GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

STARRED QUESTION NO:160
ANSWERED ON:08.03.2010
NATIONAL CYBER SECURITY POLICY
Joshi Shri Pralhad Venkatesh;Singh Shri Ganesh

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

(a) whether the Government has formulated a National Cyber Security Policy to deal with the unabated cyber crimes challenging the security and sovereignty of the nation;

(b) if so, the details thereof and if not, the reasons therefor;

(c) whether the Government has developed and established any Cyber Security system which can instantly detect any cyber crime/hacking attempts to take pre-emptive action to diffuse such criminal act;

(d) if so, the details thereof and if not, the reasons therefor;

(e) whether an audacious attempt was recently made by some foreign based hackers to hack the computers of some important offices of the Government of India; and

(f) if so, the details thereof along with the action taken by the Government in this regard?

Answer

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY(ANDIMUTHU RAJA)

(a) to (f) : A Statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. 160 FOR 8.3.2010 REGARDING NATIONAL CYBER SECURITY POLICY

(a) and (b): As a prelude to having a National Cyber Security Policy, the Government as 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. Further, an information security action plan for protection of critical information infrastructure is in place. The plan is aimed at enabling Government and critical sectors in improving the security of their Information Technology systems and networks and verification through periodic risk assessments and annual audits by third party auditing organizations. The plan has been circulated to Government and critical sector organizations. In accordance with information security action plan, Government and critical sector organizations are required to do the following on priority: ` Identify a member of senior management, as Chief Information Security Officer (CISO), knowledgeable in the nature of information security & related issues and designate him/her as a `Point of contact`, responsible for coordinating security policy compliance efforts and to regularly interact with the Indian Computer Emergency Response Team (CERT-In), Department of Information Technology (DIT). ` Prepare information security plan and implement the security control measures as per IS/ISO/IEC 27001: 2005 and other guidelines/standards, as appropriate. ` Carry out periodic Information Technology security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organizational goals/objectives. ` Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for Information Technology systems and networks. Especially, Test and evaluation may become necessary after each significant change to the Information Technology applications/ systems/ networks and can include, as appropriate the following:

Penetration Testing (both announced as well as unannounced)

# Vulnerability Assessment
# Application Security Testing
# Web Security Testing ` Carry out Audit of Information infrastructure on an annual basis and when there is major up gradation/change in the Information Technology Infrastructure, by an independent Information Technology Security Auditing organization. ` Report cyber security incidents, as and when they occur and the status of cyber security, periodically to CERT-In. In support of the above action plan, Indian computer Emergency Response Team (CERT-In) has created a panel of 40 Information Technology security auditors to help the organizations to get their Information Technology infrastructure and information systems audited from the point of view of Risk assessment, penetration of network and vulnerability assessment.

(c) and (d): National Informatics Centre (NIC) provides network and systems services to Central Government and State Government departments. As a service provider, NIC has installed state-of- art Cyber Security System, which monitors the events on the network for detection and prevention of malicious traffic on the network. The Cyber Security System includes:

Intrusion Prevention Systems, Firewalls, Anti-virus solution and application firewalls.

Similarly, other large Government organizations running services on their own also have installed Cyber Security System to protect their Systems and Network. The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Section 69B empowers Government tomonitor and collect traffic data or information through a computer resource for Cyber Security. The Indian Computer Emergency Response Team (CERT-In) scans the Indian Cyber Space to detect traces of any untoward incident that poses a threat to the cyber space. CERT-In performs both proactive and reactive roles in computer security incidents prevention, identification of solution to security problems, analyzing product vulnerabilities, malicious codes, web defacements, open proxy servers and in carrying out relevant research and development. Sectoral CERTs have been functioning in the areas of defence and Finance for catering critical domains. They are equipped to handle and respond to domain specific threats emerging from the cyber systems.

(e) and (f): There have been attempts of foreign origin from time to time to penetrate high security cyber network operating in some important offices of the Government of India. Investigations have revealed that these are merely attempts and no system has been found to be hacked or infected. National Informatics Centre has been conducting the security audit of the computer systems at regular intervals and has not found any hacked systems or infected. The following attempts have been detected on the network of NIC, in the recent past:

# Maliciously crafted email with attachments containing malware to a number of mail recipients attempting to infect the client machines.
# Scanning and probing of IT infrastructure. These attacks have been observed to be coming from the computers installed in a number of foreign countries.

However, these computers could be compromised and may be under the control of hackers from other parts of the world. Most of the attacks are stopped with the help of Cyber Security System deployed for detection and prevention of such attempts.