



**Report of the
Comptroller and Auditor General of India
on
Functioning of
Unique Identification Authority of India**



लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest



**Union Government
(Ministry of Electronics and Information Technology)
Report No. 24 of 2021
(Performance Audit)**

**Report of the
Comptroller and Auditor General of India**



लोकहितार्थं सत्यनिष्ठा
Dedicated to Truth in Public Interest

on

**Functioning of Unique Identification Authority of
India**

**Union Government
(Ministry of Electronics and Information Technology)
(Performance Audit)**

Report No. 24 of 2021

CONTENTS

Para	Title	Pages
	Executive Summary	v-x
	Chapter 1-Introduction	1-6
1.1	Introduction	1
1.2	Constitutional validity of Aadhaar	2
1.3	UIDAI Authority	3
1.3.1	Powers of the Authority	3
1.3.2	Organizational Set-up	4
1.3.3	Registrars	5
1.3.4	Enrolment Agencies	5
1.4	Legislation, Rules and Regulations	6
1.5	Structure of the Report	6
	Chapter 2-Scope of Audit, Audit Objectives and Methodology	7-10
2.1	Scope of Audit	7
2.2	Audit Objectives	7
2.3	Audit Criteria	7
2.4	Audit Methodology	8
2.5	Good Practices	8
2.6	Acknowledgement and Constraints	9
	Chapter-3 Enrolment, Update and Authentication Ecosystem	11-34
3.1	Enrolment and Update Ecosystem	11
3.1.1	Key Regulations and Amendments	12
3.1.2	Status of Aadhaar Enrolment and Update	14
3.1.3	Aadhaar Saturation Status	16
3.1.4	The Components of Aadhaar Ecosystem	16
3.1.5	De-duplication process	17
3.1.6	Bio-metric Device Certification	18
3.1.7	Managed Service Provider	18
3.1.8	Governance Risk Compliance and Performance – Service Provider	18
3.2	Audit Observations on Aadhaar Enrolment Ecosystem	18
3.2.1	Verification of the ‘Resident’ status of the applicants	18

3.2.2	Generation of Multiple Aadhaar	19
3.2.3	Enrolment for Aadhaar of Minor Children below age of five years	21
3.2.4	Management of Aadhaar Documents	23
3.3	Audit Observations on Aadhaar Update Ecosystem	24
3.3.1	Voluntary Biometric Updates	25
3.4	Aadhaar Authentication Ecosystem	26
3.4.1	Aadhaar Authentication Partners	27
3.4.2	Key Regulations and Amendments	27
3.4.3	Status of Authentication Transactions	28
3.5	Audit observations on Monitoring of Ecosystem partners on compliance to the provisions of Aadhaar (Authentication) Regulations 2016	29
3.5.1	Incidences of Authentication Errors	29
3.5.2	Non verification of the infrastructure and technical support of Requesting Entities and Authentication Service Agencies	30
3.6	Other related Audit Observations	31
3.6.1	Data Archival Policy	32
3.6.2	Delivery of Aadhaar Documents	32
Chapter-4 Management of Finances and Contracts		35-48
4.1	Introduction-Budget and Finance	35
4.2	Audit Observations on Revenue Management	36
4.2.1	Non-Levy of charges for delivery of authentication services	36
4.3	Contract Management	38
4.3.1	Selection of Contracts	38
4.4	Audit Observations on Contract Management	39
4.4.1	Liquidated damages (LD) for deficient performance of biometric solutions not levied	40
4.4.2	Deficiencies in monitoring contracts with NISG	41
4.4.2.1	State Resource Personnel (SRP) contract with National Institute of Smart Governance (NISG) extended beyond the period envisaged in the ICT guidelines	43
4.4.2.2	Deficiencies in engagement of Field Service Engineers (FSE)	44
4.4.3	Rebate on Franking Values on dispatch of Aadhaar not availed	45

4.4.4	Monitoring of Information & Communication Technology (ICT) Assistance to States	46
Chapter-5 Security of Aadhaar Information System		49-54
5.1	Introduction	49
5.2	Monitoring of the activities of authentication ecosystem partners of UIDAI	49
5.2.1	Annual Information System audit of the operations of REs and ASAs	49
5.2.2	Information System Audit of Client Applications' Systems storing biometric data not ensured	52
5.2.3	Security and safety of data in Aadhaar vaults	53
Chapter-6 Redressal of Customers Grievances		55-57
6.1	Introduction	55
6.2	Audit Observations	56
6.2.1	Data on complaints and their redressal	56
6.2.2	Grievances received through CRM	56
Chapter-7 Conclusion		59-60
Appendix-I		61-68
Annexure-I		69-71
Abbreviations		72-73

Preface

This Report has been prepared for submission to the President under Article 151 of the Constitution.

The Report includes matters arising from Performance Audit of Functioning of the Unique Identification Authority of India for the period from 2014-15 to 2018-19. Statistical information on generation, update and authentication services of Aadhaar and financial information referred to in the Report have been updated upto March 2021, to the extent as furnished by UIDAI.

The audit has been conducted in conformity with the Auditing Standards issued by the Comptroller and Auditor General of India.

Executive Summary

Identification of the right individuals, especially the targeted beneficiaries, was a major stumbling block encountered by the Union and State Governments while rolling out various welfare schemes. Absence of a valid and authenticated identity document was adversely affecting implementation and delivery of various Government welfare Schemes. Citizens were required to furnish multiple documents such as passports, driving licenses and ration cards etc. as identity proofs to various Government as well as private agencies, making it inconvenient for them and especially those who did not have any of these identity documents. To overcome the challenge, the Union Government decided to introduce a unique identity (UID) for the residents of India and to implement this project, they established Unique Identification Authority of India (UIDAI) in January 2009. The Authority was mandated to lay out plans and policies to implement the “Aadhaar” project, which gave UIDAI the mandate to generate and issue Aadhaar, to the residents of India.

The first UID, a 12-digit unique number that can be authenticated digitally, with the brand name ‘Aadhaar’ was generated in September 2010. Since then, UIDAI has generated more than 129 Crore Aadhaars, till the end of March 2021 and 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.

However the Aadhaar scheme was challenged from time to time by several petitioners in various Courts of law. The five judges Constitution Bench of the Hon'ble Supreme Court in a landmark judgment of 26 September 2018, upheld the constitutional validity of the Aadhaar (Targeted delivery of Financial and Other Subsidies and Benefits) Act 2016 (the Aadhaar Act, 2016). The Court has clearly ruled on the compulsory and voluntary requirements of Aadhaar for residents for availing benefits of various schemes and services.

The UIDAI had staff strength of 130 at its Delhi Headquarters and staff strength of 219 at its Regional Headquarters at the end of March 2021. The work was being carried out by officers and staffs mostly either on deputation or from outsourced agencies. Besides UIDAI also assisted States with ICT assistance and provided State level personnel through the National Institute for Smart Governance (NISG), for creating awareness and issue of Aadhaar. The UIDAI's budget in 2020-21 was ₹613 Crore with actual expenditure of ₹892.67 Crore (excess expenditure met from unspent balance of 2018-19 and 2019-20) whereas revenue earned was ₹322.40 Crore on account of various license fees, charges, penalties etc.

The Performance Audit for the period 2014-15 to 2018-19 examined the functioning of UIDAI in supporting the Government's vision to assign, as good governance, unique identity numbers to individuals residing in India. However, statistical information on generation, update and authentication services of Aadhaar and financial information referred to in the Report have been updated upto March 2021, to the extent as furnished by UIDAI.

Significant audit findings are given below:

- 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.

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)

- 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.

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)

- Issue of Aadhaar numbers to minor children below the age of five, based on the biometrics 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.

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)

- 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.

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)

- 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.

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 did not have a system to analyze the factors leading to authentication errors.
UIDAI may make efforts to improve the success rate of authentication transactions by analysing failure cases.

(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.

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 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.

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'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.

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 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.

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

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)

- 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.

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)

- 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.

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 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.

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

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)

- 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.

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)

- 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.

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)

UIDAI, in the Exit Conference held on 14 October 2020, has agreed to the audit recommendations.



CHAPTER 1

Introduction



Chapter 1

Introduction

1.1 Introduction

Prior to issue of a nationally accepted identity document for Indian residents, multiple documents viz., Driving License, Permanent Account Number (PAN), Voter Identity Card etc., were in use as proof of identity and address. The absence of easily verifiable identity documents was conducive to identity frauds and for leakages in the system of delivery of benefits from Government sponsored schemes and hence there was a need for having one unique identity for the residents of the country.

The concept of unique identification was first discussed and worked upon in 2006, when administrative approval for the project "Unique ID for BPL families" was given on 03 March 2006 by the erstwhile Department of Information Technology (DIT), Ministry of Communications and Information Technology. Subsequently, a Process Committee was set up (03 July 2006) to suggest processes for updation, modification, addition and deletion of data fields from the core database under the Unique ID for BPL families' project.

DIT submitted a "Strategic Vision – Unique Identification of Residents" to the Process Committee, which appreciated and approved the need of a UID Authority to be created by an executive order under the aegis of the then Planning Commission (now NITI Aayog) to ensure a pan-departmental and neutral identity for the Authority. The Process Committee decided (30 August 2007) to furnish a detailed proposal based on the resource model for seeking its "in principle" approval to the erstwhile Planning Commission.

Based on the recommendations of the Committee of Secretaries and decision of the Empowered Group of Ministers (EGoM), Unique Identification Authority of India was created on 28 January 2009 as an attached office of the then Planning Commission (replaced by NITI¹ Aayog in 2015)². Prime Minister's Council on UIDAI (substituted by a Cabinet Committee on UIDAI on 22 October 2009) was constituted on 30 July 2009 to advise UIDAI on the programme, methodology and implementation to ensure coordination between Ministries/Departments, stakeholders and partners.

As per Cabinet's approvals, the work of Aadhaar enrolment was initially geographically divided between UIDAI and Registrar General of India (RGI). Accordingly, UIDAI was assigned to do Aadhaar enrolment in 24 States and Union Territories (UTs) and RGI was to do enrolment in 12 States and UTs.

In September 2015, UIDAI was brought under the Ministry of Electronics and Information Technology (MeitY) (erstwhile Department of Electronics & Information Technology). For giving statutory standing to UIDAI, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 was introduced in Parliament as Money bill on

¹ NITI (National Institution for Transforming India) Aayog is the premier policy 'Think Tank' of the Government of India, providing both directional and policy inputs.

² In September 2015, UIDAI was attached to the Department of Electronics & Information Technology (DeitY) of the then Ministry of Communications and Information Technology (Mo CIT).

03 March 2016, which was notified (26 March 2016) as the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016) .

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 and the ambitious Aadhaar Scheme was launched on 29 September 2010 in Tembli, a village in Nandurbar district of Maharashtra State in India, from where first Aadhaar was issued. 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.

1.2 Constitutional validity of Aadhaar

After launch of Aadhaar, Government progressively made the Aadhaar Card mandatory for numerous welfare schemes. These include subsidised food under the Public Distribution System, guaranteed wages to labour under the Mahatma Gandhi National Rural Employment Guarantee Scheme, linking of PAN Card, telecom subscriber verification etc. However, the Aadhaar scheme was challenged from time to time by several petitioners in various courts of law and its constitutional validity was sub- judice since 2010. The five judges Constitution Bench of the Hon'ble Supreme Court in its landmark judgment of 26 September 2018, upheld the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, to be constitutional³.

