GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4291
TO BE ANSWERED ON: 26.03.2025

CYBERSECURITY THREATS AND NATIONAL PREPAREDNESS

4291. ADV. ADOOR PRAKASH:
SHRI BENNY BEHANAN:
DR. DHARAMVIRA GANDHI:
SHRI K SUDHAKARAN:

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

(a) the number of reported cybersecurity breaches affecting critical infrastructure and Government systems in the year 2024;
(b) the initiatives taken to enhance cybersecurity preparedness including the implementation of the National Cyber Security Strategy; and
(c) the measures being undertaken to strengthen cooperation with private sector companies and international partners to combat cyber threats?

ANSWER

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

(a): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency under the provisions of section 70B of the Information Technology Act, 2000 for responding to cyber security incidents. On observing cyber security incidents including breaches, CERT-In advises remedial measures to concerned organisations.

As per the Information Technology Act, 2000 (“IT Act”), Critical Information Infrastructure means computer resource whose incapacitation or destruction has debilitating impact on, inter alia, national security. The National Critical Information Infrastructure Protection Centre (NCIIPC) has been notified as the national nodal agency under the provisions of section 70A of IT Act for Critical Information Infrastructure Protection. NCIIPC has informed that revealing details regarding cybersecurity breaches on critical infrastructure would not be in the interest of the national security.

(b): The Government has taken following initiatives to enhance cybersecurity preparedness in the country which, inter alia, includes:

i. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination amongst different agencies.
ii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.
iii. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same. It also provides cyber security tips and best practices for citizens and organisations.

iv. Ministry of Home Affairs (MHA) has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.

v. 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.

vi. CERT-In 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. 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. 109 such drills have so far been conducted by CERT-In where 1438 organizations from different States and sectors participated.

viii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.

ix. CERT-In has empanelled 200 security auditing organisations to support and audit implementation of Information Security Best Practices.

x. CERT-In 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.

xi. CERT-In issued Guidelines for Secure Application Design, Development, and Implementation & Operations in September 2023. CERT-In has also released the Software Bill of Materials (SBOM) guidelines for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in October 2024 to help organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.

xii. 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.

xiii. CERT-In regularly conducts various activities for awareness and citizen sensitization with respect to cyber-attacks and cyber frauds.

xiv. The Ministry of Electronics and Information Technology 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): Government has taken following measures to strengthen cooperation with private sector companies and international partners and stakeholders to combat cyber threats, which, inter-alia, includes:

i. The Ministry of Electronics and Information Technology (MeitY) initiated Cyber Surakshit Bharat (CSB) programme in Public Private Partnership (PPP) mode to educate & enable the Chief Information Security Officers (CISOs) & broader IT community of Central/State Governments, Banks and PSUs to address the challenges of cyber security.

ii. MeitY has set up National Centre of Excellence (NCoE) in Cyber Security in collaboration with Data Security Council of India. NCoE's primary objective is to make coordinated efforts to catalyze and accelerate cybersecurity technology development and entrepreneurship in the country.

iii. CERT-In collaborates with product and cyber security companies for cyber threat information exchange, development of best practices and capacity building. CERT-In conducts joint cyber security training programs in collaboration with Industry partners to upskill the cyber security workforce in Government, Public and private organizations with the latest skills.

iv. CERT-In co-operates, works and coordinates incident response measures with international CERTs and service providers including private sector companies.

v. CERT-In is an accredited member of Task Force for Computer Security Incident Response Teams / Trusted Introducer. 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.

vi. CERT-In has entered into cooperation arrangements in the form of Memorandum of Understanding (MoU) with its overseas counterpart agencies for collaborating in the area of cyber security. At present such Memorandum of Understandings (MoU) have been signed with Bangladesh, Egypt, Estonia, Japan, Maldives, Russia, United Kingdom and Vietnam.

****