GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *106
TO BE ANSWERED ON: 23.11.2016

ASSISTANCE TO STATES ON CYBER SECURITY

***106. DR. SHASHI THAROOR**

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

(a) whether the National Critical Information Infrastructure Protection Centre (NCIIPC) provides expert assistance and technical support to the State Governments in the areas of concerns related to cyber security and if so, the details thereof, State-wise including Kerala;

(b) whether the Government proposes to share the strategies evolved by NCIIPC, for protection of Critical Information Infrastructure (CIC), with the State Governments, so as to avoid incidents of cyber-security violations including the hacking of the website of the State Governments, and if so, the details thereof and if not, the reason therefor;

(c) whether the Government is formulating a Cyber Crisis and Management Plan to manage cyber security breaches in departments of the Central and State Governments; and

(d) if so, the details thereof and if not, the other measures taken to prevent cyber security breaches?

ANSWER

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

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

STATEMENT REFERED TO IN REPLY TO RAJYA SABHA STARRED QUESTION NO.*106 FOR 23.11.2016 REGARDING ASSISTANCE TO STATES ON CYBER SECURITY

……

(a): National Critical Information Infrastructure Protection Centre (NCIIPC) provides the expert assistance and technical support to the State Governments (Zone wise: North Zone, South Zone, West Zone, North-East Zone and Central Zone) including the State Governments of Kerala on concerns related to the cyber security of Critical Information Infrastructure (CII).

The following activities are carried out by NCIIPC for States/UTs:

(i) Advisories and alerts are sent to registered Chief Information Security Officers
(ii) Log analysis of State Data Centre (SDC) carried out for the purpose of detecting anomalies and cyber attacks
(iii) Analysis of policy documents, audit reports, compliance reports and cyber incident reports intimated to NCIIPC
(iv) Assistance in identification of all critical information infrastructure elements for approval by the appropriate government for notifying the same
(v) Assistance in the development of policies and plans, adoption of standards, sharing of best practices and refinement of procurement processes in respect of protection of CII
(vi) Conducting training and awareness programmes

NCIIPC is interacting with Kerala State IT Mission (KSITM) and CERT-Kerala regarding cyber security and protection of critical information infrastructure.

(b): NCIIPC shares the strategies evolved by NCIIPC for protection of Critical Information Infrastructure (CII) with State Governments. These are:-

i) Reporting vulnerability in the state government Critical Information Infrastructure,
ii) Sharing of analysis report of malware
iii) Incident reporting.

The Indian Computer Emergency Response Team (CERT-In) regularly tracks the hacking of websites and alerts the concerned website owners to take actions to secure the websites to prevent recurrence. CERT-In has published guidelines for securing the websites, which are available on its website (www.cert-in.org.in). CERT-In also conducts regular training programmes to make the system administrators aware about secure hosting of the websites.

(c) and (d): Ministry of Electronics & IT (MeitY) has formulated Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism for implementation by all key Ministries/Departments of Central Government, State Governments and Union Territories. The CCMP provides the strategic framework and guides actions to prepare for, respond to and coordinate recovery from a cyber-incident. The Cyber Crisis Management Plan is updated periodically to take into account changing scenario of cyber threat landscape. The sixth version of the plan has been published in the year 2015.

The following enabling actions are taken to enable implementation of CCMP:

i. Regular workshops are conducted for Ministries/Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan (CCMP). So far, 41 workshops have been conducted, of which 11 were conducted since May 2014.
ii. Comprehensive cyber security mock drills are being regularly held based on CCMP. So far, 11 such drills have been conducted since 2009. 110 organizations from sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS and States/UTs participated in these drills.

iii. Technical assistance has been provided by MeitY/ CERT-In to 25 States & UTs and 39 Central Ministries/Departments in drawing their own sectoral Crisis Management Plans and organizational level crisis management plans.

Apart from the steps mentioned above, the Government has also taken the following measures to enhance the cyber security of the country and protect cyber space:

a) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has issued 372, 402 and 358 advisories during 2014, 2015 and 2016 (till October) respectively.
b) CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in) and are used by Central Ministries/Departments and State Governments to secure their IT Infrastructure.
c) In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out by Cert-In.
d) 57 security auditing organizations have been empaneled to support and audit implementation of Information Security Best Practices.
e) A Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country is being set up.
f) National Cyber Coordination Centre (NCCC) is being set up to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
g) MeitY is implementing 'Information Security Education and Awareness (ISEA)' project to train professionals / Government officials and create mass information security awareness among citizens. The project is implemented by 51 institutions across the country. So far, 11,110 persons have been trained/undergoing training in various formal/non-formal courses focusing on Cyber Security. 2,384 Government personnel have been trained in direct training programs. CDAC Hyderabad has conducted 377 Awareness workshops for various user groups covering 42,379 participants from 22 States/UT.
h) CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 14 such training programs were conducted covering 431 participants during the year 2016.

i) Government has set up cyber forensic training & investigation labs at CBI Academy and in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement Agencies and Judiciary in these States. More than 1250 police officers in North Eastern states have been trained. The objective of these labs is to train police officers for seizing and imaging electronic evidence. In addition, National Institute of Technical Teachers Training and Research (NITTTR), Chandigarh has trained 2756 Engineering and Polytechnic college teachers. Also National Law School of India University (NLSIU), Bangalore imparted training to 1398 officials including judiciary, law teachers & practitioners, law students, law researchers, etc.

****