The salient points of the judgment⁴ of Hon'ble Supreme Court of India are as follow:

- a.** The Aadhaar Act, 2016 does not violate fundamental right of privacy. Section 7 of the Act is constitutional. 'Benefits' and 'services' should be those which have the colour of some kind of subsidies namely welfare schemes of the Government whereby Government is doling out such benefits which are targeted at a particular deprived class.
- b.** Residents are held entitled to obtain Aadhaar number but such an enrolment was voluntary in nature. However, it becomes compulsory for those who seek to receive any subsidy, benefit or services under the welfare schemes of the Government, expenditure whereof is to be met from the Consolidated Fund of India. As such CBSE, NEET, JEE, UGC etc. cannot make the requirement of Aadhaar mandatory for the students.
- c.** No deserving persons would be denied the benefit of a scheme on the failure of authentication and it would be appropriate to make a suitable provision for establishing an identity by alternate means.
- d.** No child shall be denied benefit, of any of the welfare schemes covered under Section 7, if, for some reasons, she/he is not able to produce the Aadhaar number and the benefit shall be given by verifying the identity on the basis of any other document.

³ Writ Petition (Civil) No. 494 of 2012 before the Hon'ble Supreme Court of India which also considered several other writ petitions in its judgment dated 26 September 2018

⁴ The Bench delivered its 4:1 verdict:-

- Majority opinion of Chief Justice Dipak Misra, Justice A.K. Sikri and Justice A.M. Khanwilkar
- Concurring opinion of Justice Ashok Bhushan
- Dissenting opinion of Justice D.Y. Chandrachud

- e. Regulation 27 of Aadhaar (Authentication) Regulations 2016 which provides archiving a data for five years was struck down. Retention of data beyond six months was made impermissible.
- f. Section 57 which enabled body corporate and individuals to seek authentication was held unconstitutional and void.
- g. Section 139AA of Income tax Act 1961 (for seeding of PAN with Aadhaar) held constitutional.
- h. Rule 9 of the amended PMLA Rules, 2017 which mandates linking of Aadhaar with bank accounts was held unconstitutional.
- i. Department of Telecommunications' Circular dated 23 March 2017 mandating linking of mobile numbers with Aadhaar was held unconstitutional.

Thus, though Aadhaar is a legal document and mandatory for obtaining benefits of Government schemes and programmes, residents can furnish it voluntarily for proving identity in case of other services also. To implement the judgment of the Supreme Court, Government passed the Aadhaar and Other Laws (Amendment) Act, 2019 (notified on 23 July 2019)⁵ in the Parliament to incorporate further safeguards to protect privacy of data, foil misuse of personal information of its citizens and for averting denial of services and benefits to eligible persons. In addition, to facilitate better services through Aadhaar, voluntary use of Aadhaar authentication was provided for obtaining SIM cards and for opening bank accounts, with necessary changes in the Indian Telegraph Act, 1885 and the Prevention of Money Laundering Act, 2002 respectively.

1.3 UIDAI Authority

1.3.1 Powers of the Authority

UIDAI performs functions as defined by the Section 23 and 23A of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. It has authority to develop the policy, procedure and systems for issuing Aadhaar numbers to Individuals and perform authentication thereof under this Act.

The powers and functions of the Authority, inter alia, include

- (a) Specifying, by regulations, demographic information and biometric information required for enrolment and the processes for collection and verification thereof;
- (b) Collecting demographic information and biometric information from any individual seeking an Aadhaar number in such manner as may be specified by regulations;
- (c) Appointing of one or more entities to operate the Central Identities Data Repository;
- (d) Generating and assigning Aadhaar numbers to individuals;
- (e) Performing authentication of Aadhaar numbers;

⁵ Government of India introduced "The Aadhaar and Other Laws (Amendment) Ordinance, 2019" on 02 March 2019, notified as an Act on 23 July 2019

- (f) Maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;
- (g) Omitting and deactivating of an Aadhaar number and information relating thereto in such manner as may be specified by Regulations;
- (h) specifying the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used;
- (i) Specifying, by regulations, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof;
- (j) Establishing, operating and maintaining of the Central Identities Data Repository;
- (k) Sharing, in such manner as may be specified by regulations, the information of Aadhaar number holders, subject to the provisions of this Act;
- (l) calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of this Act of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act;
- (m) Specifying, by regulations, various processes relating to data management, security protocols and other technology safeguards under this Act;
- (n) levying and collecting the fees or authorising the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act in such manner as may be specified by regulations;

The Authority may

- (a) enter into Memorandum of Understanding or agreement, as the case may be, with the Central Government or State Governments or Union territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing, securing or processing of information or delivery of Aadhaar numbers to individuals or performing authentication;
- (b) by notification, appoint such number of Registrars, engage and authorise such agencies to collect, store, secure, process information or do authentication or perform such other functions in relation thereto, as may be necessary for the purposes of this Act.

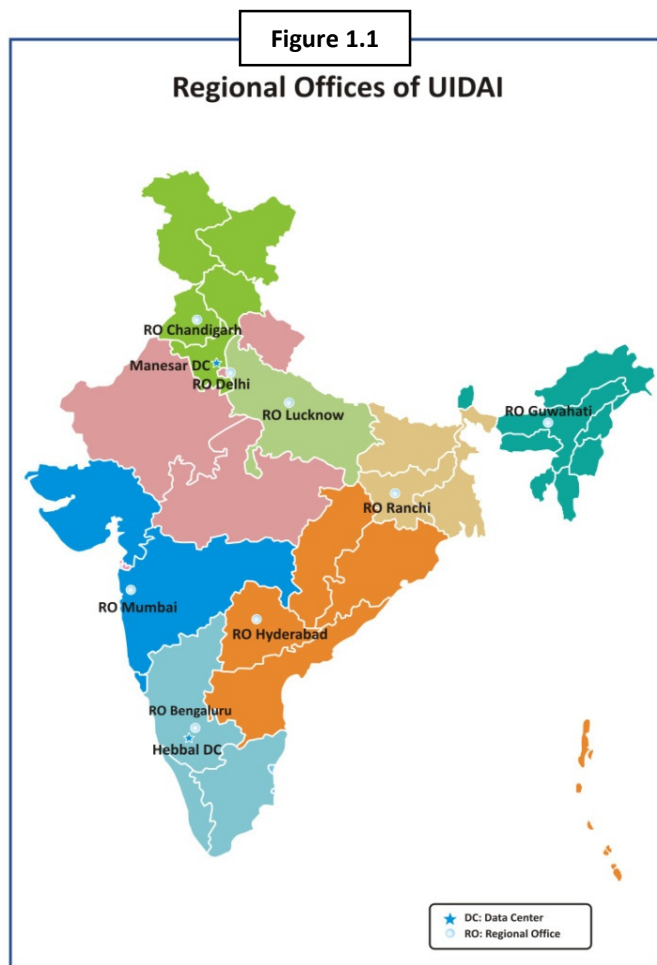
The Authority may engage consultants, advisors and other persons as may be required for efficient discharge of its functions under the Act on such allowances or remuneration and terms and conditions as may be specified by contract.

The Authority may, for the discharge of its functions under this Act, or any rules or regulations made there under, by order, issue such directions from time to time to any entity in the Aadhaar ecosystem, as it may consider necessary. Every direction issued shall be complied with by the entity in the Aadhaar ecosystem to whom such direction is issued.

1.3.2 Organizational Set-up

UIDAI has its headquarters (HQ) in New Delhi and has eight (8) Regional Offices (ROs) across the country. The locations of ROs and the States/ UTs under their jurisdiction are illustrated

in **Figure 1.1**. UIDAI also operates two Data Centers (DCs), one at Hebbal, Bengaluru, Karnataka and the other at Manesar, Haryana.



A Chairperson appointed on part-time basis heads the Authority with two part-time members and a Chief Executive Officer (CEO), who is also the Member-Secretary of UIDAI. The CEO is the legal representative of the Authority and is responsible for its day-to-day administration and implementation of its work programs including drawing up of proposals arising out of the discharge of functions assigned to UIDAI, preparation of accounts etc. At the HQ, the CEO is assisted by Deputy Directors General (DDGs) who are Joint Secretary level Officers of Government of India and are in-charge of various wings of UIDAI. Each of the eight ROs of UIDAI is headed by a DDG. As on 31 March 2021, UIDAI Headquarters had 130 sanctioned posts⁶ in various cadres whereas person-in-position were 95. In the eight UIDAI ROs, out of total

sanctioned posts of 219, person-in position were 148 as on 31 March 2021. The Authority functioned mostly with officers on deputation from various Government Departments.

1.3.3 Registrars

UIDAI authorizes entities as Registrars for the purpose of enrolling residents. Their roles and responsibilities are defined vide Memorandums of Understanding (MoU) signed by them with UIDAI. Central and State Government Departments, banks and other Public Sector organizations can be appointed as Registrars. Registrars have the option to carry out enrolment either by themselves or through Enrolment Agencies further sub-contracted by them. UIDAI had authorised 177⁷ Registrars as on 31 March 2021.

1.3.4 Enrolment Agencies

UIDAI or the Registrars appoint Enrolment Agencies (EAs) for collecting demographic and biometric information of residents as part of the enrolment process. EAs setup Enrolment Centers for enrolment of residents and for correction/ updation of resident data. The EAs employ operators who are responsible for enrolling residents, capture the demographic and

⁶ Data source: Information furnished by UIDAI.

⁷ Data source: Information furnished by UIDAI.

biometric information using the enrolment software, for uploading into the Central Identities Data Repository (CIDR)⁸. The quality of the documents collected by the EAs in respect of the demographic information of residents is scrutinized through a back-office Quality Check verification process by a quality control team. There were 436 Enrolment Agencies as on 31 March 2021.

1.4 Legislation, Rules and Regulations

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (hereafter referred to as Aadhaar Act) and the Aadhaar and Other Laws (Amendment) Act 2019 provide the statutory basis for the operations of UIDAI. Drawing from the powers conferred by the Act of 2016, UIDAI notified various regulations for discharge of its mandated responsibilities. Aadhaar (Enrolment & Update) Regulations 2016, Aadhaar (Authentication) Regulations 2016, Aadhaar (Data Security) Regulations 2016 and Aadhaar (Sharing of Information) Regulations 2016 and amendments thereto regulate the activities related to the functioning and activities of UIDAI. The regulations generally cover all the areas of operation of UIDAI. Requirements of the Act and corresponding provisions in the various regulations are mapped in **Appendix-I**. The UIDAI Procurement Manual 2014 and GFR 2005/2017 regulate purchases and procurement in the organization.

1.5 Structure of the Report

The Performance Audit 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.

⁸ Aadhaar numbers issued along with the demographic and biometric information are secured in the centralized database viz., CIDR of UIDAI at Bengaluru.

CHAPTER 2

Scope of Audit, Audit Objectives and Methodology

Chapter 2

Scope of Audit, Audit Objectives and Methodology

2.1 Scope of Audit

The Performance Audit included assessment of the Enrolment & 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 upto March 2021. Audit scrutinised the processes beginning right from the enrolment, upto 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. In addition, audit also examined selectively, the procurement of infrastructure for the project.

