GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:5757
ANSWERED ON:29.04.2015
GAP BETWEEN SECURE AND INSECURE NETWORK
Ashok Kumar Shri K.

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

(a) whether the Government have details of calls for strict access control and proper firewalls to bridge the gap between secure and insecure networks;

(b) if so, the details thereof; and

(c) the action taken in this regard?

Answer

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI RAVI SHANKAR PRASAD)

(a) and (b): In accordance with the existing guidelines of the Government, no sensitive information is stored on the computer systems connected to Internet. Security concerns with regard to sensitive data/information handling, processing, transit and storage calls for implementation of security best practices and measures. This include measures such as access control and implementation of firewalls and intrusion detection & prevention systems.

Accordingly, the critical sector organisations, Defence and sensitive organisations have been advised by the Government to use separate physical networks for operations of critical infrastructure and performing their functions. The critical networks should be isolated from other production networks connected over internet/intranet. Measures are taken to ensure air gap between critical systems and other networks/ Internet. Periodic audits are carried out to ensure strict procedures and systems are in proper order and working as per specifications.

(c): In order to improve the security posture of the networks, Government has taken following measures:

i . Government has setup National Critical Information Infrastructure Protection Centre (NCIIPC) to protect the critical information infrastructure in the country.

ii. National Informatics Centre (NIC) has implemented appropriate firewalls, intrusion detection & prevention systems, anti-virus software & other security controls and is continuously engaged in upgrading and improving the security posture of its IT infrastructure. A 24x7 security monitoring centre is operational in NIC for responding to security incidents. The security events generated from various security solutions on NIC Network (NICNET) are monitored round the clock for taking remedial measures.

iii. The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks.

iv. The Government has formulated 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 including Nuclear sector.

v. Indian Computer Emergency Response Team (CERT-In) is conducting mock cyber security drills to enable assessment of preparation of organizations to withstand cyber attacks. CERT-In issues alerts, advisories regarding latest cyber threats and counter measures.

In addition, Department of Telecom (DoT) has issued comprehensive security guidelines as part of telecom license process. The salient features of these guidelines are:

i) the Licensees shall have organisational policy on security and security management of their networks

ii) the Licensees shall audit their network or get the network audited from security point of view once a year from a network audit and certification agency.

iii) the Licensees shall create facilities for monitoring all intrusion, attacks and frauds and report the same to DoT and Indian Computer Emergency Response Team (CERT-In).

iv) the Licensees shall use only those equipment in the network which are certified to be safe to connect.