GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *143
TO BE ANSWERED ON: 12.12.2025

**CYBERSECURITY AND DATA PROTECTION
MEASURES IN KARNATAKA**

*143. SHRI LAHAR SINGH SIROYA:

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

(a) whether Government has strengthened cybersecurity measures and data protection mechanisms in Karnataka;
(b) the number of training programs conducted for Government employees and IT professionals in Karnataka to handle cyber threats;
(c) whether public awareness campaigns on cybersecurity and safe internet practices have been undertaken; and
(d) the steps taken to ensure compliance with the Digital Personal Data Protection Act and other IT security regulations?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (d):   A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *143 FOR 12.12.2025, REGARDING CYBERSECURITY AND DATA PROTECTION MEASURES IN KARNATAKA

………

(a) to (d): The policies of the Government aim to ensure an Open, Safe, Trusted and Accountable Internet for all users. The Government has undertaken several initiatives to strengthen cybersecurity and data protection in the country, including the State of Karnataka:

1. **The Indian Computer Emergency Response Team (CERT-In)** has been designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology (IT) Act, 2000.
2. **National Cyber Coordination Centre (NCCC)** is implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.
3. **Cyber Swachhta Kendra:**
   - 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.
4. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of various organisations.
5. CERT-In has empanelled 231 security auditing organizations to support and audit implementation of Information Security Best Practices.
6. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis.
7. CERT-In has issued a cyber security baseline document, in September 2025, which provides a minimum set of security controls recommended for Micro, Small and Medium Enterprises (MSMEs). This helps MSMEs to implement essential measures for strengthening their cyber security posture.
8. CERT-In has issued updated technical guidelines in July 2025 for Bill of Materials (BOM) for software, hardware, Artificial Intelligence, Quantum Computing & Cryptography requirements. These guidelines are aimed to enhance the security and transparency of supply chains for software, hardware & emerging technologies.
9. CERT-In has operationalised a Responsible Vulnerability Disclosure and Coordination Program for collection, analysis, mitigation and coordination with researchers/finders/vendors for fixing vulnerabilities in software/ devices.
10. **Information Security Education & Awareness (ISEA) Workshops**
    - ISEA is an initiative for building human resources in Information Security and to spread cyber hygiene awareness among citizens.
    - So far, 4,125 workshops have been conducted, reaching over 9.25 lakh+ participants, including academia, law enforcement, government personnel, & general public.

- 285 workshops in Karnataka covering 30,049 participants, including 79 workshops for 5,269 Government officials have been organised. District-wise details of workshops in Karnataka are at Annexure–I
- 4,062 students/professionals have been trained in Karnataka through IISc Bengaluru, NIT Surathkal, C-DAC Bengaluru and VTU Belagavi
- 1,451 Government officials have been trained in 47 specialised cybersecurity programmes by CDAC, Bangalore and Education and Research Network of India

11. **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 first Tuesday of February
- Swachhta Pakhwada (1st –15th February), and
- Cyber Jagrookta Diwas (CJD) on the first Wednesday of every month

12. **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.

53 training programs have been conducted covering around 32,000 participants during the year 2024 and 2025 (Up to November). These include over 1,900 participants from Karnataka.

CERT-In also regularly shares awareness material through its official websites and social media handles. This is for sensitizing internet users on cyber security attacks, frauds and prevention measures.

13. **Digital Personal Data Protection Act, 2023** establishes the legal framework governing the processing of digital personal data in India. The Act and Digital Personal Data Protection Rules, 2025 have been notified on 13th November 2025.

The Act requires all Data Fiduciaries to ensure lawful processing of personal data, with clear obligations relating to transparency, purpose limitation, data minimization, accuracy, security safeguards, timely erasure, and respect for the rights of Data Principals.

It mandates prompt notification of personal data breaches to both affected individuals and the Data Protection Board of India.

The Act and Rules require Data Fiduciaries to implement appropriate security safeguards, such as encryption or masking, to protect data and prevent breaches.

The Government is also ensuring widespread awareness and adoption of the DPDP Act by educating citizens on their rights and responsibilities.

14. **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011** have been notified under section 43A of the Information Technology Act, 2000.

These Rules govern protection of sensitive personal data and will remain in force until the obligations under the DPDP Act come into force. The SPDI Rules, inter alia, mandate that:

- Sensitive personal data must be collected and used only for the stated purpose and kept secure.
- Organizations handling sensitive personal data must publish a privacy policy detailing how sensitive personal data will be used.
- Prior consent of the data provider is required for disclosure to any third party.

****

**Awareness Workshops (District-wise) conducted in Karnataka
under ISEA Project**

S. No.	District Name	Number of Workshops	Number of Participants
1	Bagalkote	22	671
2	Ballari	2	190
3	Belagavi	3	225
4	Bengaluru Rural	1	54
5	Bengaluru Urban	163	15,324
6	Bidar	1	200
7	Chamarajanagara	1	106
8	Chikkaballapura	8	1,227
9	Chikkamagaluru	4	286
10	Chitradurga	2	208
11	Dakshina Kannada	23	2,908
12	Davangere	5	2,445
13	Dharwad	1	68
14	Gadag	3	300
15	Hassan	2	279
16	Haveri	1	85
17	Kalaburagi	2	300
18	Kodagu	2	140
19	Kolar	3	635
20	Koppal	1	90
21	Mandya	2	145
22	Mysuru	10	1,057
23	Raichur	3	272
24	Ramanagara	2	321
25	Shivamogga	3	555
26	Tumakuru	1	250
27	Udupi	2	439
28	Uttara Kannada	7	644
29	Vijayanagar	1	105
30	Vijayapura	1	180
31	Yadgir	3	340

	Total	285	30,049

****