

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4107
TO BE ANSWERED ON: 12.08.2026

**CYBER SECURITY PREPAREDNESS OF CENTRAL
GOVERNMENT DIGITAL PLATFORMS**

4107. SHRI RAJMOHAN UNNITHAN:

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

- (a) whether the Government has reviewed the cyber security preparedness of Central Government digital platforms and citizen service portals and if so, the details thereof;
- (b) the details of number of cyber security incidents reported during the last three years along with the corrective measures taken by the Government thereon;
- (c) whether any assistance has been extended to States including Kerala for strengthening cyber security infrastructure and digital resilience; and
- (d) the details of measures taken by the Government to enhance cyber security awareness, data protection and secure digital governance?

ANSWER

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

(a) to (d): Government is committed to ensuring an open, safe, trusted and accountable cyberspace. Several legal, technical and administrative policy measures have been implemented to strengthen the cyber security preparedness of Central Government digital platforms and citizen service portals, protect digital infrastructure and enhance cyber resilience.

Indian Computer Emergency Response Team (CERT-In) has been designated as the national agency for responding to cyber security incidents under Section 70B of the Information Technology Act, 2000.

As per the information reported to and tracked by CERT-In, the total number of cyber security incidents observed during the last three years are given below:

Year	No of incidents
2023	15,92,917
2024	20,41,360
2025	29,44,248

On observing cyber security incidents including those related to Government-managed platforms, CERT-In advises remedial measures to concerned organizations and coordinates incident response measures with affected organizations, service providers, respective sector regulators as well as Law Enforcement Agencies.

The Government has institutionalized a nationwide integrated and coordinated system to deal with cyber-attacks in the country. These measures, inter alia, include:

- a. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination related to cyber security amongst different agencies.
- b. National Cyber Coordination Centre (NCCC), implemented by CERT-In, examines cyberspace to detect cyber security threats and shares threat intelligence with concerned organisations, State Governments and stakeholder agencies for taking appropriate action.
- c. National Critical Information Infrastructure Protection Centre (NCIIPC) has been established under Section 70A of the Information Technology Act, 2000 for protection of Critical Information Infrastructure (CII).
- d. NCIIPC provides near real-time threat intelligence and situational awareness, issues regular alerts and advisories to Critical Information Infrastructure (CII)/Protected System (PS) entities, periodically undertakes vulnerability and risk assessment of CII/Protected Systems and provides feedback to the concerned entities.
- e. Cyber Swachhta Kendra (CSK)
 - A citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space.
 - It is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same.
 - It also provides cyber security tips and best practices for citizens and organisations.
- f. Sectoral Computer Security Incident Response Team (CSIRT)
 - CSIRT in the Finance sector (CSIRT-Fin) under CERT-In is operational since May 2022 to coordinate cyber incident response in the banking and financial sector.
 - CSIRT-Power has been operational since September 2024 as an extended arm of CERT-In to coordinate cyber security issues within the power sector entities.
- g. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.
- h. CERT-In has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Departments, State Governments and their organizations.
- i. Cyber security mock drills are conducted regularly by CERT-In, to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors.
- j. CERT-In has created a panel of 'Information Security Auditing Organisations' for auditing, including vulnerability assessment and penetration testing of computer systems, networks, websites and applications of various organizations of the Government and critical sectors. 237 information security auditing organisations are empanelled by CERT-In to support and audit implementation of Information Security Best Practices.

- k. All the Government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.
- l. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.
- m. The Government has put in place a statutory framework under the Digital Personal Data Protection Act, 2023. The rules framed, thereunder, to ensure that the sharing and processing of citizens' digital personal data for law enforcement purposes is undertaken in a lawful, secure and accountable manner.
- n. **Information Security Education and Awareness (ISEA) Workshops**
 - The Ministry of Electronics and Information Technology (MeitY) is implementing the ISEA project for generating human resources in Information Security and creating general awareness on various aspects of cyber hygiene & cyber security among the masses.
 - 6,650 awareness workshops have been conducted across the country covering over 11.37 lakh participants, including students, teachers, law enforcement personnel, Government officials, and the general public. This includes 70 awareness workshops organized in Kerala covering 9481 participants
 - Further, multilingual awareness material in the form of handbooks, short videos, posters, brochures, cartoon stories for children, etc. published and disseminated through print, electronics, social media, and www.isea.gov.in & <https://staysafeonline.in/>.
- o. **National Cyber Security Awareness Activities**
 - The Government organises events and activities for citizens as well as the technical cyber community across the country. Some of these include:
 - National Cyber Security Awareness Month (NCSAM) in October every year
 - Safer Internet Day on the second Tuesday of February
 - Swachhta Pakhwada (1st –15th February), and
 - Cyber Jagrookta Diwas (CJD) on the first Wednesday of every month
- p. **Training programs by CERT-In**
 - CERT-In conducts cyber security training programs in collaboration with Industry partners to upskill the cyber security workforce in Government, public and private organizations. 32 and 13 training programs were conducted covering 20799 and 12109 participants including 786 and 411 participants from Kerala during the year 2025 and 2026 (upto June) respectively
 - CERT-In is regularly sharing safety and security tips and awareness posters, infographics and videos through its official websites and social media handles such as Facebook, X(Twitter), Instagram, YouTube and LinkedIn for sensitizing internet users on cyber security attacks and frauds and prevention measures.
