GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 3075
TO BE ANSWERED ON: 19.03.2025

NATIONAL CYBER SECURITY STRATEGY

3075. SHRI GURJEET SINGH AUJLA:

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

(a) whether the Government is taking concrete steps to formulate and implement a comprehensive National Cyber Security Strategy to effectively combat cyber threats and safeguard digital infrastructure;
(b) if so, the details and the key focus areas thereof and the manner in which it aims to address rising cyber frauds data security concerns in case there is no such strategy;
(c) the measures taken by the Government to strengthen India's cyber security framework and enhancement of cyber defence mechanisms to counter growing cyber frauds;
(d) the steps taken by the Government to curb financial cyber crimes' OTP frauds and online scams; and
(e) whether the Government recognize urgent need for a proactive robust cyber security policy to protect nationals given increasing digital dependence of our citizens and if so, the details thereof and the action taken in this regard?

ANSWER

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

(a),(b) and (e): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. Government has taken several legal, technical, and administrative policy measures for addressing cyber security challenges in the country. The Government has also institutionalised a nationwide integrated and coordinated system to deal with cyber security matters 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. 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) 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.
iv. 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, and also provides cyber security tips and best practices for citizens and organisations.
v. Ministry of Home Affairs (MHA) has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.
vi. 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.

To ensure secure and resilient cyberspace, the primary focus is on the three pillars of Securing national cyberspace, strengthening existing structures comprising of people,

processes and capabilities and synergise resources for their optimal utilization to protect the Digital Environment in the country.

(c) and (d): Government has taken following measures to strengthen India's cyber security framework and prevent cyber fraud including curbing financial cyber crimes, which, inter-alia, includes:

i. CERT-In issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.
ii. 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.
iii. 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.
iv. CERT-In has issued an advisory to various Ministries in November 2023 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.
v. 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.
vi. CERT-In works in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.
vii. 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.
viii. 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.
ix. 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.
x. CERT-In has empanelled 200 security auditing organisations to support and audit implementation of Information Security Best Practices.
xi. 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.
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 is regularly carrying out various activities for awareness and citizen sensitization with respect to cyber-attacks and cyber frauds.
xiv. National Informatics Centre (NIC) mandates periodic security audits of government websites and applications through CERT-In-empanelled agencies to eliminate vulnerabilities and ensure compliance with global security standards and Vulnerability Assessment of the underlying hardware on which such applications are hosted.

xv. 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.

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

xvii. 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.

xviii. The MHA has established the Indian Cyber Crime Coordination Centre (I4C) as an attached office to provide a framework and eco-system for LEAs to deal with cyber crimes in a comprehensive and coordinated manner. The MHA has also launched the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) to enable the public to report all types of cyber crimes. Cyber crime 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. The 'Citizen Financial Cyber Fraud Reporting and Management System' has been launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters.

xix. Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency working together for immediate action and seamless cooperation to tackle cybercrime. By bringing together financial institutions, CFMC aims to detect, prevent and mitigate the cyberfinancial frauds by preventing the dissemination of fraudulent funds across various financial sectors.

xx. MHA 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.

xxi. Department of Telecommunications issued framework for Telecom Cyber Security Incident Response (T-CSIRT), sectoral computer emergency response team (CERT) on 03.08.2022 for performing, coordinating and supporting the response to a security incident within telecommunication sector. The same has been reviewed and issued on 31.01.2023.

xxii. Reserve Bank of India (RBI) has issued Master Directions on Fraud Risk Management for the Regulated Entities viz. (i) Commercial Banks (including Regional Rural Banks) and All India Financial Institutions; (ii) Cooperative Banks (Urban Cooperative Banks / State Cooperative Banks / Central Cooperative Banks); and (iii) Non-Banking Finance Companies (including Housing Finance Companies) on 15.07.2024 for strengthening of framework on Early Warning Signals (EWS), inter alia, to monitor transactions / unusual activities in the non-KYC compliant and money mule accounts etc., to contain unauthorised / fraudulent transactions.

xxiii. RBI through "RBI Kehta Hai" has issued awareness material / useful information on aspects such as different types of frauds, modus-operandi and measures to be taken during digital payment transactions and also through advertising (through prominent personalities) for creating awareness amongst public, etc.

xxiv. RBI has issued the booklet 'BE(A)WARE' on modus operandi of financial frauds in the public domain to educate the public.

****