2.2 Audit Objectives

The main audit objectives of the Performance Audit were to ascertain whether:

1. UIDAI has developed comprehensive regulations to comply with the responsibilities entrusted under the Aadhaar Act.
2. Ecosystem put in place for issue of Aadhaar and Authentication services functioned efficiently and in compliance with the statutory requirements.
3. UIDAI has put in a system to monitor the performance of the IT systems associated with its operations.
4. Contract management system in UIDAI for procurement of IT and other services is in conformity with government regulations and is executed to achieve economy and efficiency in operations.
5. Complaint redressal mechanism set up by UIDAI for handling Aadhaar related grievances was effective.

2.3 Audit Criteria

Important criteria adopted for the Performance Audit were:

- a. Cabinet Approval on the formation of UIDAI and decisions of Expenditure Finance Committee (EFC).
- b. Provisions of Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and subsequent Amendments.
- c. Relevant provisions under General Financial Rules (GFR), 2005 and its revised version GFR 2017, which have elaborately stipulated procedures for procurement, maintenance of stock and stores, their disposals, etc.
- d. The Procurement Manual 2014 (effective from 01 April 2014) issued by UIDAI, contains the principles and procedure relating to procurement of goods and services for purposes of UIDAI and is drawn from the Rule 135 of the GFR 2005.
- e. The Aadhaar (Enrolment and Update) Regulations, 2016.
- f. The Aadhaar (Authentication) Regulations, 2016.

- g.** The Aadhaar (Data Security) Regulations, 2016.
- h.** Aadhaar (Sharing of Information) Regulations, 2016
- i.** Subsequent Amendments to the above regulations and any other instructions/notifications/Regulations issued by Government/UIDAI, which have a bearing on the project and functioning of UIDAI.

2.4 Audit Methodology

The Performance Audit commenced with an entry conference with the top management of UIDAI at UIDAI Headquarters at New Delhi in February 2019 where the scope of the audit, audit objectives etc. were explained to the Management. Files and records, maintained at UIDAI HQ, its ROs⁹ and at UIDAI Tech Centre at Bengaluru were reviewed in audit.

We selected contracts for scrutiny based on statistical sampling techniques. Besides, examination of documents, we obtained information by way of replies to audit questions furnished by the auditee and through meetings with key personnel of UIDAI involved in its various operations.

On completion of Audit, we discussed important observations with the UIDAI management in an Exit Meeting in October 2020. Auditee's response given during the Exit Meeting and by way of a written reply has been suitably included in this Report. The statistical information has been updated to 31 March 2021.

The reply of the Ministry of Electronics and Information Technology (MeitY) furnished in June 2021 has also been taken into consideration in finalizing the report.

2.5 Good Practices

UIDAI has provided an identity document to over 125 crore residents of India within a decade of issue of the first Aadhaar (September 2010) in coordination with a large number of agencies/entities spread across the country. UIDAI has established the Information Security Management System and obtained the ISO 27001:2013 by STQC and the National Critical Information Infrastructure Protection Centre (NCIIPC) has declared its CIDR as "Protected System" adding another layer of IT security assurance.

We noted that UIDAI has a system of imposing financial penalties on its enrolment ecosystem partners for deficient/ defective quality of work. Complaints of overcharging of residents are followed up and financial disincentives are imposed on Registrars. It was observed that payments to Registrars are released only after crosschecking with the list of successful generation of Aadhaars obtained from UIDAI Tech Center.

Features like the Virtual ID and Biometric Locking facility provides more leeway to Aadhaar holders while availing Aadhaar related services. The Virtual ID is a temporary and revocable 16-digit random number and is mapped with the Aadhaar so that it can be used in place of Aadhaar for authentication. The Biometric Locking facility helps an Aadhaar holder to lock/unlock his/ her biometrics whenever he/ she wishes. These initiatives help in enhancing confidence of Aadhaar holders while using the ID.

⁹ Except Guwahati RO

In 2019, “Aadhaar Seva Kendras” (ASK) were introduced in 41 select locations in the country to act as a single stop destination for all Aadhaar services for the residents. These ASKs were in addition to 35,000 already available Aadhaar enrolment and Update Centers.



The ASKs offer dedicated Aadhaar enrolment and update services to residents on all seven days of the week.

Image courtesy: UIDAI

2.6 Acknowledgement and Constraints

We acknowledge the support and cooperation extended by the Management of UIDAI to the audit team during the course of audit. A detailed presentation on the functioning of the Authority was given for understating of the Audit Team. The records/ data requisitioned by Audit Team were generally furnished but audit witnessed several instances of inordinate delay/ non-supply of records which impeded in the audit exercise. Records, which could not be accessed included files related to Information Technology-Information System Security, Aadhaar Document Management System, destruction of documents collected at the time of enrolment, details of authentications and its accounting, fixation of rates/ charges for authentication and enrolment & update activities, grievances /complaints of customers, audit reports of stake holders (e.g. enrolment centres or ASAs/AUAs) etc. We also appreciate the support provided in updating the statistical and other information till March 2021.

UIDAI expressed difficulties in providing data for period prior to formation of UIDAI (July 2016) as an Authority under Aadhaar Act. Intermittent supply of data, delayed submission and partial responses to audit queries had hindered the smooth completion of audit process. We could not provide reasonable assurances on the selection process of vendors appointed by UIDAI for managing the vital services in the roles of Managed Service Providers, Data Centre Development agencies and Aadhaar Documents Management System partners or Government Risk Compliance and Performance – Service Providers. However, we relied on the UIDAI write ups and the scrutiny of files to arrive at a conclusion that the service partners for providing the services¹⁰ were selected in competitive manner by following the prescribed rules, procedures and due diligence. The contracts for supply of professional resources entered into with NISG were on nomination basis.

¹⁰ The services which were selected for audit scrutiny following the decided samples

Therefore, in keeping with the scope of the CAG's Regulations on Audit and Accounts, to the extent data and information/files were not produced to the audit, we could not derive our assurance on the areas mentioned above.

CHAPTER 3

Enrolment, Update and Authentication Ecosystem

Chapter 3

Enrolment, Update and Authentication Ecosystem

3.1 Enrolment and Update Ecosystem

Every resident in the country is eligible to obtain an Aadhaar number by submitting his/her demographic and biometric information. After verification of this information by UIDAI Aadhaar numbers are issued. UIDAI confirms the uniqueness of the identity of a resident by way of a de-duplication process where the information submitted by each new enrollee is matched with that of others in the Aadhaar database to ensure that the applicant is not already enrolled. After establishing uniqueness of identity, a 12-digit random number is generated and issued to the applicant. This unique lifetime number cannot be assigned to any other individual. The demographic and biometric details of Aadhaar holders, however, can be updated to ensure continued accuracy of the information in the CIDR.

An Aadhaar number subject to its authentication¹¹, is accepted as a valid proof of identity of the Aadhaar number holder for receiving specified benefits, subsidies and services for which expenditure is met from the Consolidated Fund of India/Consolidated Fund of State. However, Aadhaar does not confer citizenship or domicile to its holder and is only a proof of identity.

The definition of “Resident” gains prime importance as it sets the basic eligibility criteria for entitlement of Aadhaar number. A “Resident”, as per the Act, is as an individual who has resided in India for a period or periods amounting in all to 182 days or more in the 12 months immediately preceding the date of application for enrolment.

The enrolment process begins with a resident submitting his/her demographic and biometric information to the Enrolment Agency (EA) along with prescribed supporting documents to establish identity, date of birth and address of the enrollee. The information is submitted to the CIDR for further processing and generation of Aadhaar number. The UIDAI has adopted a tiered model consisting of Registrars and EAs for enrolment and updation of Aadhaar numbers. The information to be provided at the time of enrolment are as follows:

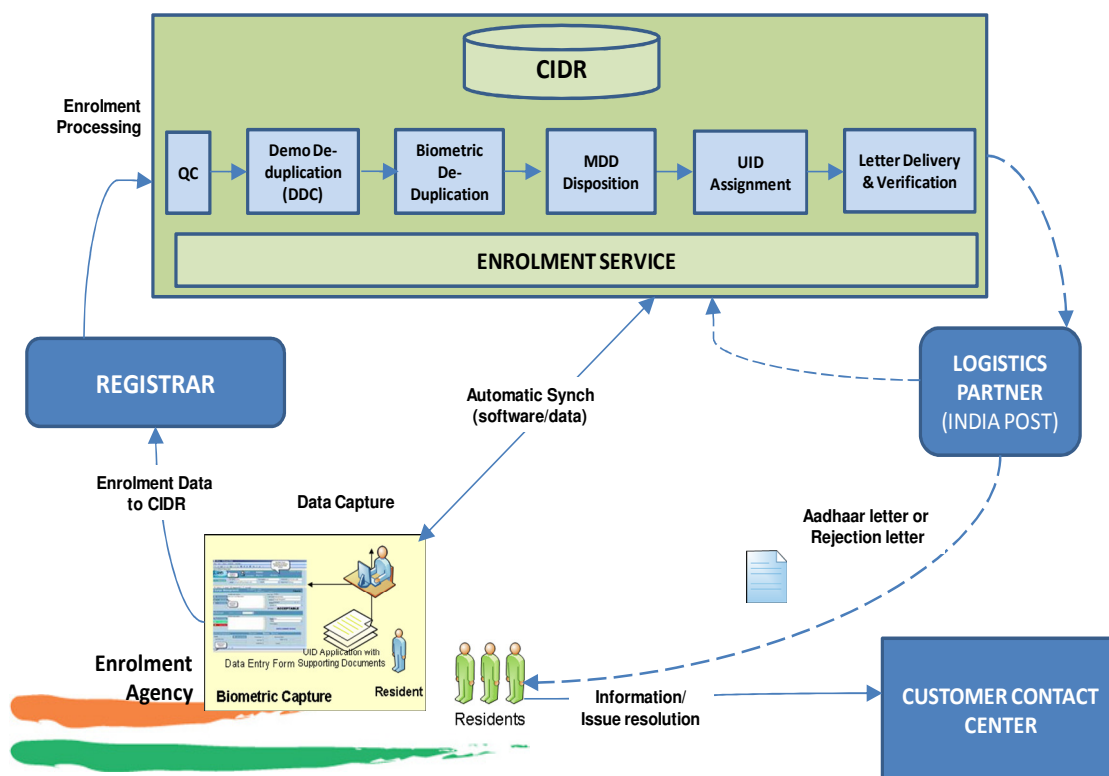
Demographic information	Name, verified date of birth or declared age, gender, address, mobile number (optional) and email ID (optional), in case of introducer-based enrolment- introducer name and introducer’s Aadhaar number, in case of Head of Family based enrolment- name of Head of Family, relationship and Head of Family’s Aadhaar number; in case of enrolment of child- enrolment ID or Aadhaar number of any one parent, proof of relationship (PoR) document.
Biometric information	Ten fingerprints, two iris scans, and facial photograph

¹¹ Authentication is the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository of UIDAI for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

Aadhaar enrolment (and mandatory biometric updates) is done free of cost for residents. However, for all enrolments and mandatory biometric updates, UIDAI makes payments to the Registrars at rates fixed by them from time to time¹².

The enrolment process is illustrated in **Figure 3.1**.

