GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1553
TO BE ANSWERED ON: 28.07.2021

CYBER SECURITY INCIDENTS

1553. SHRI BRIJENDRA SINGH:

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

(a) whether cyber security incidents in the country have increased in conjunction with escalating border disputes with neighbouring countries;

(b) if so, the details thereof and the reaction of the Government thereto;

(c) whether the Government plans to set up/has set up a central authority tackling cyber security threats to the country's critical infrastructure in particular; and

(d) if so, the details thereof and the steps being taken by the Government in this regard?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. CERT-In has reported that a total number of 394499, 1158208 and 607220 cyber security incidents are observed during the year 2019, 2020 and 2021 (upto June) respectively.

(b): Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on regular basis.
ii. CERT-In is sharing early warning threat intelligence alerts with over 700 organisations across sectors to enable active threat prevention.
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 security auditing organisations to support and audit implementation of Information Security Best Practices.

v. Government has formulated Cyber 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 and exercises are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 59 such drills have so far been conducted by CERT-In where 565 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.

viii. Government is operating 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 the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

x. CERT-In also co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

(c) and (d): The Indian Computer Emergency Response Team (CERT-In) has been functional since 2004 and has been mandated to serve as national nodal agency for incident response as per provisions of Section 70B of Information Technology (IT) Act, 2000. Under the provision of Section 70A of IT Act, Government has established National Critical Information Infrastructure Protection Center (NCIIPC), as the national nodal agency in respect of Critical Information Infrastructure protection.

****