GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 314**
TO BE ANSWERED ON: 12.12.2018

**CYBER PHYSICAL SYSTEM MISSION**

**314    SHRI KUNDARIYA  MOHAN BHAI  KALYANJI BHAI:**

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

(a)  whether the Government has launched/proposes to launch Cyber Physical System Mission;
(b)  if so, the salient features and the objectives thereof;
(c)  whether cyber security has emerged as a very important and challenging field for the Government; and
(d)  if so, the details thereof and the steps taken to strengthen cyber security in the Country?

**ANSWER**
MINISTER OF STATE FOR  ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a):    Yes, Sir.

(b):    The Mission will have major activities i.e., Technology Development, Human Resource Development (HRD) & Skill Development, Innovation, Entrepreneurship & Start-Up Ecosystem and International Collaborations.

(c) and (d):  Yes, Sir, security to the Physical Infrastructure and other infrastructure is one of the activities of the Cyber Physical System Mission.

Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:
 (i)   Information Technology Act, 2000 was enacted to deal with cyber crime. IT Act has adequate deterrent provisions for cyber threats and cyber attacks.
 (ii)  Government has established Indian Computer Emergency Response Team (CERT-IN) under section 70B of the Information Technology (IT) Act, 2000 to act as nodal centre for incidence response. The details are available on its website (www.cert-in.org.in).
 (iii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of section 70A of the Information Technology (IT) Act, 2000 for protection of critical information infrastructure in the country.
 (iv)  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.
 (v)   Cyber security exercises and trainings are being conducted regularly by CERT-In to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITes etc.
 (vi)  Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre).

(vii) Government has set up National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.

(viii) National Informatics Centre (NIC) has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems and ante-virus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardenings.

(ix) A 24*7 security monitoring centre is in place at NIC, for detecting and responding to security incidents, including NIC-CERT and Centres of Excellence for Application Security.

*******