Figure 3.1 Enrolment process



Graphics Courtesy: UIDAI

3.1.1 Key Regulations and Amendments

Enrolment and Update is central to the Aadhaar structure. Registrars and EAs, responsible for collecting the demographic and biometric information of individuals for the enrolment process, are core components of this ecosystem. EAs are responsible for adherence to processes prescribed by UIDAI and to ensure data quality. The Aadhaar (Enrolment & Update) Regulations 2016 and amendments thereto govern the activities associated with this ecosystem. Key regulations and amendments thereto governing the Aadhaar enrolment and update process are given in **Table 3.1**.

Being the backbone of the Aadhaar system, it is important that the regulations prescribe the processes and procedures in conformity with the provisions of the Aadhaar Act and UIDAI establish systems to ensure that Aadhaar numbers generated satisfy all the features and qualities envisaged in the Act.

¹² Effective from January 2019, the rate for every enrolment that has resulted in successful generation of an Aadhaar number is fixed at ₹100. Similarly, for all mandatory biometric updates UIDAI pays ₹100 per request to the Registrar with effect from January 2019. However, for all voluntary updates of demographic or biometric information, UIDAI has prescribed a fee of ₹50 per request (enhanced to ₹100 per request for voluntary biometric updates w.e.f. 09 May 2020) and is to be paid by the Aadhaar number holder.

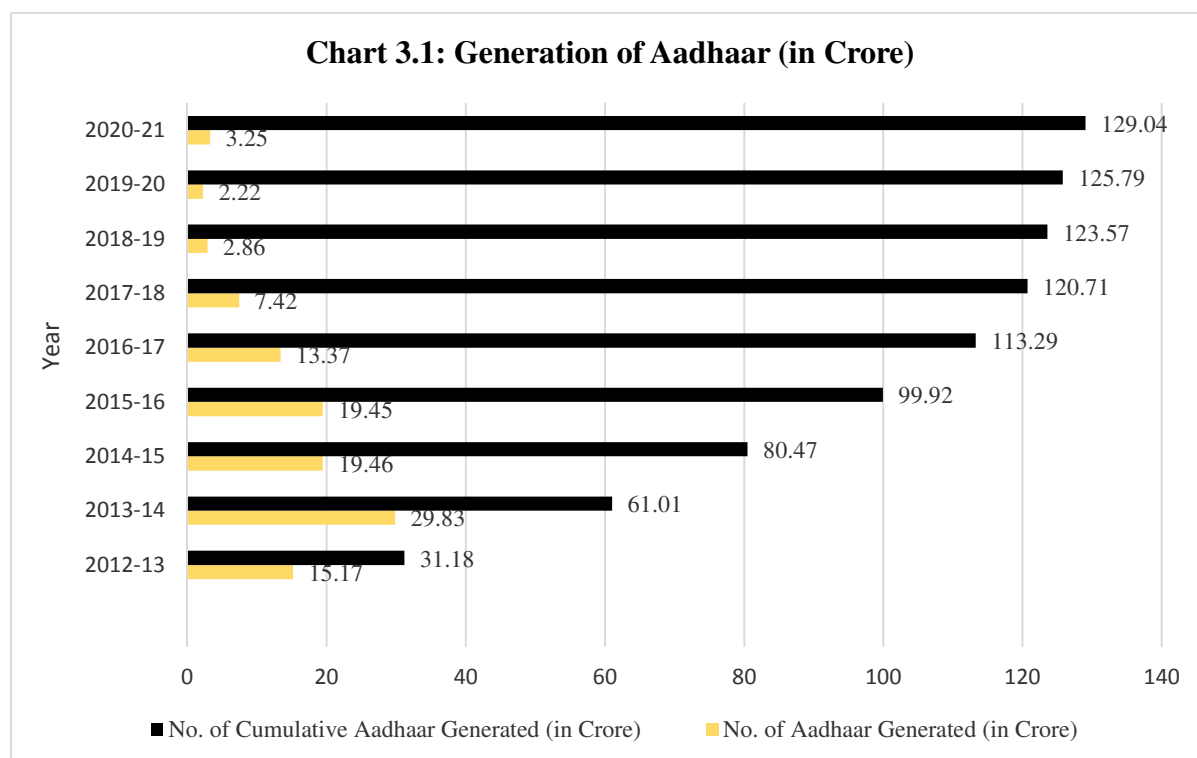
Table 3.1: Key Regulations and amendments thereto governing the Aadhaar Enrolment and Update ecosystem

Key Regulations	Key features
Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016) Dated 14-Sep-2016	<ul style="list-style-type: none"> ✓ Resident Enrolment Process: Biometric & Demographic information required, Role of Registrars, Collection of Information, Equipment, Software used in enrolment etc. ✓ Generation, Rejection & Delivery of Aadhaar numbers. ✓ Update of Resident information: Mandatory update, Modes of update, Convenience Fee to be charged for update ✓ Appointment of Registrars, Enrolling Agencies & other service providers ✓ Omission or Deactivation of Aadhaar number ✓ Grievance Redressal Mechanism. ✓ Format of enrolment/ Correction & update form, list of Documents (POI, POA, POR, DOB etc.), Code of conduct for Service providers
Aadhaar (E&U) (Second Amendment) Regulations 2017 (No. 2 of 2017) Dated 07-Jul-2017	<ul style="list-style-type: none"> ✓ Addition of Regulation 12A: Any Central or State department or agency requiring authentication or possession of Aadhaar for receipt of any subsidy, benefit or services should ensure enrolment of such individual who is yet to be enrolled or update their Aadhaar details, by setting up enrolment centres at their premises
Aadhaar (E&U) (Fourth Amendment) Regulations 2017 (No. 5 of 2017) Dated 31-Jul-2017	<ul style="list-style-type: none"> ✓ Immediate suspension of activities or imposition of Financial Disincentives on Registrar or Enrolment Agency or any service provider or any other person or Cancellation of the credential, codes or permission issued to them, for violation of any regulation, process, standard, guideline or order, by a Registrar or Enrolment Agency or any service provider or any other person
Aadhaar (E&U) (Sixth Amendment) Regulations 2018. (No. 2 of 2018) Dated 31-Jul-2018	<ul style="list-style-type: none"> ✓ New Definition of Incapacitated Person. ✓ Date of Birth of resident can be updated only once. In case the DoB is to be updated more than once, it can only be done through an exception handling process which may require the resident to visit the Regional Office (RO) of the UIDAI. ✓ Amendments in verification of update data, disclosure of information to parents/ form to be signed by parents in case of minors. ✓ Introduction of Aadhaar Address update PIN Service for residents not having acceptable proof of Address.

Aadhaar (E&U) (Seventh Amendment) Regulations 2019. (No. 3 of 2019) Dated 05-Sep-2019	✓ Enhancement in list of POI, POA, POR & DOB under Schedule II of E&U Regulations, 2016 [Regulation 10(2)]
--	--

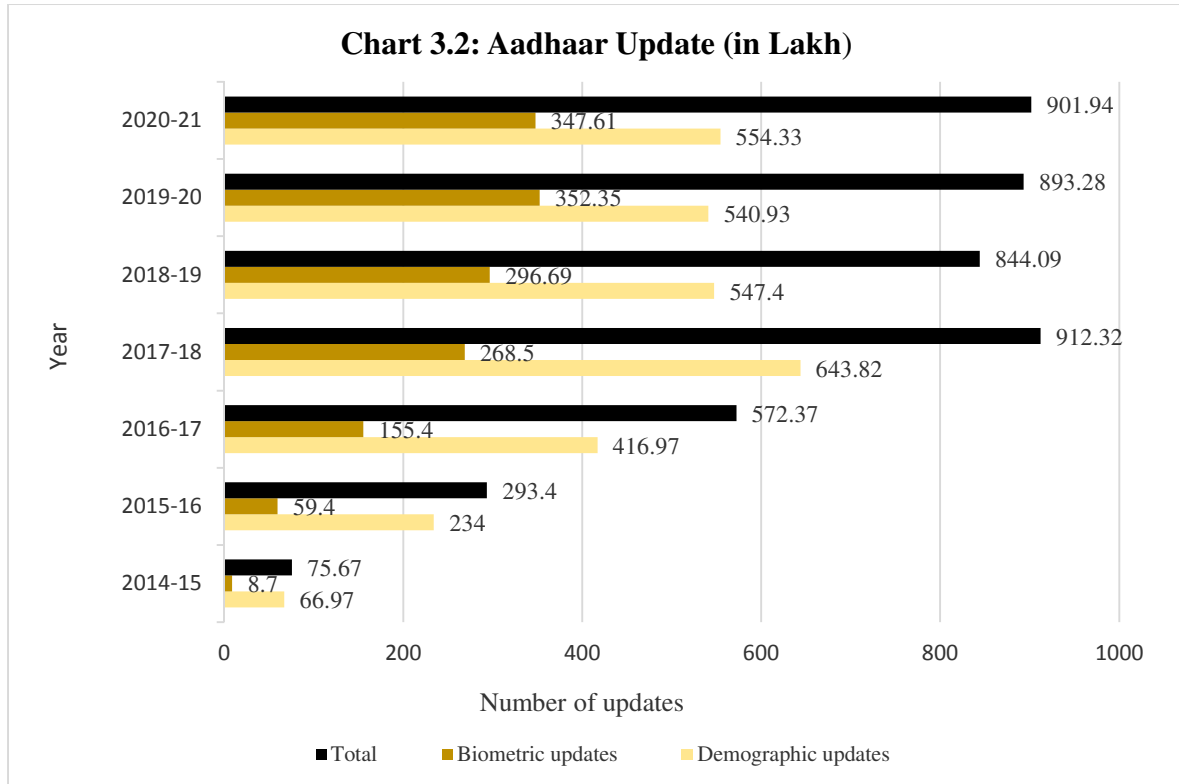
3.1.2 Status of Aadhaar Enrolment and Update

UIDAI had generated 129.04 Crore Aadhaar numbers as of March 2021 for the residents in the country, which is approximately 94 *per cent* of the projected population. The number of Aadhaar generated and updated during 2012-13 to 2020-21 are given in **Chart 3.1** and **Chart 3.2** respectively.



(Data Source: UIDAI)

Chart 3.1 shows that growth of Aadhaar generated in 2013-14 was 95.67 *per cent* as compared to previous year and gradually it reached the plateau after 2017-18 wherein it grew less than 3 *per cent* as compared to previous year.



(Data Source: UIDAI)

Chart 3.2 shows that growth of Aadhaar update had picked up pace from 2015-16 onwards. The total updates at the end of 2014-15 standing at 75.67 Lakh has multiplied around 12 times in five years to reach at 901.94 Lakh at the end of 2020-21.

