

OFFICE OF THE COMPTROLLER AND AUDITOR GENERAL OF INDIA

**New Delhi
06 April, 2022**

**AUDIT REPORT ON 'FUNCTIONING OF UNIQUE IDENTIFICATION
AUTHORITY OF INDIA' PRESENTED**

Performance Audit Report No. 24 of 2021 on 'Functioning of Unique Identification Authority of India- Union Government, Ministry of Electronics and Information Technology was tabled in Lok Sabha on 5.4.22 and in Rajya Sabha here today.

This Report of the Comptroller and Auditor General of India contains significant observations and recommendations emanating out of the Performance Audit conducted on 'Functioning of Unique Identification Authority of India'.

The Performance Audit included assessment of the Enrolment and Update Ecosystems as well as the Authentication Ecosystems of the UIDAI for the period from 2014-15 to 2018-19. The figures have been updated wherever received up to March 2021. Audit scrutinised the processes beginning right from the enrolment, up to delivery of Aadhaar number and subsequent use of the authentication services. The systems put in place for maintaining security and confidentiality of data were also subject to audit examination.

The Report contains seven Chapters. **Chapter 1** gives introduction to the topic. **Chapter 2** explains the audit scope, audit objectives, audit criteria and audit methodology applied along-with the good practices followed by the Authority and the constraints faced during audit. **Chapter 3** describe the audit findings relating to "Enrolment and Update Ecosystem" and "Authentication Ecosystem" whereas **Chapter 4** contains audit findings on "Management of Finances and Contracts". **Chapter 5** and **Chapter 6** are related to "Security of Aadhaar information system" and "Redressal of Customer Grievances" respectively. Finally, **Chapter 7** gives the conclusion of the Audit Report.

A.

SUMMARY OF PERFORMANCE OF UIDAI

UIDAI has responsibility to issue a Unique Identification (UID) to all residents, that was robust enough to eliminate duplicate or fake identities and could be verified and authenticated anytime, anywhere. The digital identity platform set up by UIDAI with the brand name 'Aadhaar', generated the first UID in September 2010. The Aadhaar database has since reached 129.04 Crore by March 2021 and is considered as one of the largest biometric based identification systems in the world. Aadhaar is now established as an important identity

document for residents. Various Ministries/Departments of the Government as well as other entities such as banks, mobile operators, rely upon Aadhaar for identity of the applicant. During 2020-2021, UIDAI authenticated 1524.65 Crore transactions which included 111.25 Crore e-KYC transactions. During 2020-21, UIDAI earned revenue of ₹ 331.65 Crore.

A1.

SIGNIFICANT AUDIT FINDINGS

- The Aadhaar Act stipulates that an individual should reside in India for a period of 182 days or more in the twelve months immediately preceding the date of application for being eligible to obtain an Aadhaar. In September 2019, this condition was relaxed for non-resident Indians, holding valid Indian Passport. However, UIDAI has not prescribed any specific proof/ document or process for confirming whether an applicant has resided in India for the specified period and takes confirmation of the residential status through a casual self-declaration from the applicant. There was no system in place to check the affirmations of the applicant. As such, there is no assurance that all the Aadhaar holders in the country are 'Residents' as defined in the Aadhaar Act.

(Paragraph 3.2.1)

- Uniqueness of identity of the Applicant, established through a de-duplication process is the most important feature of Aadhaar. It was seen that UIDAI had to cancel more than 4.75 lakh Aadhaars (November 2019) for being duplicate. There were instances of issue of Aadhaars with the same biometric data to different residents indicating flaws in the de-duplication process and issue of Aadhaars on faulty biometrics and documents. Though UIDAI has taken action to improve the quality of the biometrics and has also introduced iris-based authentication features for enrolment for Aadhaar, the database continued to have faulty Aadhaars which were already issued.

