GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 557
TO BE ANSWERED ON: 07.02.2025

DEVELOPMENT OF ROBUST CYBER ECOSYSTEM

557. SHRI AYODHYA RAMI REDDY ALLA:

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

(a) the steps taken to develop a robust cybersecurity ecosystem that integrates people, processes, technology to effectively mitigate cyber threats and the implications of emerging technologies like Artificial Intelligence (AI), Blockchain, the Internet of Things (IoT) on India's cybersecurity landscape;
(b) the steps taken to develop a culture of cybersecurity awareness and responsibility among citizens, businesses, Government agencies, the strategies employed to promote behavioral change; and
(c) the implications of data localization and cross-border data flows on India's cybersecurity and economic growth, the manner in which Government balances these competing interests?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a): The Government is fully cognizant and aware of various cyber security threats due to emerging technologies and need to create guardrails to effectively mitigate cyber threats and the implications emerging due ofArtificial Intelligence (AI), Blockchain, the Internet of Things (IoT). One of the seven pillars of AI is Safe and Trusted AI. Government had convened a consultation session with a diverse group of representatives from industry, academia, civil society organizations, and international bodies to discuss the framework, scope, and operational model of an Artificial Intelligence Safety Institute. The Artificial Intelligence Safety Institute aims to serve as a key pillar in advancing AI governance, while fostering multi stakeholder partnerships.

To develop a culture of cybersecurity awareness and responsibility among citizens, businesses, government agencies, Government has taken legal, technical, and administrative policy measures to strengthen cyber security in the country. Government has taken several actions to enhance cybersecurity in the country, these include:

(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 an ongoing basis.
(ii) CERT-In has empanelled 191security auditing organisations to support and audit implementation of Information Security Best Practices.
(iii) CERT-In coordinates incident response measures with international CERTs and service providers.
(iv) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations and enhance resilience in Government and critical sectors. 108 such drills have so far been conducted by CERT-In where 1435 organizations from different States and sectors participated.
(v) The Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) has been setup for responding to and containing and mitigating cyber security incidents reported from the financial sector under the umbrella and guidance of CERT-In.

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

(vii) NCIIPC provides threat intelligence, situational awareness, alerts & advisories and information on vulnerabilities to organisations having Critical Information Infrastructure (CIIs)/ Protected Systems (PSs) for taking preventive measures from cyber-attacks and cyber terrorism.

(viii) CERT-In is an accredited member of Task Force for Computer Security Incident Response Teams / Trusted Introducer. This signals to other parties that CERT-In has reached a certain level of maturity and functionality, which is valuable in building trust within the CERT community. CERT-In is an operational member of Asia Pacific Computer Emergency Response Teams, a regional forum for Internet security in the Asia-Pacific region. CERT-In is a member of Forum of Incident Response and Security Teams (FIRST), a global forum for cyber security teams.

(ix) National Informatics Centre (NIC) provides Information Technology (IT) support to ministries, departments and agencies of the Central Government, State Governments and district administrators for various e-governance solutions and follows information security policies and practices in line with industry standards and practices, aimed at preventing cyber-attacks and safeguarding data.

(x) NIC mandates periodic security audits of government websites, applications and hosting infrastructure through CERT-Inempanelled agencies to eliminate vulnerabilities and ensure compliance with global security standards.

(xi) NIC has deployed advanced security tools including Threat Intelligence Platform to identify the security issues associated with Government network.

(b): Government has taken up various initiatives to develop a culture of cybersecurity awareness, which includes:

(i) The Ministry of Electronics and Information Technology (MeitY) is implementing 'Information Security Education and Awareness' (ISEA) programme, which envisions capacity building, education, training and creation of mass awareness in the area of Information Security in the country. The academic activities of the project are implemented through a network of 52 academic and training institutions across the country. Mass awareness programmes are conducted across schools, colleges and for senior citizen, women, Government officials and general public.

(ii) CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks. A total of 12,014 officials have been trained in 23 training programs in 2024.

(iii) MeitY conducts programmes to generate information security awareness. Awareness material in the form of handbooks, short videos, posters, brochures, cartoon stories for children, advisories, etc. on various aspects of cyber hygiene & cyber security including deepfakes are disseminated through portals such as www.staysafeonline.in, www.infosecawareness.in and www.csk.gov.in.

(c): The Government of India adopts a balanced approach to data localization, enhancing safety and security while allowing cross-border data flows to drive global trade and innovation. This strategy strengthens cybersecurity resilience while fostering digital progress.

****