GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 3789
TO BE ANSWERED ON: 18.12.2024

NATIONAL CYBER SECURITY POLICY

†3789. SHRI IMRAN MASOOD:

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

(a) whether any steps are being taken to draft a comprehensive National Cyber Security Policy for the country;
(b) if so, the details of such strategy including its estimated date of publication and if not, the reasons therefor; and
(c) whether the Government has taken any measures to enhance cyber security infrastructure and capacity building in the country including cooperation with international partners and stakeholders and if so, the details thereof?

ANSWER

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

(a) and (b): 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): Government has taken following measures to strengthen the nation's cyber security infrastructure and capacity building in the country including cooperation with international partners and stakeholders, 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 issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.

(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) 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.

(vii) 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.

(viii) CERT-In has empanelled 155 security auditing organisations to support and audit implementation of Information Security Best Practices.

(ix) CERT-In coordinates incident response measures with international CERTs and service providers.

(x) 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.

(xi) 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.

(xii) 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.

(xiii) 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, Brazil, Egypt, Estonia, Japan, Maldives, Russian Federation, United Kingdom, Uzbekistan and Vietnam.

(xiv) 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 9,807 officials have been trained in 20 training programs in 2024 (upto October).

(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) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations and enhance resilience in Government and critical sectors. 104 such drills have so far been conducted by CERT-In where 1420 organizations from different States and sectors participated.

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

(xviii) 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.

****