Press Statement 05.03.2017

During the last few days, some news items and articles have appeared in various print and social media alleging breach of Aadhaar data, misuse of biometrics, breach of privacy, and creation of parallel databases etc. The UIDAI has carefully gone into these reports and would like to emphasise that there has been no breach to UIDAI database of Aadhaar in any manner whatsoever and personal data of individuals held by UIDAI is fully safe and secure.

2.   So far as the incident of misuse of biometrics reported in a leading newspaper is concerned, it is an isolated case of an employee working with a bank's Business Correspondent's company making an attempt to misusehis own biometrics which was detected by UIDAI internal security system and subsequently actions under the Aadhaar Act have been initiated.

3.   During the last five years, more than 400 crore Aadhaar authentication transactions have taken place and to the best of knowledge of UIDAI no incident of misuse of biometrics leading to identity theft and financial loss has been taken place. Aadhaar based authentication is robust and secure as compared to any other contemporary systems. Aadhaar system has the capability to inquire into any instance of misuse of Aadhaar biometrics and identity theft and initiate action.

4.   UIDAI uses one of world's most advanced encryption technologies in transmission and storage of data. As a result, during the last 7 seven years, there has been no report of breach or leak of residents' data out of UIDAI.

5.   It may be emphasised that UIDAI is continuously updating its security parameters looking at the new threats in cyber space. It also

undertakes security audits and takes necessary steps to augment its security features. It is in this direction that the UIDAI has decided to have registered devices for capturing biometrics data and further that such biometrics will be encrypted at the point of capture itself. This will further strengthen the security features of Aadhaar eco system.

6.   There have also been some media reports about on boarding of the ecosystem partners, misuse of e-KYC data by various agencies and also allegations that the e-KYC API is available in public domain. Further, the reports also state that there are no extant regulations available to prevent storage and misuse of e-KYC data while citing instances like capturing IRIS from high resolution photograph.

7.   In this regard, the regulations under the Aadhaar Act strictly regulate the on-boarding, functioning including the data sharing restrictions imposed on the companies which want to use Aadhaar information. E-KYC APIs are available only to authorized Authentication User Agencies (AUAs) and e-KYC User agencies (KUAs) through authorized Authentication Service agencies (ASAs) which have established secured network connectivity for the purpose of authentication with the CIDR, in compliance with the Regulations, specifications, standards and technology architecture as prescribed by UIDAI. Further, there are stringent provisions in the Aadhaar (Authentication) Regulations governing the usage of e-KYC data including storage and sharing, resident consent being paramount in both the cases. Any unauthorized capture of IRIS or fingerprints or storage or replay of biometrics or their misuse is a criminal offence under the Aadhaar Act.

8.   The news reports also speak of private agencies hired by mobile operators and banks for eKYC leading to availability of these data in parallel database and the vulnerabilities in the scenario where there is no

Privacy Law in the country.

9.   Aadhaar authentication or eKYC is only available to authorised agencies whose appointment, responsibilities, statutory obligations, penal provisions for contraventions are clearly provided for in the Aadhaar Act and the regulations framed thereunder. Banks or mobile operators have to become UIDAI's AUA/ASAs to obtain E-KYC data of their customers from UIDAI. The E-KYC data can be given by UIDAI to these agencies only after they obtain consent of their customers and can be used only for the purpose for which it was obtained. For example,a telecom operator can obtain the E-KYC data of its subscribers and will keep them in their records without biometrics and use them only for the purpose of proving telecom services. Similarly a bank, after obtaining the E-KYC information of its account holders, will keep the information without their biometrics within the bank and will use it only for the purpose of providing banking services and cannot use it for any other purpose without obtaining consent of the customer. Violations of above provisions attract strict penalties under the Aadhaar Act which will be enforced strictly.

10.Aadhaar is also an important tool of good governance and empowerment of people. It has helped more than 4.47 crore people to open bank accounts through Aadhaar E-KYC. It has enabled the government to do Direct Benefit Transfer under various schemes such as LPG Subsidy under Pahal, Scholarships, MNREGA, and Pensions directly into the bank accounts of beneficiaries eliminating corruption, diversion, and leakages by middlemen etc. Through Aadhaar based Direct Benefit Transfers the government has saved over Rs 49,000 Crore during the last two and half years. Aadhaar based Public Distributions System is benefitting people by ensuring the their food grain entitlement are given only to the deserving beneficiaries and are not cornered by unscrupulous and corrupt elements. These are just few examples of how

Aadhaar is changing lives of common men and women of India, a task that the UIDAI is steadfastly committed to performing in a citizen-friendly, inclusive and secure manner.

****