GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1850
TO BE ANSWERED ON: 04.08.2023

INDIGENOUS CYBER FIREWALL FOR CYBERSECURITY

1850. SMT. VANDANA CHAVAN:

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

(a) whether Government is considering to develop a robust mechanism for cybersecurity to counter the growing threat of cyber-attacks and cyber breaches;
(b) if so, the details of the measures being adopted;
(c) whether Government is considering the development of indigenous cyber firewalls for securing its critical infrastructures;
(d) if so, the details of the progress made in this regard;
(e) whether Government has undertaken measures to strengthen the efficiency of cyber commands; and
(f) if so, the details thereof and if not, the reasons therefor?

ANSWER

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

(a) and (b): The Government is committed to ensure that the Internet in India is Safe & Trusted and Accountable for all users. Government is fully cognizant and aware of various cyber security threats.

The Government has taken the following measures to enhance the cyber security posture and prevent cyber-attacks.

i. On observing the data breaches, the Computer Emergency Response Team (CERT-In) notifies the affected organisations along with remedial actions to be taken. CERT-In coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as Law Enforcement Agencies.
ii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.
iii. CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
iv. CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.
v. CERT-In has empaneled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

vi. Government has formulated a 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.

vii. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.

viii. CERT-In operates an automated cyber-threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

ix. CERT-In is providing the requisite leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to containment and mitigation of cyber security incidents reported from the financial sector.

x. Regular training programmes for network and system administrators and the Chief Information Security Officers of government and critical sector organisations are conducted by CERT-In, for securing the information technology infrastructure and mitigating cyber-attacks.

xi. The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

(c) and (d): Yes. In order to strengthen the cyber security and expand cyber security innovation ecosystem in the country, the Government encourages startups and industry to develop indigenous cutting edge cyber security products, solutions and platforms through various initiatives including centres of excellence in Centre for Development of Advance Computing(C-DAC) and National Informatics Centre(NIC).

(e) and (f): As per the information provided by Ministry of Defence (MoD), there are no cyber commands in Defence Forces.

****