GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 653**
TO BE ANSWERED ON: 23.07.2025

## STEPS FOR ENHANCING CYBER SECURITY STANDARDS

**653. DR. AMAR SINGH:**

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

(a) whether the Government has taken any necessary steps for enhancing cyber security standards, building digital infrastructure and promoting cyber security awareness;
(b) if so, the details thereof and if not, the reasons therefor;
(c) whether the Government has taken cognizance of the fact that the nation has seen a significant increase in cyber threats in recent years, with both individuals and organisations facing various types of cyber attacks; and
(d) if so, the details of the initiatives that have been taken/being taken by the Government to combat the cyber security challenges in the country?

## ANSWER

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

(a) to (d): The Government has undertaken several initiatives to enhance cyber security standards, strengthen digital infrastructure, and promote cybersecurity awareness, with the objective of ensuring an Open, Safe, Trusted, and Accountable Internet for all users. Government remains cognizant and aware of cyber threats and challenges. Following measures have been taken to strengthen cybersecurity in the country:

i. With participation from the government, industry, and academia, the Bureau of Indian Standards (BIS) formulates cybersecurity standards through its technical committees. These committees also serve as the National Mirror Committees for the corresponding international committees of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). India’s active role in international standardization efforts fosters collaboration with global partners, provides early insights into emerging developments, promotes alignment with evolving best practices, and strengthens national cybersecurity capabilities.
ii. 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.
iii. The Government has established the 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.

iv. CERT-In works with other agencies involved in ensuring cybersecurity including Telecom Security Operations Centre (TSOC), India Cyber Crime Coordination Centre (I4C), National Centre Information Infrastructure Protection Centre (NCIIPC), etc.

v. CERT-In along with other agencies was able to successfully prevent cyber-attacks during the G20 summit, Parliament 20 summit, Ram Janmabhoomi event, Maha Kumbh etc.

vi. Regular training workshops are conducted for cybersecurity professionals, Chief Information Security Officers (CISO) and government employees etc.

vii. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.

viii. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors.

ix. 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.

x. CERT-In has formulated Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Central Government Departments, State Governments and their organizations and critical sectors.

xi. CERT-In has empaneled 200 security auditing organizations to support and audit implementation of Information Security Best Practices.

xii. Computer Security Incident Response Team in Finance sector (CSIRT-Fin) under CERT-In is operational since May 2020 to coordinate cyber incident response in the banking and financial sector.

xiii. MeitY observes the Cyber Security Awareness Month (NCSAM) during October of every year, Safer Internet Day on 2nd Tuesday of February every year, Swachhta Pakhwada from 1st to 15th February of every year and Cyber Jagrookta Diwas (CJD) on 1st Wednesday of every month by organising various events and activities for citizens as well as the technical cyber community in India.

******