

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**RAJYA SABHA**  
**UNSTARRED QUESTION NO. 1941**  
TO BE ANSWERED ON: 05.12.2019

**SECURITY MEASURES TAKEN TO PROTECT CYBER NETWORKS**

**1941. SHRI HARSHVARDHAN SINGH DUNGARPUR:**

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

- (a) the details of the security measures taken/proposed to be taken by Government to protect cyber networks and also the action taken against the culprits;
- (b) whether there is acute shortage of cyber professionals/experts in the country to deal with cyber attacks; and
- (c) whether Government is planning to give training for cyber professionals?

**ANSWER**

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

(a): Government has taken several measures to enhance the cyber security posture and protect cyber networks. These, *inter alia*, include :

- (i) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology (IT) Act, 2000.
- (ii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.
- (iii) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
- (iv) Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.
- (v) 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.
- (vi) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 44 such drills have so far been conducted by CERT-In where 265 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.
- (vii) 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. 19 trainings covering 515 participants conducted in the year 2019 (till October).

- (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.
- (ix) Government has 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 individual entities. Phase-I of NCCC has been made operational.
- (x) Ministry of Home affairs has prepared National Information Security Policy and Guidelines (NISPG) and shared with the Central Ministries as well as the State Governments/ Union territories. They have been advised to take appropriate steps to strengthen information security controls as per NISPG for strengthening Information Security and preventing information security breaches.

‘Police’ and ‘Public Order’ are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery.

(b) and (c): Cyber Security is an evolving area and new technologies are regularly introduced in this domain causing ever increasing demand for human resources in the area. To address the requirement of trained professionals in this niche area, Government has taken several initiatives which includes

- (i) Information Security Education and Awareness (ISEA) Project Phase II was approved in the year 2014 for a period of 5 years with an objective of capacity building in the area of Information Security, training of Government personnel and creation of mass Information Security awareness targeted towards various user segments. The project aims to train more than 1 lakh candidates in various formal/non-formal courses and more than 13,000 Government officials by March 2020. In addition, the project envisaged creation of mass awareness on Information Security through direct and indirect mode.

So far, 51,164 candidates have been trained/under-going training in various formal/non-formal courses through 52 institutions; 7,523 Government officials have been trained in various short term courses of 2/3/5 days duration and 1,193 Government officials have been trained through e-learning mode in the area of Information Security. Besides this, 1,029 half day general awareness workshops on Information Security have been organized across the country for various user groups covering 1,33,990 participants.

- (ii) Cyber Security is increasingly getting introduced in curriculum of schools and colleges every year. Many universities and institutions are offering PhDs and Master’s degree specializing in Cyber/ Information Security. Vocational training program on cyber security have been introduced by Ministry of Skills Development and Entrepreneurship, and also in universities like IGNOU.
- (iii) 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. 24 trainings covering 845 participants and 19 trainings

covering 515 participants conducted in the year 2018 and 2019 (till Oct) respectively.

\*\*\*\*\*