3.1.3 Aadhaar Saturation Status

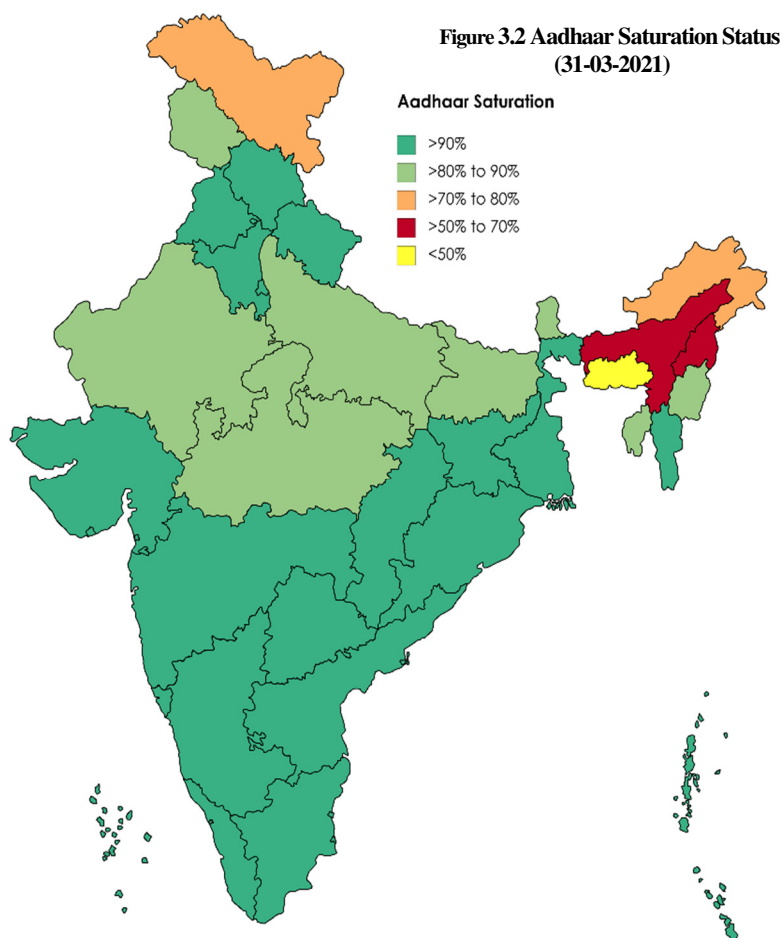


Figure 3.2 depicts the Aadhaar saturation status across the States and Union Territories as on 31 March 2021. UIDAI had issued more than 124.67 Crore (live) Aadhaar till 31 March 2021¹³ and in 23 States/ Union Territories more than 90 per cent saturation levels were achieved whereas eight States/ Union Territories had saturation of around 80 to 90 per cent. In two States/ Union Territories (Arunachal Pradesh and Ladakh) the saturation level is between 70 to 80 per cent whereas in other two States (Assam and Nagaland) the saturation status was above 50 per cent but less than 70 per cent.

However, one State (Meghalaya) has not reached the saturation level of 50 per cent. There was overall saturation of 91 per cent in issue of Aadhaar across India.

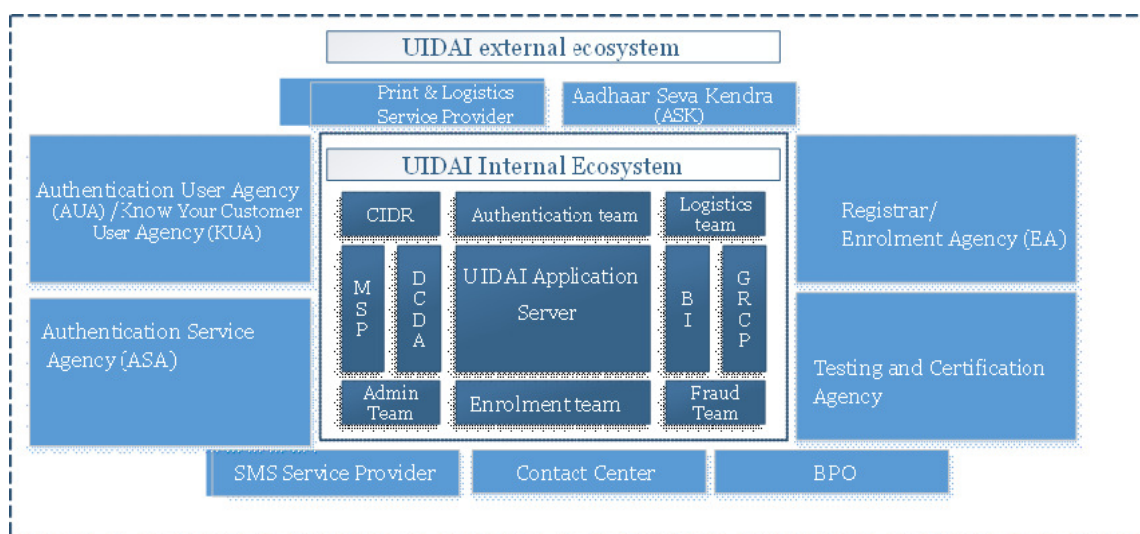
Thus, the UIDAI needed to continue with its efforts to enroll Aadhaar eligible residents and increase the enrolment in States which have not achieved 90 per cent benchmark.

3.1.4 The Components of Aadhaar Ecosystem

The various components of the ecosystem, external as well as internal, involved in the enrolment to authentication, printing to delivery of Aadhaar card and the customer support is depicted in the **Figure 3.3**.

¹³ Source: Aadhaar Saturation Report of UIDAI as on 31 March 2021.

Figure 3.3: The Aadhaar Ecosystem



3.1.5 De-duplication process

UIDAI has employed a two-step process for identifying duplicate enrolments. In the first stage, demographic data match is done and in the second stage biometric matching of fingerprints and iris with the database of all others enrolled in the Aadhaar database is done to identify duplicates and establish uniqueness of the enrollee. After successful clearance at the de-duplication stage, a 12-digit Aadhaar number is generated which is communicated to the resident through UIDAI’s logistics partner India Post. Residents who have submitted their mobile numbers during enrolment can also download e-Aadhaar¹⁴.

UIDAI has agreements with three vendors for providing Automatic Biometric Identification Systems (ABIS). These vendors were selected by the Managed Service Provider (MSP). If one ABIS identifies a duplicate, it will be subject to verification by another ABIS for enhancing accuracy. Further, UIDAI has a manual adjudication system also where duplicates identified are subject to a further verification before rejection. UIDAI also undertakes demographic de-duplication to identify errors in the demographic data submitted by a resident at the time of enrolment.

Details of de-duplication carried out by UIDAI as on 31 March 2019 are given below:

A. Biometric Residents

Aadhaar generated through Biometric De-duplication through

- (i) ABIS: 111,11,40,041
- (ii) Manual De-duplication: 89,45,010

B. Non-Biometric Residents:

Aadhaar generated without Biometric

- (i) Children below five years: 11,48,27,267

¹⁴ An e-Aadhaar is an electronic form of Aadhaar letter downloadable from e-Aadhaar portal of UIDAI’s website. Resident can download e-Aadhaar in pdf format by visiting <https://aadhaar.uidai.gov.in>. They can use either 28-digit enrolment no. received at the time of enrolment or 12-digit Aadhaar Number.

(ii) Residents with 100 *per cent* Biometric exception category: 5,69,196

Issues of large member of de-duplications done and Aadhaar issued to minor children are commented in Report.

3.1.6 Bio-metric Device Certification

Standardization, Testing and Quality Certification (STQC) Directorate, an attached office of MeitY, is the nodal agency appointed to carry out specifications as well as certification activity for enrolment and authentication devices requirements for the UIDAI.

3.1.7 Managed Service Provider

The entire end-to-end technology infrastructure of UIDAI including data center operations, management of IT systems of UIDAI ROs, technical helpdesk etc., is managed by the Managed Service Provider (MSP) viz M/s HCL Infosystems Ltd. The MSP was appointed in August 2012 through Expression of Interest and Request for Proposal method for a period of seven years. At present (March 2021), the MSP is functioning under extension period. The total value of contract with the MSP was ₹1,978.62 Crore.

3.1.8 Governance Risk Compliance and Performance – Service Provider

Government Risk Compliance and Performance – Service Provider (GRCP-SP) is an independent monitoring agency on behalf of UIDAI, deployed by the Authority to ensure compliance and security of the UIDAI ecosystem. The role of GRCP-SP is to facilitate creation of a robust, comprehensive, secure environment for UIDAI to operate. (including external agencies such as a Registrars, Enrolment Agencies, Aadhaar Seva Kendra's, ASAs, AUA/ KUA/ Sub-KUAs, Contact Center, SMS Service Provider and Logistics Service Providers etc.), in terms of Visibility, Effectiveness and Control.

Service level monitoring of all contracts is one of the important works of the GRCP-SP, which helps the UIDAI in having a financial control. All the data pertaining payments is to subjected to GRCP Audit and processed for payments on the basis of their reports.

3.2 Audit Observations on Aadhaar Enrolment Ecosystem

Audit observations on the Aadhaar Enrolment *vis-à-vis* provisions of the Aadhaar Act 2016 are given in succeeding paragraphs:

3.2.1 Verification of the 'Resident' status of the applicants

UIDAI relied on self-declaration made by the residents regarding their 'Resident' status at the time of Aadhaar enrolments and thus status of Resident or non-Resident remained unverified.

As per the provisions of the Aadhaar Act, 2016, every resident in the country is entitled to obtain an Aadhaar number by submitting his demographic and biometric information by undergoing the process of enrolment. A "Resident" as per the Act, is as an individual who has resided in India for a period or periods amounting in all to 182 days or more in the 12 months immediately preceding the date of application for enrolment. The definition of "**Resident**" sets the basic eligibility criteria to be fulfilled by each individual for obtaining Aadhaar.

The Aadhaar (Enrolment and Update) Regulations 2016 prescribes the nature of documents a resident should submit as proof of identity (PoI), proof of address (PoA), date of birth (DoB),

proof of relationship (PoR) etc. to the EAs. Whenever a resident applies for enrolment/ correction/ updation, a standard form containing demographic details of self along with ticking the residential status, has to be filled

It was however, noted that UIDAI had not specified any proof/document in the regulation for confirming the “Resident” condition, to qualify as a resident. No procedure has been prescribed to check the veracity of the applicant’s testimony. Thus UIDAI had not put in place a system for fulfilling the fundamental requirement of identifying residents. Audit is of the view that non-verification of status of residence may lead to issue of Aadhaar to non-bona fide residents.

UIDAI stated (September 2019) that the validity of the documents provided by individual applicants in support of identity, address, date of birth etc., are confirmed during enrolment and cases appearing as fraudulent are dealt in accordance with provisions of Aadhaar (Enrolment & Update) Regulations 2016. UIDAI (October 2020) asserted that self-declaration in conjunction with the prescribed documents was the only practical means to ascertain the resident status of applicants. The Ministry of Electronics and Information Technology (MeitY) agreed (June 2021) with replies of UIDAI to the audit observations.

The replies of UIDAI/ MeitY are not tenable as Aadhaar (Enrolment & Update) Regulations 2016 stipulates actions to be taken against fraudulent cases only after generation of Aadhaar numbers, whereas the issue here is of conducting prior checks to ascertain residential status of an applicant, as one of the condition for issue of Aadhaar, as provided in the Aadhaar Act 2016. UIDAI should explore a workable system of verification of residence status based on the criteria prescribed under the Act. A review of the definition of a resident for this purpose has gained more importance in light of the fact that non-resident Indians holding a valid Indian passport were also entitled for an Aadhaar number after their arrival in India bypassing the 182 days residency criteria as per the Gazette notification dated 20 September 2019.

Recommendation: 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.

3.2.2 Generation of Multiple Aadhaar

De-duplication process remained vulnerable for generating multiple Aadhaar numbers and manual interventions had to be done to resolve the problem.

