GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 2132
TO BE ANSWERED ON: 09.08.2024

LEAKAGE OF PERSONAL DATA ON DARK WEB

2132. SHRI A. D. SINGH:

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

(a) whether it is a fact that an American Cyber Security Company has claimed that personal identifiable information of many Indian citizens including Aadhar and Passport details are being sold on Dark Web;
(b) if so, the details and the extent of leakage;
(c) whether the matter has been investigated, if so, the details thereof;
(d) the threat level due to data leakage; and
(e) the efforts being made to protect the personal data of the citizens effectively?

ANSWER

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

(a) to (e): 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 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) 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.

(iv) 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.

(v) 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.

(vi) 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 to prevent cyber-attacks and safeguard data.

(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) CERT-In has empanelled 176 security auditing organisations to support and audit implementation of Information Security Best Practices.

(ix) CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

(x) 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.

(xi) 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.

(xii) Cybersecurity mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. 92 such drills have been conducted by CERT-In where around 1400 organizations from different States and sectors participated.

(xiii) 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.

******