GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1193
TO BE ANSWERED ON: 29.07.2021

SECURITY POLICIES TO STRENGTHEN THE CYBER SECURITY

1193. DR. AMEE YAJNIK:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether any security policies have been introduced by Government during the last three years to strengthen the cyber security of the country;
(b) if so, the details thereof and if not, the reasons therefor;
(c) whether any measures have been taken by Government during the last three years to restrict data theft of an individual; and
(d) if so, the details thereof?

ANSWER

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

(a) and (b): Government has introduced the National Digital Communications Policy (NDCP) 2018 with the vision "To fulfil the information and communication needs of citizens and enterprises through the establishment of a ubiquitous, resilient, secure, accessible and affordable Digital Communications Infrastructure and Services; and in the process, support India's transition to a digitally empowered economy and society."

More specifically, for cyber security, the Government has formulated a draft National Cyber Security Strategy 2021 (NCSS2021)which holistically looks at addressing the issues of security of national cyberspace.The vision of the Cyber Security Strategy is to "Ensure a safe, secure, trusted, resilient and vibrant cyber space for India's prosperity". The three pillars of this strategy are - Securing the national cyberspace, Strengthening existing structures, people, processes & capabilities and Synergizing resources for optimal utilization.

(c) and (d): Post 2017, informational privacy is the fundamental right of citizen. It is the responsibility of intermediaries to protect data of citizens /consumers against any theft or breach of data. Further, the Personal Data Protection (PDP) Bill was introduced in Lok Sabha during winter session 2019. The Bill has been referred to Joint Parliamentary Committee. The PDP Bill ensures the protection against privacy and misuse of personal data of individuals.

In addition, Government has taken following measures to enhance cyber security:

i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on regular basis. CERT-In has issued 60 advisories for data security and mitigating fraudulent activities for organisations and citizens.

ii) The Indian Computer Emergency Response Team (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 for citizens and organisations.

iii) Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.

iv) As per National Informatics Centre (NIC) Security audit guidelines and advisories, respective web application owners take necessary proactive measures to enforce data security and privacy at web application end and also check that data privacy of Personally Identifiable Information (PII) and application audit log trail is duly maintained. Additionally for enhancing data security, security audits and vulnerability assessment of resources are periodically performed. As per the NIC best practices, sensitive data access is also controlled through multifactor authentication and strong authorization checks.

v) The comprehensive security guidelines in the form of license Amendments have been issued to Telecom Service Providers (TSPs)which were subsequently incorporated as a separate chapter on Security Conditions in Unified License.Vide these license conditions, it is mandated that TSPs are responsible for the security of their network. It is also mandated that only those network elements shall be inducted into their Telecom Network which have been tested as per relevant contemporary Indian or International Security Standards. As per Unified License condition, each licensee has to undertake an audit of their networks or get their networks audited from security point of view once in a financial year from a network audit and certification agency.

vi) Reserve Bank of India (RBI) issued a cyber-security framework on December 31, 2019 to strengthen the cyber security resilience of the urban cooperative banks (UCBs). The framework inter alia mandates the implementation of progressively stronger security measures based on the nature, variety and scale of digital product offerings of banks.

vii) Reserve Bank of India (RBI) has issued "Master Direction on Digital Payment Security Controls" dated February 18, 2021, providing necessary guidelines for the Regulated Entities (REs) to set up a robust governance structure and implement common minimum standards of security controls for digital payment products and services.

viii) Security tips have been published for users to secure their desktops, mobile/smart phones and preventing phishing attacks.

ix) Ministry of Electronics & Information Technology (MEITY) is conducting 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”.

****