GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3540
TO BE ANSWERED ON: 08.08.2018

PRIVACY OF CITIZENS

3540. SHRI M.I. SHANAVAS:

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

(a) whether it is true that any information stored by people in servers can be accessed by others and if so, the reasons therefor; and
(b) the extent to which the Government has ensured privacy of citizens information stored in the IT apparatus?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a): Any information stored by people in servers is not supposed to be accessed by others unless otherwise specifically authorized by the user. Information Technology Act, 2000 provides punishment and penalty for any unauthorized access of information.

(b): The Government websites host information for public dissemination and no sensitive information is hosted on such portals. As per the guidelines of the Government, the computer systems with sensitive information are isolated from the Internet. Also, user level access control is built into the systems so that only authorized users can access information to the extent intended. In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made to protect information stored on servers by way of appropriate security controls.

Government has taken the following measures to protect information and securing Information Technology infrastructure:-

(i) National Information Centre (NIC), which provides IT/e-Governance related services to Government departments, protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place. NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems, and antivirus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardening. These are complemented by round-the –clock monitoring of security events and remedial measures are carried out for solving the problems subsequently.
(ii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.cert-in.org.in).
(iii) Government has formulated 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.
(iv) 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.
(v) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 30 such exercises have so far been

conducted by CERT-In wherein organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc. participated.

****