

GOVERNMENT OF INDIA

MINISTRY OF PLANNING

LOK SABHA

UNSTARRED QUESTION NO: 4158

ANSWERED ON:19.12.2012

BIO METRIC EXCEPTION CLAUSE FOR AADHAR

ANURAG SINGH THAKUR

(a) whether there is a 'bio-metric exception' clause in the protocol for registration under Aadhar;

(b)if so, the details thereof;

(c)whether a large number of enrolments have been made in many States without providing bio-metric identification and if so, the details thereof, State-wise;

(d)whether the Government has a mechanism to verify details such as residential address of each individual enrolling under the scheme before the issue of Aadhaar Numbers and if so, the details thereof;

(e)if not, the number of individuals who have been issued number without complete verification of details provided; and

(f)the steps taken by the Government to make Aadhar system foolproof?

Will the Minister of PLANNING be pleased to state:-

ANSWER

MINISTER OF STATE FOR PARLIAMENTARY AFFAIRS & PLANNING (SHRI RAJEEV SHUKLA)

(a): Yes Madam.

(b): Aadhaar provides unique identity to a resident based on his/her demographic and biometric information. The biometric information collected as part of Aadhaar enrolment includes photograph, all 10 fingerprints and 2 iris images. However, to ensure that no resident is denied an opportunity to enroll in the absence of some or all biometrics, Aadhaar enrolment process also has provision for enrolling such persons, under biometric exception (BE) enrolment. This is in line with the principle of universal inclusion followed by UIDAI in Aadhaar enrolments. The exception enrolment requires photograph of missing fingers/hand/eyes in such a manner that the proof of missing biometrics is recorded in the data base. All exception enrolments are to be signed off by the enrolment operators and approved by the supervisor of the Enrolment Agency. At the backend, systems exist to carry out demographic de-duplication in respect of such enrolments. Furthermore, all 100% biometric exception data packets undergo manual check at the backend.

(c): A few instances of false biometric exception enrollments have been found in some States. These cases were manually scrutinized and Aadhaar numbers have been cancelled in some cases while some cases are under investigation. It was also observed that some of these cases were genuine biometric exception enrolments and Aadhaar numbers have been generated against such cases. State wise details of such enrolments is at Annexure-I.

(d) & (e) : The basic objective of the Aadhaar project is inclusion. The enrolments under the project can be based on

(i) documents and

(ii) introducer. For document based enrolments, the resident must be enrolled on the basis of Proof of Identity(PoI) & Proof of Address(PoA). The list of documents acceptable as PoI & PoA are at Annex-II. For residents who do not have documentary Proof of Identity and Address, the concept of trusted introducers is used to facilitate their enrolment as per recommendation of the Demographic Data Standards and Verification Procedures Committee (DDSVPC). Introducers can be people from various walks of life such as elected members, members of local bodies, postmen, local officials such as Anganwadi/ASHA workers, representatives of local NGOs etc. The list of Introducers has to be duly notified by the Registrars and the introducers themselves should have an Aadhaar number based on approved documents.

(f): UIDAI has put in place standardized procedures/processes for enrolment across the country, in accordance with the recommendations of Demographic Data Standards & Verification Process Committee Report and the Biometrics Standards Committee Report. UIDAI has prescribed a standardized software for enrolment of residents. The enrolment is carried out by operators after certification. They are properly tagged to an enrolment agency and registrars for ensuring traceability in future. Each enrolment station is also duly registered with the Central Identities Data Repository (CIDR) at Bangalore before it is permitted to undertake enrolments, and before any data packet is taken up for processing and validation check for the enrollment machines and operator is carried out. In addition, a number of processes have been put in place to ensure that the data collected by UIDAI is not accessed in any unauthorized manner. These include encryption of data at source, immediately on completion of enrolment; transfer of data to the data centre in encrypted and zipped format which is tamper proof; putting standard security infrastructure such as virtual providers, firewalls and intrusion prevention system in place and limiting physical access to UIDAI infrastructure and data to authorized personnel only. UIDAI has

also issued data protection and security guidelines for Registrars, Enrolment Agencies, Logistics Service Providers, UIDAI Employees, Authentication User Agencies, and Data Centre Service Providers, Standardization, testing and Quality Certification(STQC) Directorate has done the audit of the UIDAI software applications and IT infrastructure Security Audit for Data Centres.