GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:6471
ANSWERED ON:06.05.2015
CYBER SECURITY UNDER DIGITAL INDIA
Lekhi Smt. Meenakashi

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

(a) whether the existing cyber security framework commensurate with the latest technology that will be developed and implemented under the Digital India project;

(b) if not, whether the Government has considered any measures to strengthen cyber security vis-Ã -vis the Digital India project; and

(c) the details of the recent updates made to the Indian cyber security framework from the policy and legislative perspective?

Answer

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

(a) and (b): In tune with the dynamic nature of Information Technology, continuous efforts are required to be made to prevent and recover from cyber attacks. Government of India under the flagship programme of "Digital India" has a vision of providing digital infrastructure as a utility to every citizen in safe and secure cyberspace. Security of cyberspace is identified as one of the key components envisaged for the success of 'Digital India' programme. As part of this, key initiatives of the Government are:

i) Technology for cyber security by way of development of indigenous security solutions by promoting Cyber Security R&D with a focus on capacity building, infrastructure creation, R&D test beds and proof-of-concepts for application on a wider scale. The R&D efforts is a continuous activity to cater to changing needs and cyber security threat landscape.

ii) Efforts for setting up National Cyber Coordination Centre (NCCC) to generate near real time macroscopic views of the cyber security breaches and cyber security threats in the country. The centre will provide a structured mechanism and facilitate coordination of efforts of all stakeholder agencies in the country. NCCC will be a multi stakeholder body and will be implemented by Indian Computer Emergency Response Team (CERT-In) at Department of Electronics and Information Technology (DeitY).

iii) Efforts for setting up of "Botnet Cleaning and Malware Analysis Centre" to provide for detection of malware infected computer systems and enable cleaning and securing the systems of end-users to prevent further malware infections. The project is being implemented in coordination and collaboration with Internet Service Providers (ISPs) and Industry. This would help in enhancing the security of computer systems across the country.

(c): In order to address the issues of cyber security in a holistic manner, the Government has released the "National Cyber Security Policy-2013" for public use and implementation by all relevant stakeholders. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country. It aims to facilitate creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders actions for protection of cyber space. The policy is expected to serve as a long-term template for continuous evolution, guided actions and measurement of effectiveness of such actions. It also provides for creation of national level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. As provided in the policy, steps have been initiated for adopting a prioritised approach to implement the policy so as to address the most critical areas in the first instance.

In addition, Government has also taken steps to put in place a Framework for Enhancing Cyber Security, which envisages a multi-layered approach for ensuring defence-in-depth with clear demarcation of responsibilities among the stakeholder organizations in the country.

Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology Act, 2000 for protection of Critical Information Infrastructure in the country.

Further, the Information Technology Act, 2000 provides a comprehensive legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.