

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1386
TO BE ANSWERED ON: 04.12.2024

CYBER SECURITY MEASURES

**1386. SHRI VIJAYAKUMAR *Alias* VIJAY VASANTH:
SHRI MANICKAM TAGORE B:**

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

- (a) the manner in which the Government proposes to/is strengthening cyber security in the country; and
- (b) the details of measures taken/to be taken in this regard?

ANSWER

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

(a) and (b): The Government is committed to ensure that the Internet in India is Open, Safe, Trusted and Accountable for its users. Government has taken legal, technical, and administrative policy measures to strengthen cyber security challenges in the country. Government has taken following actions 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 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, and also provides cyber security tips and best practices for citizens and organisations.
- iv. 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.
- v. 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.
- vi. Government has given directions to all Central Ministries/Departments and States/UTs to appoint Chief Information Security Officers (CISOs) to deal with cyber security matters.
- vii. 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.
- viii. 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.

- ix. 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.
- x. 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.
- xi. 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.
- xii. CERT-In 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.
- xiii. CERT-In has empanelled 155 security auditing organisations to support and audit implementation of Information Security Best Practices.
- xiv. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations 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.
- xv. CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government, public and private sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks. A total of 9,807 participants have been trained in 20 training programs in 2024 (upto October).
- xvi. CERT-In coordinates incident response measures with international CERTs, service providers as well as law enforcement agencies.
- xvii. CERT-In collaborates with Industry to exchange information on latest cyber threats, best practices, and conduct joint skilling and capacity building programs.
- xviii. The Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country under the provisions of section 70A of the Information Technology (IT) Act, 2000.
- xix. The Ministry of Electronics and Information Technology 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.
- xx. National Informatics Centre (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.
