

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**LOK SABHA
UNSTARRED QUESTION NO. 1338**

**TO BE ANSWERED ON THE 18TH DECEMBER, 2018/ AGRAHAYANA 27, 1940
(SAKA)**

CYBER SECURITY

1338. SHRI MUTHAMSETTI SRINIVASA RAO (AVANTHI):

Will the Minister of HOME AFFAIRS be pleased to state:

- (a) whether cyber security is lacking in the country;**
- (b) if so, the details of the steps being taken to strengthen cyber security in various States, including Andhra Pradesh;**
- (c) whether the Government is seeking foreign collaboration in this regard; and**
- (d) if so, the details thereof and if not the reasons therefor?**

ANSWER

**MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI HANSRAJ GANGARAM AHIR)**

(a) & (b): No Madam. Government has taken a number of legislative, technical and institutional measures for addressing issues related to cyber security. These include National Cyber Security policy (2013), enactment of Information Technology (IT) Act, 2000 and setting up of Indian Computer Emergency Response Team (CERT-In). Some specific measures taken by the Government of India to strengthen cyber security system in the country are as under:

- (i) National Cyber Security Coordinator (NCSC) under National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for cyber security matters.**
- (ii) Information Technology Act, 2000 was enacted to provide legal recognition forelectronic communication, electronic commerce andcyber crimes etc. IT Act has deterrent provisions to deal with cyber threats and cyber attacks.**
- (iii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.**
- (iv) National Critical Information Infrastructure Protection Centre (NCIIPC) has been established for protection of critical information infrastructure in the country.**
- (v) Cyber security exercises are being conducted regularly to enable assessment of preparedness of organizations in Government and critical sectors.**
- (vi) Guidelines have been issued for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.**

- (vii) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for detection of malicious programs and provide free tools to remove the same.**
- (viii) National Cyber Coordination Centre (NCCC) has set upto 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.**
- (ix) All the new government websites and applications are audited prior to their hosting and on regular basis after hosting.**
- (x) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.**
- (xi) Under Cyber Crime Prevention for Women and Children (CCPWC) Scheme, Government of India has released grants to States/UTs including Andhra Pradesh for setting up of a Cyber Forensic cum Training Laboratory and organizing capacity building programme on cyber awareness and cyber crime investigation. Rs. 4.42 Crore has been released to Andhra Pradesh for the purpose.**

(xii) A Division has been established under the Ministry of Home Affairs to deal with Cyber and Information Security.

(c) & (d): The Indian Computer Emergency Response Team (CERT-In) has entered into Memorandum of Understanding (MoU) with its overseas counterpart agencies/Computer Emergency Response Teams (CERTs) for information exchange and collaboration for cyber security incident response.