(Paragraph 3.2.2)

- Issue of Aadhaar numbers to minor children below the age of five, based on the bio metrics of their parents, without confirming uniqueness of biometric identity goes against the basic tenet of the Aadhaar Act. Apart from being violative of the statutory provisions, the UIDAI has also incurred avoidable expenditure of ₹310 Crore on issue of Bal Aadhaars till 31 March 2019. In Phase- II of ICT assistance a further sum of ₹288.11 Crore was released upto the year 2020-21 to states/ schools primarily for issue of Aadhaars to minor children. The UIDAI needs to review the issue of Aadhaar to minor children below five years and find alternate ways to establish their unique identity, especially since the Supreme Court has stated that no benefit will be denied to any child for want of Aadhaar document.

(Paragraph 3.2.3)

- All Aadhaar numbers were not paired with the documents relating to personal information of their holders and even after nearly ten years the UIDAI could not identify the exact extent of mismatch. Though with the introduction of inline scanning (July 2016) the personal information documents were stored in CIDR, existence of unpaired biometric data of earlier period indicated deficient data management.

(Paragraph 3.2.4)

- During 2018-19 more than 73 *per cent* of the total 3.04 Crore biometric updates, were voluntary updates done by residents for faulty biometrics after payment of charges. Huge volume of voluntary updates indicated that the quality of data captured to issue initial Aadhaar was not good enough to establish uniqueness of identity.

(Paragraph 3.3.1)

- UIDAI did not have a system to analyze the factors leading to authentication errors.

(Paragraph 3.5.1)

- UIDAI did not carry out verification of the infrastructure and technical support of Requesting Entities and Authentication Service Agencies before their appointment in the Authentication Ecosystem, despite stipulations in Aadhaar (Authentication) Regulations.

(Paragraph 3.5.2)

- UIDAI is maintaining one of the largest biometric databases in the world; but did not have a data archiving policy, which is considered to be a vital storage management best practice.

(Paragraph 3.6.1)

- UIDAI's arrangements with the Department of Posts were not adequate to guarantee delivery of Aadhaar letters to the right addressee, as seen from the large number of Aadhaar letters being returned as undelivered.

(Paragraph 3.6.2)

- UIDAI provided Authentication services to banks, mobile operators and other agencies free of charge till March 2019, contrary to the provisions of their own Regulations, depriving revenue to the Government.

(Paragraph 4.2.1)

- UIDAI did not penalise the Managed Service Provider for failure to achieve the expected service levels in the performance of biometric solutions.

(Paragraph 4.4.1)

- The support services to States by way of a State Resource Personnel to be provided by National Institute of Smart Governance (NISG) through the ICT assistance given to them, was duly approved by the Cabinet Committee for one year only, but the same continued for years together as approved by UIDAI.

(Paragraph 4.4.2.1)

- There was deficiency in assessment of the requirements for Field Service Engineers (FSE) resources to be hired from NISG and in monitoring the payments made to them.

(Paragraph 4.4.2.2)

- UIDAI could not avail rebate on franking values worth ₹30.19 Crore offered by the Department of Posts due to deficiency in their agreements with Print Service Providers.

(Paragraph 4.4.3)

- UIDAI had not effectively monitored funds released to States as Grants-in-Aid towards ICT assistance for creating infrastructure.

(Paragraph 4.4.4)

- Monitoring of the information system operations of authentication ecosystem partners was deficient to the extent that UIDAI could not confirm compliance to its own regulations.

(Paragraphs 5.2)

- The process of capturing of grievances/complaints has not been streamlined and does not display a clear picture for analysis. Also the complaints lodged at the RO level did not get the attention of UIDAI HQ, compromising the effectiveness of the grievance redressal mechanism, besides the delays in settlement of grievances.

(Paragraphs 6.2)

