GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2770
TO BE ANSWERED ON: 20.12.2023

STRENGTHENING CYBER SECURITY

2770. SHRI NARANBHAI KACHHADIYA:
SHRI DILIP SAIKIA:
SHRI SUDHAKAR TUKARAM SHRANGARE:
SHRI SHIVAKUMAR C. UDASI:
SHRI RANJEETSINGH NAIK NIMBALKAR:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) the details of the measures taken by the Government to strengthen cyber security in the Country;
(b) the key objectives of the National Cyber security Policy in the Country; and
(c) the benefits of the Startup India programme in promoting entrepreneurship?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. The Internet technology and Internet used to be seen as force for good, but in recent years, technology is also exploited for causing user harms and criminality.

Government is fully cognizant and aware of various cyber security threats and challenges and has taken following measures to strengthen cyber security in the country:

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

(ii) National Critical Information Infrastructure Protection Centre (NCIIPC) has been established for protection of critical information infrastructure in the country under the provisions of section 70A of the Information Technology (IT) Act, 2000, NCIIPC provides near real-time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

(iii) The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs is designated as the nodal point in the fight against cybercrime. A toll-free number 1930 is operational for citizens to get assistance in lodging online complaints in their own language. To spread awareness on cybercrime, the Ministry has taken several steps, which include dissemination of messages on cybercrime through the Twitter handle @cyberDost and radio campaigns.

(iv) The Department of Telecommunications monitors and detects cyber-attacks and threats to Indian telecom networks, including those initiated from foreign countries, and provides timely alerts to stakeholders for necessary action.

(v) National Informatics Centre (NIC) provides IT support to user ministries, departments and agencies of the Central Government, State Governments and district administrations 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.

(vi) The Ministry of Electronics and Information Technology (MeitY)has issued Guidelines for Cybersecurity Audit that cover both comprehensive and limited audit on periodic basis by competent auditors with clear responsibilities for ensuring such audit regularly, inclusive of vulnerability assessment and penetration testing.

(vii) MeitY conducts programmes to generate information security awareness. Books, videos and online materials about information security are developed for general users, children and parents, and are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

(viii) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.

(ix) 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.

(x) CERT-In operates 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 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.

(xii) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) 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.

(xiii) 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.

(xiv) CERT-In has empanelled 177 security auditing organisations to support and audit implementation of Information Security Best Practices.

(xv) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 86 such drills have so far been conducted by CERT-In where 1159 organizations from different States and sectors participated.

(xvi) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. A total of 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022. In 2023, up to October, a total of 7007 officials from Government, critical sectors, public and private sector have been trained in 21 training programs in the area of cyber security.

(xvii) RBI has issued various instructions in respect of security and risk mitigation measures related to electronic/digital transactions. Thesecover securing of card transactions, securing payments through Internet banking / electronic payments, ATM transactions, pre-paid payment instruments (PPIs), limiting customer liability on unauthorised electronic banking transactions (including PPIs issued by authorised non-banks), safeguarding against email spoofing attacks, etc.

(b): Government published National Cyber Security Policy 2013 to build a secure and resilient cyberspace for citizens, businesses and Government, and the mission of protecting information and information infrastructure in cyberspace, building capabilities to prevent and respond to cyber threats, reducing vulnerabilities and minimising damage from cyber incidents, through a
combination of institutional structures, people, processes, technology and cooperation.

The followings are the key objectives of National Cyber Security Policy:

- To create a secure cyber ecosystem in the country includingcreating a security assurance and regulatory framework
- To create national and sectoral CERTs, NCIIPC for 24x7 operation
- To develop suitable indigenous technologies
- To create a workforce of skilled cyber security professionals
- To enable protection of information and safeguard privacy
- To enable cyber crime prevention, investigation and prosecution
- To create a culture of cyber security and develop effective public-private partnerships
- To enhance global cooperation in cyber security

(c): As per the Department for Industrial Policy and Promotion (DPIIT), Ministry of Commerce and Industry has launched the Startup India initiative on 16thJanuary 2016 with an intent to build a strong ecosystem for nurturing innovation, startups and encouraging investments in startup ecosystem in the country.

The Government unveiled a Startup India Action Plan comprising of schemes and incentives envisaged to create a vibrant startup ecosystem in the country. The Action Plan comprises of various action items spanning across areas such as Simplification and handholding, Funding support and incentives and Industry-academia partnership and incubation, promotion of ease of doing business for startups, greater role of technology in executing various reforms, building capacities of stakeholders and enabling a digital Atmanirbhar Bharat.

****