GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 739
TO BE ANSWERED ON: 22.07.2022

WORKFORCE FOR DIGITAL SECURITY

739 SHRI PARIMAL NATHWANI:

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

(a) whether Government is taking any steps to provide a cyber security workforce which will have competency to oversee India's digital security from malicious threats to which it is becoming vulnerable;

(b) any steps taken by Government to include cyber security as part of curriculum in schools and colleges

(c) whether Government has considered including cyber security architecture in its 'Make in India' scheme to encourage indigenization of the same;

(d) whether Government has created a Centralized body for coordination of all matters, especially inter-Ministerial, related to cyber security threats, both foreign and domestic; and

(e) if so, details thereof, if not, reasons therefor?

ANSWER

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

(a): Yes sir. 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 users get connected and use Internet.

Government has taken following steps to create cyber security workforce which, inter alia, includes:

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. MeitY conducts deep dive training on cyber security for Chief Information Security Officers (CISOs) and frontline IT officials from Central/State Governments, Public Sector Undertakings (PSUs), PSU Banks and Government organisations in collaboration with industry consortium in Public Private Partnership (PPP) mode to enable them to deal with challenges of cyber security.

iii. MeitY offers generic training (awareness level) and foundation training (advanced level) online in Cyber Security for officers of Central Government Ministries/Departments. A total number of 10700 officers/staff from various Ministries/Departments have attended generic training (awareness level) and 605 officers/staff have attended foundation training (advanced level).

iv. 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.

v. 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.

vi. Indian Computer Emergency Response Team (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. 19 and 5 training programs were conducted covering 5169 and 449 participants during the year 2021 and 2022 (upto June) respectively.

vii. Cyber security exercises and drills are conducted regularly by CERT-In for capacity building and to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 67 such drills have so far been conducted by CERT-In where 886 organizations from different States and sectors participated.

viii. Computer Security Incident Response Team-Finance Sector (CSIRT-Fin), CERT-In, National Institute of Securities Markets (NISM) and Centre for Development of Advanced Computing (CDAC) are conducting a self-paced 60 hour certification program on "Cyber Security Foundation Course" for professionals in financial sector.

ix. Cyber security training programmes for employees of Government and Private Sector Utilities in the Power Sector are conducted through National Power Training Institute (NPTI).

(b): Government has taken a number of steps to include cyber security as part of education in schools and colleges which, inter alia, includes :

i. Information Security Education and Awareness (ISEA) Project has been implemented under which a total of 81,285 candidates have been trained in various courses in the area of Information Security through 52 institutions.Under the project, 5 participating Technical Universities have reported around 2.74 lakh candidates as trained/under-going training in formal courses in their respective affiliated colleges). A detailed model course structure/syllabus for - New M. Tech. in Information Security, M. Tech/MS by Research, M. Tech/B. Tech Retrofit, 1 year/6-month training programmes has been designed by experts. Several participating institutes/Technical Universities under the ISEA project have adopted the model syllabus.

Under the awareness activity, 1,413 awareness workshops on Information Security have been organized through direct/virtual mode across the country for various user groups covering 2,69,203 participants, out of which 866 awareness workshops have been organized for school and college students covering 1,92,118 participants. In addition, 1,24,068 school teachers have been trained as Master Trainers in 41 training programmes through direct/e-learning/Virtual Instructor Led Training (VILT) mode in the area of Information Security.Awareness material in the form of handbooks, posters, brochures, videos, etc. are also made available for download on the website www.isea.gov.in and www.infosecawareness.in.

ii. Central Board of Secondary Education (CBSE) has launched a 'Cyber Security Handbook' to ensure safe and healthy digital habits among students. This covers

topics in cyber safety, such as cyber bullying, including social exclusion, intimidation, defamation, and emotional harassment, online sexual abuse, cyber radicalisation, online attack and frauds, and online enticement. The 'Cyber Security Handbook' can be accessed at this link: http://cbseacademic.nic.in/web_material/Manuals/Cyber_Safety_Manual.pdf

PRAGYATA guidelines for school heads and teachers describe the need assessment, planning and steps to implement digital education while ensuring cyber safety and privacy measures. The guidelines can be accessed at: https://www.education.gov.in/sites/upload_files/mhrd/files/pragyata-guidelines_0.pdf

(c): Yes, Sir. Government is committed to 'Make in India' scheme for indigenization of electronics & IT products including cyber security. Ministry of Electronics & IT (MeitY) has notified Public Procurement (preference to Make in India) Order 2019 for Cyber Security Products.

(d) and (e): Yes, Sir.

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. 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.

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.

****