De-duplication process ensures that the Aadhaar numbers generated are unique and no second number is assigned to the same resident by comparing the resident’s demographic and biometric information collected during the process of enrolment, with the records in the UIDAI database. It also ensures that a data with an already assigned Aadhaar number cannot be used to generate a new number to another resident.

As per information provided by UIDAI Tech Centre, nearly 4.75 Lakh duplicate Aadhaar numbers were cancelled as of November 2019. This data indicated that on an average no less than 145 Aadhaars generated in a day during the period of nine years since 2010 were duplicate numbers requiring cancellation.

Besides this, verification of records at the UIDAI Regional Office Bengaluru showed that residents reported 5,388¹⁵ cases of issue of multiple Aadhaars during the period 2015-16 to 2019-20 forcing UIDAI to cancel the second Aadhaar issued, based on complaints received. We could not ascertain the number of multiple Aadhaars reported at other ROs as access to the related documents was not given to us. UIDAI HQ also could not provide RO wise data on the number of multiple Aadhaars and stated (September 2019) that such data was not available with them. Apart from issue of multiple Aadhaars to the same resident, instances of issue of Aadhaars with the same biometric data to different residents were also seen reported in RO Bengaluru.

Further, information like the date of issue of first Aadhaar, the date of issue of subsequent Aadhaars and the time taken to identify and cancel them were also not provided to Audit limiting our scope for further scrutiny on the issue.

UIDAI stated (September 2019) that the biometric de-duplication ensures uniqueness with accuracy of 99.9 *per cent*, but in cases where residents with poor biometrics enroll, their accuracy could be slightly poor which could lead to generation of multiple Aadhaars. It was also informed that UIDAI has deployed self-cleaning system (an automated process) to identify duplicate Aadhaars and for taking corrective actions. However, no details on the frequency of the deployment of the self-cleaning system, the number of duplicates detected through the process etc., were provided to audit as of July 2020. The fact that residents reported 860 cases of multiple Aadhaars in Bengaluru RO alone during 2018-19 suggested that the self-cleaning system employed by UIDAI was not effective enough in detecting the leakages and plugging them. Though the number of cases reported could be termed as miniscule when compared with the total number of Aadhaars generated.

UIDAI later, (October 2020) explained the “whitelisting process” invoked in case a genuine person is denied Aadhaar through the de-duplication process. It claimed significant improvements in detecting duplicate and fraudulent enrollment after application of Service Level Agreement (SLA) parameters independently for each of the three Biometric Service Providers (BSPs) and incorporation of other SLA parameters like FNIRA¹⁶, attack presentation classification error rate etc. in the new contract. UIDAI also informed that a project with IIIT Hyderabad in the field of biometric was going on to develop indigenous technology to achieve “atmanirbharta”. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

It is evident that UIDAI was aware of generation of multiple Aadhaar which had remained unidentified/detected by it unless brought to their notice. It was also noted that to ensure provision of unique identities to residents, UIDAI has even resorted to Manual De-duplication (MDD) processes in cases where biometric data was rejected by BSPs. The cancellation of duplicate Aadhaars or generation of Aadhaars through MDD indicated flaws in the functioning of BSPs appointed by UIDAI. The failure in De-duplication resulting in denial of Aadhaar can be negated by invoking the whitelisting process for the aggrieved residents. As a result, UIDAI/MeitY needs to devise foolproof mechanisms for capturing unique biometric data.

¹⁵ The total 5,388 cases of multiple Aadhaar reported comprises of 1,131, 2,339, 330, 860 & 728 cases during the years 2015-16, 2016-17, 2017-18, 2018-19 & 2019-20 respectively.

¹⁶ FNIRA: False Negative Identification Rate for Anomalous matches

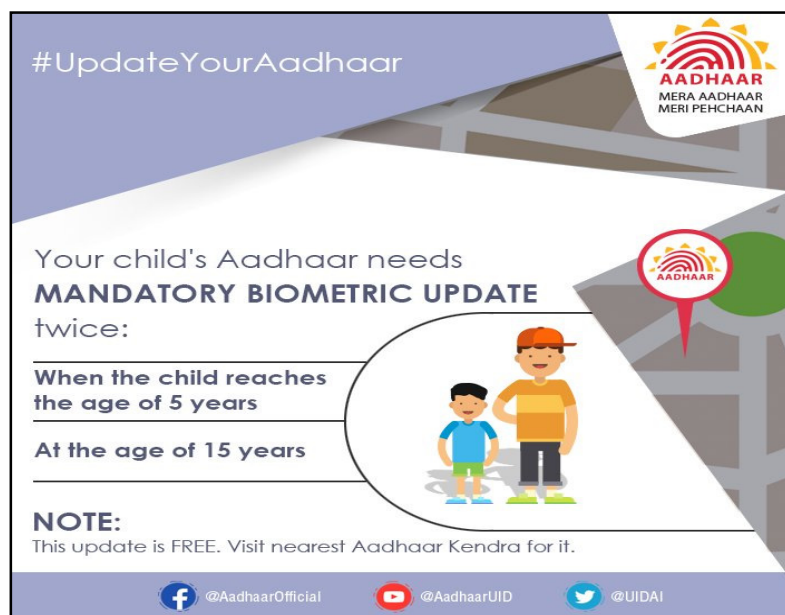
UIDAI also needs to strengthen the Automated Biometric Identification System so that generation of multiple Aadhaars can be curbed at the initial stage itself.

Recommendation: *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.*

3.2.3 Enrolment for Aadhaar of Minor Children below age of five years

The uniqueness of identity, one of the distinctive attributes of Aadhaar, was not ensured while issuing Aadhaar to minor children below the age of five years.

As per the provisions of the Aadhaar Act, 2016, every resident in the country is entitled to obtain an Aadhaar number by submitting his demographic and biometric information by as part of the enrolment process. However, as per Aadhaar (Enrolment and Update) Regulations 2016, biometrics are not captured for Aadhaar generation in respect of minor children below five years of age. Their UID is processed as per Section 5 (1) of these Regulations on the basis of demographic information and facial photograph by linking with the UID of any one of the parents. These children are required subsequently, to update their biometrics (ten fingers, iris and facial photograph), when they turn five and then again on attaining fifteen years of age.



(Image courtesy: UIDAI)

UIDAI regulations state that if a child having attained the age of five or fifteen years of age, fails to update his/her biometric information within two years of attaining such age, his/her Aadhaar number would be deactivated. In cases where such update had not been carried out at the expiry of one year after deactivation the Aadhaar number would be omitted.

Further, UIDAI notified (September 2018) that if the current age of an Aadhaar holder enrolled as a child had crossed 15 years and if his/her biometrics are not updated such Aadhaar would be cancelled.

Audit observed that since UIDAI does not capture biometrics of minor children below five years for generating Aadhaar, the basic condition for issue of Aadhaar i.e. uniqueness of identity was not being met. As per information furnished, UIDAI had generated approximately

11.48 Crore Aadhaars for children below five years till March 2019. The assistance provided to the Registrars/ Enrolment agencies for enrolment @ ₹27 per child along with related costs worked out to ₹310 Crore.

UIDAI informed, that they had deactivated about 40.91 Lakh Aadhaar for want of Biometric Update as on 01 November 2019. With the increase in saturation level, there remains always a possibility that children whose Aadhaar has been deactivated as mentioned above might have enrolled themselves afresh after crossing the age of five, with their biometrics.



(Image courtesy: UIDAI)

Based on the Hon'ble Supreme Court's judgment¹⁷, that no subsidy, benefits, or services could be denied to a child to whom no Aadhaar number was assigned, we are of the view that, the issue of cards, devoid of biometric authentications to children below five years served limited purpose considering the costs involved.

UIDAI stated (June 2020) that it is mandated to issue Aadhaar number to all the residents, including children. Even though, biometrics of children are not collected, child Aadhaar is issued based on authentication of a parent. It added that the chances of creation of duplicate Aadhaar were very low even in the absence of biometric data, and the number of duplicate numbers found/ reported was insignificant. They claimed that issuing an identity to a child, led to monetary savings for the exchequer as it helped eliminate ineligible beneficiaries, and was hence beneficial. They were of the view that the cost incurred was insignificant.

In its subsequent reply (October 2020), UIDAI accepted that the de-duplication done based on the demographic data and photograph may not be as robust as the automated biometric identification system (ABIS). They issue SMS and letters to all the parents/ guardians whose children were due for mandatory update for bringing them back in the Aadhaar ecosystem. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

We are of the view that the UIDAI's mandate was to issue Aadhaar number to a resident after establishing uniqueness of the applicant through his/her biometrics. Therefore, issue of Aadhaar numbers to children without biometric data did not meet the criteria of establishing the uniqueness of the holder and could not be justified on the grounds of the mandate to issue ID to all residents including children. Moreover, as per judgment of the Supreme Court on

¹⁷ Five bench Supreme Court Judgement dated 26 September 2018 on writ petition (civil) No. 494 of 2012 & connected matters

Aadhar, no subsidy, benefits or services cannot be denied to a child for want of an Aadhar number.

Issue of Bal Aadhar to minor children below five years, without capturing their unique identity could not be justified on basis of unquantified advantages as suggested by UIDAI. The fact that an individual is required to apply for regular Aadhar cards for at two stages after crossing five years, UIDAI requires to review the issue of non- mandatory Aadhar to minor children below five years. They may explore alternate ways to capture unique identity of minor children below five years, in keeping with its mandate.

Recommendation: 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.

3.2.4 Management of Aadhaar Documents

All the Aadhaar numbers stored in the UIDAI database were not supported with documents on the demographic information of the resident, causing doubts about the correctness and completeness of resident's data collected and stored by UIDAI prior to 2016.

Upto July 2016, it was the responsibility of the Aadhaar Document Management System (ADMS) (M/s Hewlett Packard Sales India Private Ltd. (HP)) to store the physical sets of records provided by individuals at the time of enrolment, both in electronic as well as physical form in a secured manner. The documents¹⁸ collected by the Enrolment Agencies (EAs) during enrolment/ update were picked up by the ADMS agency on a regular basis from EAs for scanning and uploading into a portal. With effect from July 2016, UIDAI mandated inline scanning¹⁹ of residents' documents²⁰ bringing an end to pick-up of the documents by the ADMS Agency in June 2017.

As significant gaps were noted in the enrolments done and documents submitted by the Registrars/EAs to the DMS Agency, UIDAI issued (December 2015) a set of instructions with the aim of minimizing the gaps and to reconstruct missing documents, for compliance by the DMS agency, the Tech Centre, ROs and Registrars/ EAs. Accordingly, the Tech Centre was to compare the list of Enrolment Identity (EID²¹) received from the DMS agency and generate State/ Registrar/ EA wise list of such EIDs against which Aadhaar has been generated but data prepared by the Agency was missing. The Registrars were to forward the information received from Tech Centre to its EAs for collection of missing documents. The ROs in their turn, were to guide the Registrars/ EAs for reconstruction of data and monitor this activity. The ROs were to furnish monthly progress report (State/ Registrar/ EA wise) to UIDAI HQ showing the number of EIDs requiring reconstruction, number of EIDs for which reconstruction completed and the number of EIDs for which reconstruction was not completed.

