GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1348
TO BE ANSWERED ON: 06.12.2024

LEAKAGE OF AADHAR AND PASSPORT DATA

1348. SHRI P. WILSON:

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

(a) whether personal data of 81.5 crore Indian including Aadhar and passport details are being leaked from Indian Council of Medical Research (ICMR) and sold in dark web as claimed by American cybersecurity firm, if so, the details of extent of leakage
(b) the details of total number of data leaks reported during the past five years; and
(c) the details of steps taken to prevent leakage of data?

ANSWER

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

(a) to (c) : There has been no breach of Aadhaar data from the Central Identities Data Repository (CIDR) maintained by the Unique Identification Authority of India (UIDAI).

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. On reporting of cyber security incidents, CERT-In advises remedial measures to concerned organisations.

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

Year	Number of cyber security incidents
2019	394499
2020	1158208
2021	1402809
2022	1391457
2023	1592917

The Government is fully cognizant and aware of various cyber security threats and challenges and has taken following measures to protect data including Aadhar and Passport data of the citizens:

i. UIDAI has put comprehensive measures in place to protect the personal data of Aadhaar number holders. It has implemented multi-layered security infrastructure with defence-in-depth concept to protect the Central Identities Data Repository (CIDR) database and continuously reviews/audits the same to protect UIDAI systems. Further, CIDR is declared as a protected system and the National Critical Information Infrastructure Protection Centre provides security inputs on an ongoing basis to maintain its cybersecurity posture. UIDAI uses advanced encryption technologies for protecting data in transmission and storage.

ii. UIDAI's Information Security Management System is ISO 27001:2013certified. UIDAI is also certified for ISO/IEC 27701:2019 (Privacy Information Management System). An independent audit agency is engaged for the creation of the Governance, Risk, Compliance and Performance framework for the Aadhaar ecosystem and oversight for adherence to the same.

iii. Indian Council of Medical Research (ICMR) has actively coordinated with various agencies to enhance security measures and bolster defences against cyber threats.

iv. A Zero trust security framework has been deployed with 7-Layers of security in the passport seva programme (PSP). Security Operational Centre (SOC) is also in place to monitor security related incidence and required mitigation on 24x7x365 basis. Apart from this all compliances aligned to ISO27001:2022.

v. MeitY has issued Guidelines for Cybersecurity Audit that cover both comprehensive and limited audit on periodic basis by competent auditors with clear responsibilities for ensuring such audit regularly, inclusive of vulnerability assessment and penetration testing.

vi. The Digital Personal Data Protection Act, 2023 (The DPDP Act) provides for the processing of digital personal data in a manner that recognizes the need to process personal data for lawful purposes by the data fiduciaries.

vii. CERT-In has issued an advisory to various Ministries outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.

viii. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

ix. CERT-In has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

x. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats

xi. NIC mandates periodic security audits of government websites and applications through CERT-In-empaneled agencies to eliminate vulnerabilities and ensure compliance with global security standards and Vulnerability Assessment of the underlying hardware on which such applications are hosted.

xii. A dedicated cyber security team is operational under NIC CERT to detect, prevent, and respond to cyber incidents. The team monitors, detects, and mitigates cybersecurity threats related to applications hosted at NIC Data Centres and ICT infrastructure managed by NIC.

xiii. Various advanced security tools including Threat Intelligence Platform has been deployed by NIC to identify the security issues associated with Government network.

****