GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3259
TO BE ANSWERED ON: 20.03.2026

DATA BREACHES AND CYBER SECURITY PREPAREDNESS FOR DIGITAL CENSUS

3259. SMT. RENUKA CHOWDHURY:

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

(a) the total number of reported instances of data breaches, leaks or cyber attacks involving Aadhaar data or other major Government databases since 2021, year-wise;
(b) the action taken in each such case, including investigations, penalties and corrective cybersecurity measures;
(c) whether Government has assessed the risks arising from shifting the Census to a fully digital, app- and web-based data collection system covering over one billion citizens; and
(d) the cybersecurity architecture and safeguards proposed for the digital Census, including encryption, access control, device security and data storage within sovereign Government infrastructure?

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 secure and trustworthy cyberspace while taking active measures to mitigate risk to India's digital infrastructure and Government services.

The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cybersecurity incidents under the provisions of Section 70B of the Information Technology (IT) Act, 2000.

CERT-In observes and tracks cybersecurity incidents in Indian cyberspace, including platforms managed by Government. CERT-In coordinates incident prevention and response measures with organisations, service providers and sector regulators.

No breach of data has occurred from the Central Identities Data Repository (CIDR) maintained by the Unique Identification Authority of India (UIDAI).

UIDAI has put comprehensive measures in place to protect the personal data of Aadhaar number holders. It has implemented multi-layered security infrastructure with the defence-in-depth concept to protect the CIDR database and continuously reviews/audits the same to protect UIDAI systems.

Further, CIDR is declared as a protected system under Section 70 of the IT Act 2000. The National Critical Information Infrastructure Protection Centre (NCIIPC) provides security advice to maintain its cybersecurity posture. UIDAI uses advanced encryption technologies for protecting data in transmission and storage.

UIDAI's 'Information Security Management System' is ISO 27001:2022 certified and has also implemented a 'Privacy Information Management System', which is ISO/IEC 27701:2019 certified.

The Office of the Registrar General and Census Commissioner of India (ORGI & CCI) has undertaken a comprehensive, multi-agency risk assessment covering all major components for the conduct of the Census of India, 2027, using digital means.

ORGI & CCI have deployed a comprehensive, defence-in-depth cybersecurity architecture across all layers of the infrastructure for the conduct of Census of India, 2027. The security of infrastructure is strengthened through implementation of access control, device security, user device binding, network security and Security Operations Centre (SOC).

The National Data Centre and Disaster Recovery sites of ORGI & CCI has also been notified as Critical Information Infrastructure (CII) under Section 70 of the IT Act 2000.

****