

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**LOK SABHA**  
**UNSTARRED QUESTION NO. 4515**  
TO BE ANSWERED ON: 20.08.2025

**NATIONAL VISION FOR GOVERNANCE REFORMS IN AMRIT KAAL**

**4515. SMT. ROOPKUMARI CHOUDHARY:**

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

- (a) the key strategic pillars of the Amrit Kaal vision (2022–2047) with measures to bridge regional disparities and enhance institutional transparency through real-time open-data platforms;
- (b) the extent to which emerging technologies Artificial Intelligence (AI) under the National AI Strategy, blockchain for land records and ONDC have been integrated into core public services by mid-2025 and the targets for their wider adoption by 2027; and
- (c) the measures enacted to ensure robust cybersecurity, data privacy and governance frameworks across AI, blockchain and ONDC platforms integrated into public services including the institutional arrangements, policy guidelines and the timeline for achieving full compliance by 2027?

**ANSWER**

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

(a): The key strategic pillars of Amrit Kaal vision (2022-2047) are focussed on creating an inclusive, transparent, and equitable governance ecosystem through the extensive use of digital technologies with real-time data accessibility. The Government's core initiative includes:

- i. AIKosh platform: The Aikosh platform under IndiaAI mission provides seamless access to AI ready datasets, models, computational resources, tools, community features and secure based access mechanism; including AI sandbox for innovation.
- ii. Open Government Data platform: The OGD platform is a globally recognized platform (<https://data.gov.in>) enabling institutional transparency by allowing accessibility of government-shared open data by Central/State Ministries and Departments.
- iii. Multilingual and Accessible Design: Bhashini – a national language translation mission enabling voice-first multilingual solutions to bridge the digital literacy and language divide, ensuring access to digital services in multiple Indian languages.
- iv. Digital Literacy (PMGDISHA): Provided digital literacy to over 63.9 million citizens, focusing on vulnerable groups, with capacity-building initiatives to enhance adoption of digital services.
- v. Digital Public Infrastructure (DPI) – Platforms like Aadhaar, DigiLocker, UMANG and UPI enable equitable, population-scale access to public and private services, reducing regional disparities in digital service delivery.

These measures collectively address disparities, and provide citizens with reliable, quick, and transparent access to government schemes and digital services. All Government Ministries/Departments are taking measures to enhance institutional transparency through accessibility of real time open data to citizens and bridging the regional disparities at their respective level.

(b): The emerging technologies such as AI, Blockchain are at the forefront of the technological advancement in core public services. Programmes such as “Digital India” has served as a foundational framework for this technological advancement with a clear focus on enhancing citizen centric service delivery. Further, Open protocol such as ONDC has witnessed rapid adoption and growth, transforming the digital commerce landscape. The Government is advancing to utilise the emerging technologies in following way:

- i. India’s AI strategy: Government launched IndiaAI mission in March 2024 as a strategic initiative to establish a robust and inclusive AI ecosystem aligned with India's development goals. The IndiaAI mission comprises of the following key pillars:
  - IndiaAI Compute Capacity
  - IndiaAI Foundation Models
  - AIKosh
  - IndiaAI Application Development Initiative
  - IndiaAIFutureSkills
  - IndiaAI Startup Financing
  - Safe & Trusted AI

The Government has actively worked on integrating the AI into core public services. IndiaAI application development, a pillar of IndiaAI mission, is developing, deploying and adopting the AI application in various public service sector including education, health etc.

- ii. Blockchain Technology: The Government of India has taken progressive steps to integrate blockchain technology into land record management as part of its broader digital governance initiatives, to ensure transparency, accountability and streamline property transactions. The UT of Chandigarh and the State of Telangana have piloted and demonstrated the potential of blockchain in maintaining tamper proof and immutable land records. These measures showcase the government’s commitment to using new technologies to improve public services
- iii. Open Network for Digital Commerce (ONDC): It is an initiative of the DPIIT, Ministry of Commerce and Industry, promoting open networks for all aspects of the exchange of goods and services over digital or electronic networks. It is an open protocol on which platforms/marketplace can be built.

Ministries/Departments at the centre are driving the adoption of ONDC to empower small businesses, retailers, artisans, and suppliers. Notable measures taken are as under:

- The Ministry of Micro, Small and Medium Enterprises has launched Trade Enablement and Marketing (TEAM) scheme, which facilitates the onboarding of

micro and small enterprises onto ONDC by providing financial assistance for onboarding, cataloguing, account management, logistics, packaging material and design.

- eSaras.in, the e-commerce platform under National Rural Livelihood Mission (NRLM) of Ministry of Rural Development, is live on ONDC - with operations through a central warehouse in DELHI-NCR. e-Saras is integrated with ONDC with some 800+ handcrafted products made by Self Help Groups (SHGs) and are available online.
- Common Services Centre (CSC's) have gone live on ONDC to connect villages in India to the national digital market.

Apart from above initiatives each Ministry/Department are leveraging AI, blockchain and Emerging technologies for effective delivery of services.

(c): The government has taken proactive steps in establishing strong cybersecurity, data privacy, and good governance frameworks for integration of emerging technologies such as AI, Blockchain and ONDC into public services. Government remains cognizant and aware of cyber threats and challenges. Following measures have been taken to strengthen cybersecurity 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) project is being implemented by CERT-In. NCCC examines the cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.
- iii. 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.
- iv. 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.
- v. Regular training workshops are conducted for cybersecurity professionals, government employees, police and law enforcement professionals, lawyers and public prosecutors, students, etc.
- vi. The Insurance Regulatory and Development Authority of India (IRDAI) also issues cybersecurity guidelines for regulated entities including insurers, brokers, corporate agents, 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

Legal provisions:

- i. In order to ensure data protection, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 ('SPDI Rules') mandates reasonable security practices and procedures for body corporate or any person on its behalf, handling sensitive personal data or information.
- ii. In order to safeguard the personal data of individuals and ensure that their data is shared only with their consent, the Digital Personal Data Protection Act, 2023 (DPDP Act) has been enacted. The DPDP Act is aimed at safeguarding the personal data of individuals and ensuring processing of personal data for the lawful purposes.
- iii. As per the Act, appropriate technical and organisational measures must be implemented for processing of the personal data and reasonable security safeguards must be taken to prevent any personal data breach.

\*\*\*\*\*