¹⁸ Enrolment Identification Documents collected from the residents as their proof of identification, proof of address, proof of date of birth or relationship etc., along with the copy of enrolment/ update form.

¹⁹ Inline scanning is the process where the original documents are scanned and uploaded with the enrolment/ update form to the CIDR at the time of enrolment/ update itself and hence no physical copy is retained/ collected by the operators.

²⁰ Proof of identification, proof of address, proof of date of birth or relationship etc.

²¹ EID- means a 28-digit Enrolment Identification Number allocated to residents at the time of enrolment.

These instructions further suggested that not all the Aadhaar numbers stored in the UIDAI database were supported with documents on the demographic information of the resident, raising questions on the correctness and completeness of resident's data collected and stored by UIDAI.

Data on the number of EIDs against which Aadhaar has been generated but documents were missing and the nature of document(s) identified as missing along with the status of their reconstruction was sought from UIDAI. UIDAI informed (June 2020) that the MSP (Managed Service Provider) had been given the responsibility to map EID-UID linkage for which software development was under progress. It was also informed that with effect from 01 July 2016, inline scanning and upload of Personally Identifiable Information (PII) documents along with enrolment and update packets have been made mandatory and hence all new Aadhaar numbers generated and updated after 01 July 2016 are presumed to have their PII documents. It was further added that since update of Aadhaar numbers by residents is a regular activity, the reconstruction of PII documents was a continuous process and the documents collected from Registrars and EAs were being uploaded/ reconciled, the exact position of deficiency of PII documents had not been worked out.

The response of UIDAI suggested that the enrolments were carried out without confirming availability of all required documents. UIDAI, despite being aware of the fact that not all Aadhaar numbers were paired with the personal information of their holders, was yet to identify the exact extent of mismatch though nearly ten years have elapsed since the issue of first Aadhaar. Non pairing of biometric data in the system with demographic information was not in consonance with the instructions issued by UIDAI and non availability of PII documents with the Authority, for those already collected from the residents, impacts the reliability of the Aadhaar database. Further, any quality check of demographic data by UIDAI post issue of Aadhaar will lead to deactivation of these Aadhaar numbers as stipulated by the Regulations. As a matter of fact, till 01 November 2019, 37,551 Aadhaar numbers were deactivated due to disputed PII documents.

Therefore, UIDAI may identify and fill the missing documents by taking proactive steps at the earliest in order to avoid any legal complications or inconvenience to Aadhaar holder due to suspension/ deactivation of Aadhaar for want of paired PII documents.

UIDAI agreed (October 2020) with the audit recommendation and assured to explore the possibility to fill the gaps in documentation without causing avoidable inconvenience to Aadhaar holders. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

Recommendation: 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.

3.3 Audit Observations on Aadhaar Update Ecosystem

Audit observations on the Aadhaar Update Ecosystem is given below:

3.3.1 Voluntary Biometric Updates

High numbers of voluntary biometric updates indicated deficient capture of biometric during enrolments resulting in Authentication failures resulting in residents having to update their biometrics.

Biometric updates fall into two categories viz., mandatory updates and voluntary updates.

A. Mandatory updates usually arise in the following situations:

- a. A child with age less than five years at the time of initial enrolment should provide biometric information on attaining the age of five years and this initial capture is treated as a mandatory update of an existing Aadhaar.
- b. Children aged between five and 15 years at the time of enrolment should furnish all biometrics for updates when turns 15 years.

B. Voluntary updates may arise in following situations:

- a. Age more than 15 years at the time of enrolment – Residents are recommended to update their biometric data every ten years.
- b. Events like accidents or diseases leading to biometric exception
- c. Biometric updates arising out of authentication failures (False Rejects – where authentication attempts of a resident with valid Aadhaar number is rejected) resulting from incorrect biometric capture or poor biometric quality captured at the time of enrolment.

While mandatory updates are free for the residents, voluntary updates are chargeable for the residents at rates prescribed by UIDAI.

An analysis of data on biometric updates for the year 2018-19 revealed that during the year, UIDAI updated 3.04 Crore biometrics data successfully. Out of the successful updates, 0.81 Crore (26.55 per cent) were mandatory and the remaining 2.23 Crore (73.45 per cent) were voluntary updates.

According to UIDAI, the need for biometric update could arise on account of authentication failures (called “false rejects”- where a correct resident with a valid Aadhaar Number is incorrectly rejected) due to incorrect biometric capture or poor biometric quality captured at the time of enrollment. Thus, a significantly high percentage of voluntary biometric updates indicated occurrence of a high volume of authentication failures, which compel Aadhaar number holders to update their biometrics. This was also a reflection on the quality of biometric data stored in CIDR for establishing the uniqueness of the Aadhaar number holder. It was observed that the UIDAI takes no responsibility for deficient biometric capture and the onus of updating biometric is passed on to the Aadhaar number holders and they are also required to pay for such updates.

UIDAI stated (July 2020) that it was not possible to ascertain reasons for authentication failures or attribute it to incorrect/poor quality biometrics at the backend. It however, confirmed that biometric mismatch could happen due to reasons such as poor quality of biometric capture at the time of enrollment, improper placement of finger at the time of authentication, entering of incorrect Aadhaar number and device quality issues. UIDAI also stated that as per the approved

procedure for enrollment, operators could complete the enrollment even with poor quality biometrics through “forced capture” after four unsuccessful attempts to capture biometric data. It was reported that this procedure was adopted to improve inclusiveness of residents under the Aadhaar programme.

UIDAI agreed (October 2020) with audit observations and explained that most authentication was based on fingerprints which do change in adults with time based on their job profiles. Further, the two other modes of authentication viz “Iris” and “Face” could also be utilized but the devices for Iris checks were comparatively more expensive than the fingerprint authentication devices and efforts were on to introduce more technically certified devices for Iris checks. It also added that it was requesting their ecosystem partners to deploy Iris authentication devices. UIDAI had also developed a model for face authentication which was under trial phase, and that it planned to utilize all the three modes of authentication to overcome the lacunae faced in fingerprint authentications. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

While noting the action taken/ proposed by UIDAI to improve upon the capture of biometrics, we are of the view that acceptance of poor-quality biometrics at the time of enrolment showed that UIDAI had not ensured the quality of biometric data included in the CIDR, adversely impacting the programme’s objective of establishing the uniqueness of the Aadhaar number holder. Further, acceptance of poor-quality biometrics on the plea of expanding the enrollment under the programme and then passing the burden of the updation of biometrics cost to Aadhaar holders did not seem appropriate. Since UIDAI is not in a position to identify reasons for authentication failures of biometrics, it is felt that charging residents a fee for voluntary update of their biometrics was not in order, for no fault of them.

Recommendation: 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.

3.4 Aadhaar Authentication Ecosystem

Entities engaged in providing Aadhaar enabled services can avail the authentication services of UIDAI. The authentication facility allows verification of the identity information of an Aadhaar number holder by providing a Yes/ No response or e-KYC data.

Authentication services are provided online and in real-time basis through its Data centers and are offered through the following modes:

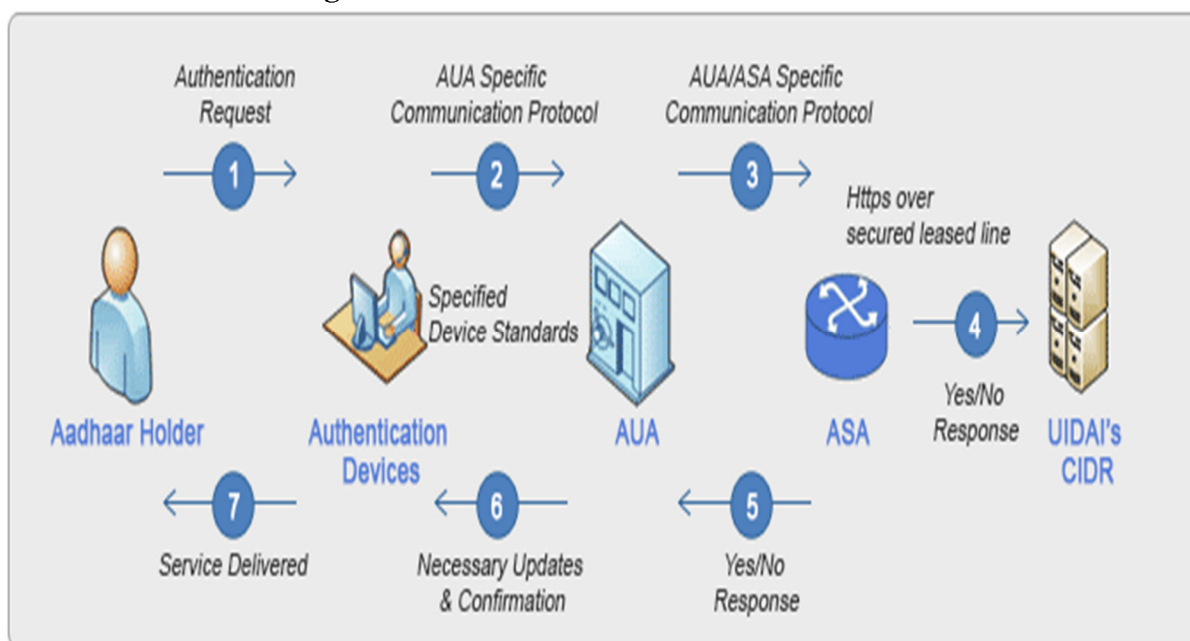
- a. **Demographic authentication:** Aadhaar number and demographic data submitted for authentication is matched with the corresponding data in the CIDR.
- b. **One Time Pin (OTP) based authentication:** OTP is sent to the mobile number or e-mail address of the Aadhaar holder registered with the Authority and the Aadhaar number and OTP is matched with the OTP sent by UIDAI.
- c. **Biometric based authentication:** The Aadhaar number and biometric information submitted by the Aadhaar holder is matched against the biometric data of said Aadhaar number stored in CIDR.

d. Multi-factor authentication: A combination of two or more of the above modes.

3.4.1 Aadhaar Authentication partners

The main players in authentication eco-system are the Authentication User Agencies²² (AUAs)/ e-KYC User Agency²³ (KUA) or the Requesting Entity (RE)²⁴ and the Authentication Service Agencies²⁵ (ASAs). A requesting entity submits the Aadhaar number and demographic information or biometric information of an individual through an ASA, to the CIDR for authentication. The ASA provides the infrastructure for connectivity and related services for enabling a requesting entity to undertake authentication. There were 164 AUAs, 162 KUAs and 22 ASAs entities active as on 31 March 2021. The Aadhaar authentication process is illustrated in **Figure 3.4**.

Figure 3.4: Aadhaar Authentication Process



(Image courtesy: UIDAI)

3.4.2 Key Regulations and Amendments

Key regulations relating to Aadhaar authentication are given in **Table 3.2**.

²² UIDAI provides Yes/ No authentication services through requesting entities called Authentication User Agency (AUA). AUA is any government/ public legal entity registered in India that uses Aadhaar authentication for providing its services to the residents/customers. An AUA is connected to the UIDAI Data Centre/ Central Identities Data Repository (CIDR) through an ASA.

²³ KUA is a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility.

²⁴ Requesting Entities are Authentication User Agencies (AUAs) and e-KYC User Agencies (KUAs).

