GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *139
TO BE ANSWERED ON: 28.07.2021

NEW CYBER SECURITY POLICY

***139. SHRI ARJUN LAL MEENA:**
SHRI SUNIL KUMAR SINGH:

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

(a) whether the Government is planning to frame/introduce a new Cyber Security Policy and if so, the details thereof;

(b) the amount of funds allocated for strengthening cyber security during each of the years between 2015 and 2021;

(c) the details of the capacity building exercises undertaken/being undertaken by the Government personnel to deal with cyber security threats; and

(d) the steps being taken by the Government to develop infrastructure to avert cyber attacks in all Government departments?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (d): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED Q. NO.*139 FOR 28-07-2021 REGARDING NEW CYBER SECURITY POLICY

……….

(a): The Government has formulated a draft National Cyber Security Strategy 2021 (NCSS2021), which holistically looks at addressing the issues of security of national cyberspace.

(b): The total amount of funds allocated by the Ministry of Electronics & Information Technology for strengthening cyber security during each of the years between 2015 and 2021 is as under:

Year	Total allocation (Rupees in crores)
2015-16	85.00
2016-17	70.00
2017-18	140.48
2018-19	150.00
2019-20	162.00
2020-21	310.00
2021-22	416.00

(c): The details of the capacity building exercises undertaken/being undertaken by the Government personnel to deal with cyber security threats are given below:

i. Indian Computer Emergency Response Team (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. During the year 2020 and 2021 (upto June), 15 and 10 training programmes have been conducted covering 708 and 646 participants respectively.

ii. Cyber security exercises and drills are conducted regularly by CERT-In for capacity building and to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 59 such exercises and drills have been conducted so far where 565 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

iii. CERT-In is regularly conducting workshops for Ministries, Departments, States & UTs and organizations to sensitise them about the cyber security threat landscape and enable them to prepare and implement the Cyber Crisis Management Plan (CCMP). 114 CCMP workshops have been conducted till July 2021 by CERT-In.

iv. National Critical Information Infrastructure Protection Centre (NCIIPC) has undertaken several initiatives towards capacity building exercise for Critical Information Infrastructure Protected Systems.

v. Information Security Education and Awareness (ISEA) programme: So far, a total of 18,926 Government officials have been trained in various short term courses through direct/self-paced e-learning/ virtual instructor-led training mode in the area of information security. Under this programme, the Ministry of Electronics and Information Technology (MeitY) is offering generic training (awareness level) and foundation training (advanced level) online in Cyber Security for officers of Central Government Ministries/Departments. A total number of 6347 officers/staff from various Ministries/Departments have attended generic training (awareness level) and 569 officers/staff have successfully completed foundation training (advanced level).

vi. Cyber Surakshit Bharat (CSB) programme: 22batches of deep-dive cyber security training have been conducted in partnership with industry consortium. 880 CISOs/IT officials from Government, PSUs, Banks and Government organisations have attended the CSB programme.

(d): Government has taken the 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 and networks 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 empanelled 58 security auditing organisations to support and audit implementation of Information Security Best Practices.

iv. 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.

v. 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.

vi. 24x7 Security Monitoring Centre is in place at National Informatics Centre (NIC) for detecting and responding to security incidents related to NIC infrastructure and data centres. Additionally for enhancing Data Security, periodic security audits and vulnerability assessment of resources are performed followed by subsequent hardenings.

vii. 24X7 Cyber Security Incident Response mechanism is in place at Indian computer Emergency Response Team (CERT-In).

viii. Indian Cyber Crime Coordination Centre (I4C) under Ministry of Home Affair (MHA) has been designated as the nodal point in the fight against cybercrime. Government has launched National Cyber Crime reporting portal namely www.cybercrime.gov.in to enable public to report incidents pertaining to all types of cyber crimes with a special focus on cyber crimes against women and children

ix. The analytics centre at NCIIPC provides near real time threat intelligence and situation awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure / Protected System entities to avert cyber attacks.

****