GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 1526
TO BE ANSWERED ON: 15.12.2023

LEAKS OF AADHAAR AND OTHER DATA ON DARK WEB

1526. SMT. PHULO DEVI NETAM:

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

(a) whether the Government is aware of the alleged Aadhaar and other data leaks on the dark web;
(b) if so, the steps Government has taken to respond to this data leak, if not, the reasons therefor;
(c) whether Government has taken steps to strengthen security of Aadhaar data of the citizens; and
(d) if so, the details thereof, if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) to (d): The Government has taken following measures to protect data including Aadhaar data of the citizens:

a. 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.
b. UIDAI's Information Security Management System is ISO 27001:2013-certified. UIDAI is also certified ISO/IEC 27701:2019 (Privacy Information Management System).
c. 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.
d. 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.
e. On observing data breach / data leak incidents, CERT-In notifies the affected organisations along with remedial actions to be taken and coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as Law Enforcement Agencies.

f. 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.

g. A special advisory on security practices to enhance resilience of health sector entities has been communicated by CERT-In to the Ministry of Health and Family Welfare, for sensitising health sector entities regarding latest cyber security threats in December 2022. The Ministry has been requested to disseminate the advisory among all authorised medical care entities / service providers in the country.

h. National Informatics Centre (NIC) provides IT support to user ministries, departments and agencies of the Central Government, State Governments and district administrations for various e-governance solutions and, as part of this, helps maintain various government databases that contain data of citizens. NIC follows information security policies and practices in line with industry standards and practices, aimed at preventing cyber-attacks and safeguarding data.

****