GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 85
TO BE ANSWERED ON: 02.02.2018

ACCESS TO INFORMATION STORED IN ITSERVERS

85. SHRI C.P. NARAYANAN:

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

(a) whether it is a fact that any information stored by us in servers can be accessed by others;
(b) to what extent Government has ensured privacy of citizens information stored in IT apparatus;
(c) to what extent Government information is protected; and
(d) whether it is also a fact that interested countries and entrepreneurs are capitalizing on citizens information?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ALPHONS KANNANTHANAM)

(a) to (c): 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) 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).
(ii) 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.
(iii) Government has issued general guidelines for Chief Information Security Officers (CISOs) for securing applications and infrastructure and their key roles and responsibilities for compliance.
(iv) CERT-In has empanelled 54 security auditing organizations to support and audit implementation of Information Security Best Practices.

(v) 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.

(vi) Cyber security mock drills are being conducted regularly by CERT-In to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. In addition 3 drills were conducted in coordination with The Reserve Bank of India and The Institute for Development and Research in Banking Technology.

(vii) 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 hardenings. These are complemented by round-the –clock monitoring of security events and remedial measures are carried out for solving the problems subsequently.

(viii) Cyber Security is a continuous process and the protection elements are updated on a regular basis. A 24×7 security monitoring centre is in place at NIC, for detecting and responding to security incidents, including NIC-CERT.

(ix) Government has issued Guidelines for Indian Government Websites, details of which are available at http://www.guidelines.gov.in. Compliance Testing and certification of Government websites is done through STQC directorate.

(d): No such instance has been reported to Government.

****