GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1338
TO BE ANSWERED ON: 02.08.2024

STRENGTHENING OF CYBER SECURITY INFRASTRUCTURE

1338. SMT. SANGEETA YADAV:

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

(a) whether it is a fact that the number of cyber crimesare increasing significantly;
(b) the measures being taken by Government to enhance public awareness about cybersecurity best practices;
(c) the manner in which Government is collaborating with private sector organizations to strengthen cybersecurity infrastructure;
(d) the status of the implementation of the National Cyber Security Policy; and
(e) the steps being taken to protect critical infrastructure (such as power grids, transportation systems, etc.) from cyber threats?

ANSWER

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

(a) to (e):‘Police’ and ‘Public Order’ are state subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cybercrime through their Law Enforcement Agencies (‘LEAs’). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their Law Enforcement Agencies (LEAs)

Government has taken following measures to enhance awareness among organisations and users for safe usage of digital technologies and prevent cyber attacks:

(i) The Ministry of Electronics and Information Technology (MeitY) is implementing a project on "Information Security Education and Awareness (ISEA)’ for generating human resources in the area of Information Security and creating general awareness on various aspects of cyber hygiene/cyber security among the masses. Awareness material in the form of handbooks, short videos, posters, brochures, cartoon stories for children, etc. are also made available for download through www.isea.gov.inand www.infosecawareness.in.

(ii) 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.

(iii) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.

(iv) CERT-In is regularly carrying out various activities for awareness and citizen sensitization with respect to cyber-attacks and cyber frauds.

(v) CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.

(vi) CERT-In regularly conducts trainings / workshops to train officials of Government, Public and Private sector organizations across all sectors on focused topics of Cyber Security.

(vii) The Government has established the Indian Cyber Crime Coordination Centre (I4C) under Ministry of Home Affairs (MHA) to provide a framework and eco-system for LEAs to deal with cyber crimes in a comprehensive and coordinated manner. The Government has launched the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) to enable the public to report all types of cyber crimes, with special focus on incidents reported on this portal are routed automatically to the respective State/UT law enforcement agency for further handling as per the provisions of law.

(viii) The 'Citizen Financial Cyber Fraud Reporting and Management System' was launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters. A toll-free Helpline number '1930' is operationalized to provide assistance in lodging online cyber complaints.

(ix) To strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Central Government has taken steps for spreading awareness about cyber crimes; issuance of alerts/advisories; capacity building/training of law enforcement personnel/ prosecutors/ judicial officers; improving cyber forensic facilities, etc.

(x) The Ministry of Home Affairs has taken many steps to spread awareness on cyber crime that inter-alia include; issuance of alerts/advisories, dissemination of messages through SMS, I4C social media account i.e Twitter handle (@Cyberdost), Facebook (CyberDostI4C), Instagram (cyberdosti4c), Telegram (cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple media, publishing of Handbook for Adolescents/Students, organizing of Cyber Safety and Security Awareness week, in association with police department in different States/UTs etc. The Ministry of Home Affairs has issued advisory to all the State/UT Governments to carry out publicity of National Cyber Crime Reporting Portal (https://cybercrime.gov.in) and Toll-free helpline number '1930' to create mass awareness.

Government has taken following steps to collaborate with private sector organizations to strengthen cybersecurity infrastructure:

(i) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) was established for detection of compromised systems in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The centre is working in close coordination and collaboration with Internet Service Providers, Academia and Industry. The centre is providing detection of malicious programs and free tools to remove the same for common users.

(ii) CERT-In collaborates with cyber security and product companies from industry in the area of cyber security for exchanging information on cyber threats and best practices. CERT-In conducts joint cyber security training programs and exercises in collaboration with Industry partners to upskill the cyber security workforce in Government, Public and private sector organizations.

(iii) The National Center of Excellence (NCoE)for Cybersecurity Technology Development is supported by MeitY to create a conducive ecosystem to accelerate cyber security technology development and innovation in the country.

(iv) The Cyber Surakshit Bharat programme was launched in Public Private Partnership (PPP) with the objective to educate & enable the Chief Information Security Officers (CISO) & broader IT community in Central/State Governments, Banks, PSUs and Government organizations to address the challenges of cyber security.

The Government has institutionalised a nationwide integrated and coordinated system to deal with cyber-attacks in the country which, inter alia, includes:

(i) National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for cyber security matters.

(ii) Under the provisions of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents

(iii) National Cyber Coordination Centre (NCCC) is a multi-stakeholder project and is implemented by the Indian Computer Emergency Response Team (CERT-In) under the Ministry of Electronics and Information Technology (MeitY). NCCC scans the cyberspace in the country at the meta-data level to generate near real-time macroscopic views of the cyber security threats. NCCC provides a structured system and facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats. Phase-I of NCCC has been made functional since July, 2017.

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

(v) Under the provisions of section 70A of the Information Technology (IT) Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.

(vi) CERT-In is working in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.

(vii) CERT-In has issued an advisory to various Ministries outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.

(viii) CERT-In has empanelled 176 security auditing organisations to support and audit implementation of Information Security Best Practices.

(ix) 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.

(x) CERT-In is operating 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.

(xi) 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.

(xii) Cybersecurity mock drills are being conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors.

(xiii) CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.

(xiv) Department of Telecommunications has set up a Telecom Security Operation Centre (TSOC), for monitoring and detecting potential cyber threats to the Indian telecom network and providing timely alerts to stakeholders for necessary actions.

****