

**GOVERNMENT OF INDIA  
MINISTRY OF HOME AFFAIRS**

**LOK SABHA  
UNSTARRED QUESTION NO. 3978**

**TO BE ANSWERED ON THE 20<sup>TH</sup> MARCH, 2018 /PHALGUNA 29, 1939 (SAKA)**

**CYBER SECURITY**

**3978. SHRI VINCENT H. PALA:**

**Will the Minister of HOME AFFAIRS be pleased to state:**

**(a) whether the national level cyber security policy has been updated since 2013;**

**(b) if so, the details thereof;**

**(c) the status of public-private partnership in strengthening India's cyber security as mentioned in the earlier policy of 2013; and**

**(d) the mechanism put in place to ensure digital safety and cyber security in light of the push for Digital India?**

**ANSWER**

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

**(a) & (b): National Cyber Security Policy – 2013 is in force.**

**(c): National Cyber Security Policy (2013) provides for developing effective Public Private Partnership and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace. A Joint Working Group (JWG) for Public Private Partnership on cyber security has been set up at NSCS which is working in following areas:**

- i. Setting up of Information Sharing and Analysis Centres (ISACs) in critical sectors like Banking, Telecommunications and Power.**
  - ii. Establishment of Centres of Excellence (CoEs) on Policy Research, Standards, Audit.**
  - iii. Capacity building for law enforcement agencies and cyber forensics.**
  - iv. Establishment testing labs for telecom and IT equipment under PPP model**
- (d): The following mechanism and measures are in place to ensure digital safety and cyber security:**
- i. Indian Computer Emergency Response Team (CERT-In) is designated as a National nodal agency to coordinate matters related to cyber security incidents in the country.**
  - ii. National Critical Information Infrastructure Protection Centre (NCIIPC) has been setup to enhance the protection and resilience of Nation's Critical information infrastructure.**
  - iii. Government has issued general guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance Organisations are encouraged to develop their organisation level cyber security policy.**

- iv. Public Private Partnership has been developed for cooperation and collaboration for responding cyber security incidents.**
- v. Awareness has been created in law enforcement agencies through conducting cybercrime awareness workshops.**
- vi. Information Security Education and Awareness (ISEA) Project is being implemented with an objective of capacity building in the area of Information Security, training of Government personnel and creation of mass Information Security awareness. The project aims to train 1.14 Lakhs persons under Academic activities (formal and non-formal courses) by the year 2020. So far more than 71000 candidates have been trained in various formal/non-formal courses in Information Security through 52 academic and training institutions.**
- vii. Cyber forensics training labs in all north eastern states, CBI Academy Ghaziabad and cities such as Mumbai, Pune, Kolkata and Bangalore have been setup and more than 28,000 state police from North Eastern States, Maharashtra, West Bengal and Karnataka have been trained for dealing with cybercrime.**
- viii. Cyber Crisis Management Plan (CCMP) for countering cyber threats and cyber terrorism has been developed and so far 60 workshops have been conducted for Central Govt. Ministries/Departments, States/Union Territories and other organisations.**

- ix. Research and development is carried out in the thrust areas of cyber security including (a) Cryptography and cryptanalysis, (b) Network & System Security, (c) Monitoring & Forensics, and (d) Vulnerability Remediation & Assurance through sponsored projects at recognized R&D organizations.**
  
- x. Government has initiated setting up of 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.**
  
- xi. Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) which provides detection of malicious programs and free tools to remove the same.**

\*\*\*\*\*