- ❖ UIDAI may prescribe a procedure and required documentation other than self-declaration, in order to confirm and authenticate the residence status of applicants, in line with the provisions of the Aadhaar Act.
(Paragraph 3.2.1)
- ❖ UIDAI may tighten the SLA parameters of Biometric Service Providers (BSPs), devise foolproof mechanisms for capturing unique biometric data and improve upon their monitoring systems to proactively identify and take action to minimize, multiple/ duplicate Aadhaar numbers generated. UIDAI may also review a regular updation of technology. UIDAI also needs to strengthen the Automated Biometric Identification System so that generation of multiple/duplicate Aadhaars can be curbed at the initial stage itself.
(Paragraph 3.2.2)
- ❖ UIDAI may explore alternate ways to capture uniqueness of biometric identity for minor children below five years since uniqueness of identity is the most distinctive feature of Aadhaar established through biometrics of the individual.
(Paragraph 3.2.3)
- ❖ UIDAI may take proactive steps to identify and fill the missing documents in their database at the earliest, in order to avoid any legal complications or inconvenience to holders of Aadhaar issued prior to 2016.
(Paragraph 3.2.4)
- ❖ UIDAI may review charging of fees for voluntary update of residents' biometrics, since they (UIDAI) were not in a position to identify reasons for biometric failures and residents were not at fault for capture of poor quality of biometrics.
(Paragraph 3.3.1)
- ❖ UIDAI may make efforts to improve the success rate of authentication transactions by analysing failure cases.
(Paragraph 3.5.1)
- ❖ UIDAI may conduct thorough verification of the documents, infrastructure, and technological support claimed to be available, before on-boarding the entities (Requesting Entities and Authentication Service Agencies) in the Aadhaar ecosystem.
(Paragraph 3.5.2)
- ❖ UIDAI may frame a suitable data archival policy to mitigate the risk of vulnerability to data protection and reduce saturation of valuable data space due to redundant and unwanted data, by continuous weeding out of unwanted data
(Paragraph 3.6.1)
- ❖ UIDAI may address the delivery problems with their logistic partner namely DoP, by designing a customized delivery model, which will ensure delivery of Aadhaar letters to the correct addressee.
(Paragraph 3.6.2)
- ❖ UIDAI needs to be alert and cautious in matters concerning charges for delivery of services and ensure that decisions for non-levy of charges are taken with due process and approvals, which are properly documented and available for verification by any stake holder.

(Paragraph 4.2.1)

- ❖ UIDAI may levy penalties on Biometric Service Providers for deficiencies in their performance in respect of biometric de-duplication (FPIR/ FNIR) and biometric authentication (FMR/ FNMR). Agreements in this regard should be modified, if required

(Paragraph 4.4.1)

- ❖ UIDAI have to accept their own responsibility for issue of Aadhaar and limit/reduce their continued reliance on other agencies for support. They may partner with State Governments to increase the enrolment functions for issue of Aadhaar.

(Paragraph 4.4.2.1)

- ❖ UIDAI should strictly follow the standards of financial propriety while procuring services and ensure that advances are not paid for in excess of requirements.

(Paragraph 4.4.2.2)

- ❖ UIDAI may incorporate suitable clauses in their Agreements with all agencies mentioning clearly that the benefits accruing due to UIDAI's resources need to be passed on to them and vendors to indemnify UIDAI towards the loss/ cost arising due to their actions.

(Paragraph 4.4.3)

- ❖ UIDAI may improve upon its financial management of grants given to State Authorities by proper monitoring and ensuring regular and timely receipt of Utilization Certificates from them. It may also discontinue monetary assistance given to States/schools and other agencies for enrolment of minor children below five for issue of Aadhaar numbers.

(Paragraph 4.4.4)

- ❖ UIDAI may ensure that each of the existing REs and ASAs are audited by them or by the Auditor appointed by it within a cycle of three years so as to provide adequate assurance about compliance to the Regulations.
- ❖ UIDAI may consider suspension of the services of REs and ASAs if they fail to conduct annual audit in time as prescribed by the Regulations 2016.
- ❖ UIDAI may ensure the implementation of Aadhaar Data Vault process and institute/carry out periodic audits independently, to enhance the security of Aadhaar number storage data by user organizations. UIDAI may deal the cases of non-compliance of directions as per the Act and as per conditions in the agreement with AUAs/KUAs (Authentication User Agencies and e-KYC User Agencies)

(Paragraphs 5.2.1, 5.2.2 and 5.2.3)

- ❖ UIDAI may explore the possibility of introducing a single centralized system where grievances/complaints lodged even at ROs are also captured so as to enhance the quality of customer servicing.

(Paragraphs 6.2.1 and 6.2.2)

BSC/SS/TT/5/22