv). All the government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

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

(vi). Government 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.

(vii). Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 64 such drills have so far been conducted by CERT-In where 820 organizations from different States and sectors participated.

(viii). 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 19 training programs were conducted covering 708 and 5169 participants during the year 2020 and 2021 respectively.

(ix). CERT-In is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

(x). CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

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

(c): Yes, Sir. As per Department of Atomic Energy, Indian Nuclear establishment has set up rigorous procedure for design, development and operation of the systems used in its installations. The safety and security of critical systems are designed and developed in house using custom built hardware and software. As per National Critical Information Infrastructure Protection Centre (NCIIPC), sensitive installations of Indian Space Research Organisation (ISRO) are declared as Protected Systems. NCIIPC works with ISRO to ensure that they are safe from cyber hackers.

(d): Government has cooperated with other institutions to strengthen the Government cyber security, these include:

(i). CERT-In has entered into cooperation arrangements in the form of Memorandum of Understanding (MoU) with its overseas counterpart agencies for collaborating in the area of cyber security. At present such MoUs have been signed with Bangladesh, Brazil, Estonia, Finland, France, Israel, Japan, Nigeria, Singapore, South Korea and Uzbekistan.

(ii). CERT-In collaborates with product and security companies for cyber threat information exchange, development of best practices and capacity building.

(iii). CSIRT-Fin, CERT-In, National Institute of Securities Markets (NISM) and Centre for Development of Advanced Computing (CDAC) conduct a self-paced 60 hour certification program on “Cyber Security Foundation Course” for professionals in financial sector.

(e): Government has taken a number of steps to create awareness about cyber security in the country, these include:

(i). MeitY has implemented 'Information Security Education and Awareness' (ISEA) programme with the objective of capacity building in the area of Information Security, training of Government personnel and creation of mass Information Security awareness. The project is implemented involving 52 academic and training institutions across the country through formal and non-formal courses.

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".

(ii). Table Top Exercises are conducted by CERT-In regularly for senior management and Chief Information Security Officers (CISOs) to build awareness on threat landscape and best practices to counter cyber threats.

(iii). National Informatics Center (NIC) undertakes capacity building exercises (both classroom and virtual) from time to time, for knowledge awareness and capacity building in various key domains of cyber. Knowledge awareness training programs on Cyber Security are also conducted for Government personnel to help them adopting best recommended security practices.

****