GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1675
TO BE ANSWERED ON: 26.07.2017

CYBER SECURITY APPARATUS

1675 SHRI ANURAG SINGH THAKUR:

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

(a) whether there is a cyber security threat apparatus in place;

(b) if so, details thereof;

(c) the details of the National encryption policy being followed in India; and

(d) the main characteristics of our National Policy on Privacy and the National Policy on Right to be Forgotten?

ANSWER

MINISTER OF STATE FOR ELECTRONICS & INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a) and (b): Yes, Sir. Government have taken a number of steps to meet cyber security threat. These are described below:

i) Government has set up Indian Computer Emergency Response Team (CERT-In) and has designated it as the nodal agency for responding to cyber security incidents in the country as per provisions of Section 70B of the Information Technology Act 2000. CERT-In is operating a round the clock incident response help desk, issuing alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures, conducting training programs on specific areas of cyber security.

ii) Government has formulated Cyber Crisis Management Plan (CCMP) 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) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different states and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc. have participated.

iv) Government has empanelled 54 security auditing organisations to support and audit implementation of Information Security Best Practices.

v) Sectoral CERTs are operational in Defence and Power sectors. Actionshas been initiated to setup the CERT in Financial sector.

vi) Government has setup National Critical Information Infrastructure Protection Centre (NCIIPC) under section 70A of the Information Technology Act 2000 to protect the critical information infrastructure in the country

vii) Information Sharing and Analysis Center (ISAC) has been set up as a non-profit organization that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two way sharing of information between the private and public sector. Since 2013, the following ISACs have been initiated in India:

- Central Electricity Authority has set up ISAC-Power.
- Indian Banks Center for Analysis of Risks and Threats (IB-CART) has been set up by IDRBT as the ISAC-Banking.

viii) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The Centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.

ix) Government has initiated action to set up National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by stakeholders. NCCC is a multi stakeholder body and is implemented by Indian Computer Emergency Response Team (CERT-In) at Ministry of Electronics and Information Technology (MeitY). The Phase I of NCCC has been made operational.

(c): Use of strong encryption with appropriate modes and methods of encryption has been recognized by the Government as means to securing data/transactions in Electronic Media and Promotion of E-Governance and E-Commerce. Information Technology Act 2000 enables the use of encryption for such purposes.

Taking into account national security concerns & technology trends as well as the need for protection of information, critical infrastructure, increasing online digital transactions and citizen's privacy aspects, Government has initiated steps to revise the encryption policy in consultation with all the stakeholders, including industry, to arrive at a balanced and holistic encryption policy. In this regard, the Government has setup a Committee of Experts with an objective to explore possible approaches to promote strong encryption, while also enabling lawful access to the plain text information corresponding to the encrypted information in order to ensure public safety and national security.

(d): There is no national policy either on Privacy or Right to be Forgotten.

****