GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2297
TO BE ANSWERED ON: 19.12.2025

DIGITAL PUBLIC INFRASTRUCTURE AND CYBER INCIDENT TRENDS

2297. SHRI RAVI CHANDRA VADDIRAJU:

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

(a) the year-wise data on cyber incidents reported to CERT-In since 2022;
(b) the number of entities onboarded to key Digital Public Infrastructure platforms such as Aadhaar, DigiLocker and UMANG;
(c) the funds allocated and utilised for cybersecurity capacity-building; and
(d) the steps taken to strengthen early-warning systems for large-scale cyber threats?

ANSWER

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

(a) to (d): The policies of the Government of India aim to ensure a safe, trusted, and accountable cyberspace. It remains vigilant and fully conscious of the cyber threat to India's digital infrastructure.

Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) work continuously to safeguard digital services, including the critical sectors.

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.

Total number of cyber security incidents reported to CERT-In since 2022 are given below:

Year	Number
2022	13,91,457
2023	15,92,917
2024	20,41,360
2025*	25,80,655

*(Upto Oct)

There are various entities onboarded on **Digital Public Infrastructure** (DPI) platforms, namely Aadhaar, DigiLocker, and UMANG, is as follows:

- **Aadhaar:** A total of 652 entities have been onboarded to the Unique Identification Authority of India (UIDAI) Aadhaar authentication ecosystem
- **DigiLocker:** The platform has onboarded 2,310 issuers and 3,031 requestors
- **UMANG:** 240 government entities (Central:80 and State:160) have been onboarded to the UMANG platform, providing 2384 services.

Government of India is implementing a project on **Information Security Education and Awareness (ISEA)** with the budget allocation of Rs. 332.74 crores for five years since 2023.
The Government has undertaken several steps to strengthen early-warning systems for large-scale cyber threats, which inter alia, includes:

1. National Cyber Coordination Centre (NCCC), implemented by CERT-In, examines cyberspace to detect cyber security threats.
2. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.
3. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.
4. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.
5. 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.

6. CERT-In has empanelled 231 security auditing organisations to support and audit implementation of Information Security Best Practices.
7. CERT-In has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all government organizations and in critical sectors.
8. Cyber security mock drills are conducted regularly by CERT-In, to enable assessment of cyber security posture and preparedness of various organisations.
9. Certified Security Professional in Artificial Intelligence (CSPAI) program launched by CERT-In in September 2024 equips cybersecurity professionals with the skills to secure AI systems.

a. It helps in addressing AI-related threats, and ultimately ensure trustworthy AI deployment in business environments.

******