²⁵ ASA is an agency that has secured leased line connectivity with CIDR. They play the role of enabling intermediaries through secure connection established with the CIDR. ASAs transmit authentication requests of AUAs to the CIDR and transmit back the CIDR's response to the AUAs.

Table 3.2: Key regulations and amendments thereto governing Aadhaar Authentication System

Key Regulations	Key features
Aadhaar (Authentication) Regulations 2016 (No. 03 of 2016) Dated 14-Sep-2016	<ul style="list-style-type: none"> ✓ Authentication Framework- Types/ Modes of Authentication, capturing of biometric information, Consent of/ Notification to holder, Devices, Client applications used, Biometric Locking etc. ✓ Appointment of Requesting Entities & Authentication Service Agencies- (Procedures, Eligibility Criteria, Roles & Responsibilities, Obligations, Code of Conduct, maintenance of logs, Audit, Data Security, Surrender, Liabilities & Action in case of Default etc.) ✓ Use of Yes/No & e-KYC authentication ✓ Authentication Transaction Data & its Records- Storage& Maintenance of Transaction Data, Duration of Storage, Access by Aadhaar holder
Aadhaar (Pricing of Aadhaar Authentication Services) Regulation 2019 Dated 06-Mar-2019	<ul style="list-style-type: none"> ✓ Aadhaar Authentication Services to be charged (including taxes) @ ₹20 for each e-KYC transactions and @ ₹0.50 for each Yes/No authentication transaction by requesting entities. ✓ Exemption to Government entities and Department of Posts and conditional exemptions to Scheduled Commercial Banks engaged in Aadhaar enrolment & update facilities

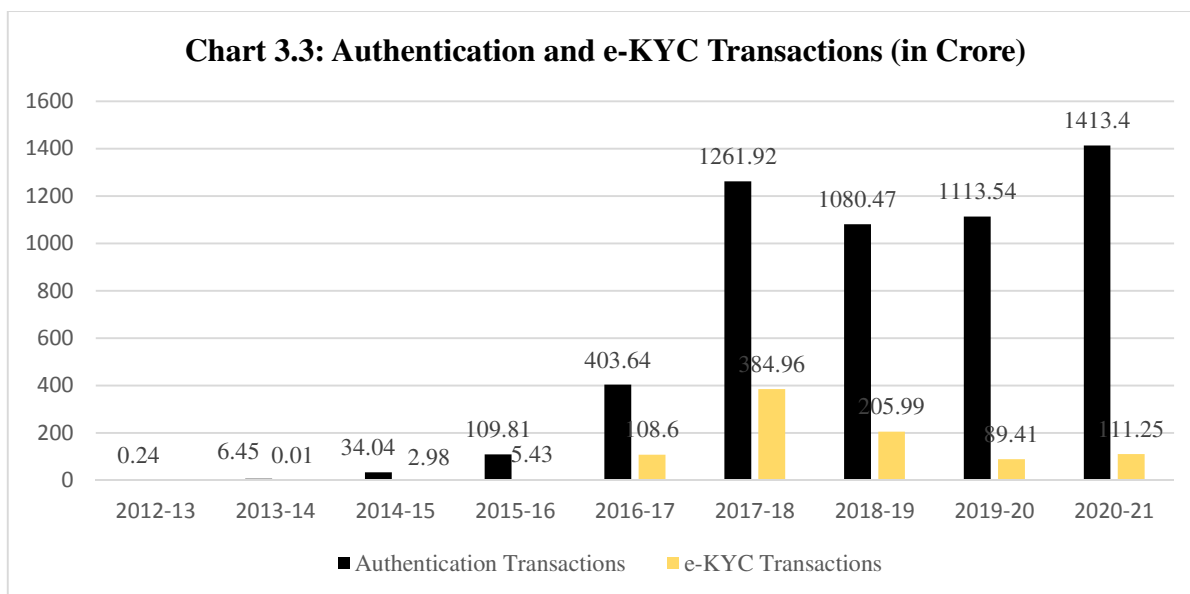
3.4.3 Status of Authentication Transactions

Aadhaar authentication is the process by which the CIDR, based on the information available with it, verifies the correctness of the Aadhaar number submitted to it along with the demographic and biometric information for verification. UIDAI provides two types of authentication services viz. “Yes/ No²⁶” authentication facility and “e-KYC²⁷” authentication facility using Aadhaar.

As of March 2021, UIDAI has performed more than 5,400 Crore authentication transactions and above 900 Crore e-KYC transactions. The year wise authentication and e-KYC transactions are as in **Chart 3.3**.

²⁶ “Yes/ No” Authentication: UIDAI started Yes/ No Authentication facility in February 2012 under which requesting entity sends Aadhaar and necessary demographic and/ or OTP and/ or biometric information of the Aadhaar number holder in an encrypted format. UIDAI validates the input parameters against the data stored in CIDR and authenticates in a ‘Yes or No’ response.

²⁷ e-KYC Authentication: UIDAI started e-KYC Authentication facility in May 2013 under which a requesting entity sends Aadhaar and necessary biometric information and/ or OTP from the Aadhaar number holder in encrypted format. UIDAI validates the input parameters against the data stored in CIDR therein and returns authentication response as an encrypted digitally signed e-KYC.



3.5 Audit observations on Monitoring of Ecosystem partners on compliance to the provisions of Aadhaar (Authentication) Regulations 2016

Aadhaar authentication framework comprises of REs and ASAs. These entities collect the biometric information of the Aadhaar holder for validation purposes. Their interaction with Aadhaar number holders and UIDAI is through the digital mode. Aadhaar (Authentication) Regulation 2016 and other directions of UIDAI notified from time to time, contain instructions on the arrangements which all the entities involved in the authentication ecosystem should follow for ensuring the security of data of the residents. The regulation also specifies the responsibilities of UIDAI in monitoring e-compliance with its instructions by the ecosystem partners’ viz. ASA, AUA, KUA etc.

Audit observations on compliance with provisions of the Regulation and the processes put in place by UIDAI to monitor the activities of the REs and ASAs are given in the succeeding paragraphs.

3.5.1 Incidences of Authentication Errors

Aadhaar was conceived to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services to Aadhaar number holders by means of successful authentication. The fingerprint authentication transaction success rate remained a cause of dissatisfaction among the users due to biometric authentication failures.

Authentication services of UIDAI is a tool relied upon by government departments to confirm the genuineness of recipients of various benefits from government schemes and programmes. Inaccurate authentication therefore, would lead to errors in identification with consequent implications for effective delivery of services and benefits. In addition, authentication errors compel an Aadhaar number holder to update his/her biometric data. As per a Government of India Report²⁸ Aadhaar authentication failures in certain States were as high as 49 per cent in 2016-17.

²⁸ The Economic Survey 2016-17 (Refer 9.76) published by the Ministry of Finance: “While Aadhaar coverage speed has been exemplary, with over a billion Aadhaar cards being distributed, some states report authentication failures: estimates include 49 per cent failure rates for Jharkhand, six per cent for Gujarat, five per cent for Krishna District in Andhra Pradesh and 37 per cent for Rajasthan”

On the subject of authentication errors, UIDAI informed (July 2020) that it does not receive location data during authentication, and in the absence of State-wise information on authentication failures reasons for the same have not been analyzed.

UIDAI further explained (October 2020) that there might be failure of fingerprint authentication in the first attempt due to various reasons, but subsequent attempts may succeed. It claimed that there had been improvement in transaction wise fingerprint authentication success rate from 70-72 per cent in 2016-17 to 74-76 per cent in 2019-20. It mentioned that to address connectivity issues, buffer authentication had been allowed to REs and in addition, efforts were underway to promote iris authentication and launch face authentication on pilot basis. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.



Image 3.1: Illustrative image of authentication success.
Image courtesy: www.basunivesh.com

While there may be various reasons for fingerprint authentication requiring multiple attempts for authentication, this may result in dissatisfaction to Aadhaar holders for repeated biometric authentication failures. The promotion or launch of other forms of biometric authentication might improve the success rate of transactions but their performance has not yet been tested on large scale.

Also Audit has not been provided any basis on which UIDAI has claimed the success rate mentioned here as improvement in failure rates.

Audit is of the view that since Aadhaar as an instrument facilitates good governance through authentication, UIDAI may make efforts to improve the success rate of authentication and also take action to analyze failure cases.

Recommendation: UIDAI may make efforts to improve the success rate of authentication transactions by analysing failure cases.

3.5.2 Non verification of the infrastructure and technical support of Requesting Entities and Authentication Service Agencies

UIDAI did not verify the infrastructure and technological support claimed by the REs and ASAs independently before onboarding the entities in the Aadhaar authentication ecosystem.

The Aadhaar (Authentication) Regulations 2016 stipulate that agencies seeking to become REs and ASAs should fulfill the criteria laid down by UIDAI. Regulation 12 of the Aadhaar (Authentication) Regulation, details the conditions for appointment of REs and ASAs. The regulation authorizes UIDAI to verify the information furnished by the applicants in support of their eligibility through physical verification of documents, infrastructure and technological support, before approval of the applications.

In this context, data on systems put in place for physical verification of the infrastructure and technological support claimed by the applicants for appointment as REs, and details of audit undertaken of infrastructure and technical systems of the REs prior to their appointment were sought (July 2019) from UIDAI. In response UIDAI informed (June 2020) that they had not felt the need so far for conducting physical verification of the infrastructure and technical systems of the applicants prior to signing agreements with them. It was further informed that the REs while moving from pre-production to production environment, were required to submit an IS Audit Report from a CERT-IN empaneled Auditor which was scrutinized by UIDAI.

As of March 2021, 326 REs (164 AUAs and 162 KUAs) and 22 ASAs were active in production environment of the CIDR. Out of these 326 REs, 43 AUAs and 41 KUAs were Government entities whereas out of 22 ASAs, 12 ASAs were Government entities. Further six Government REs (three AUAs & three KUAs) and 44 other than Government REs (22 AUAs & 22 KUAs) had permission in pre-production environment as of March 2021. UIDAI had not verified information furnished by any of the applicants independently (October 2020).

UIDAI accepted (October 2020) the audit observation and assured that it would conduct thorough verification of the documents, infrastructure and technological support before on-boarding the entities (REs and ASAs) in Aadhaar ecosystem. It added that such verification would however, be conducted at the discretion of UIDAI keeping in view the nature of AUA/KUA and the urgency of implementing authentication service. UIDAI will initiate measures to implement it to the extent possible also keeping in view the constraints posed due to the ongoing Covid- 19 pandemic. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

Therefore, UIDAI should institute a mechanism for physical verification of the documents, infrastructure, and technological support before on-boarding the entities (REs and ASAs) to ensure high standards of IS security across the Aadhaar authentication ecosystem. Audit appreciates UIDAI's decision to conduct physical verification of the documents, infrastructure and technological support before on boarding the entities (REs and ASAs) in Aadhaar ecosystem. However, use of discretionary power to not conduct any verification should be governed by a well-defined criteria/ benchmarks and exemptions from physical verification of the entities, may be granted in exceptional cases only, in interest of IS concerns.

Recommendation: *UIDAI may conduct thorough verification of the documents, infrastructure, and technological support claimed to be available, before on-boarding the entities (Requesting Entity and Authentication Service Agencies SAs) in the Aadhaar ecosystem.*

3.6 Other related Audit Observations

Audit observations on compliance with provisions of the Regulation and the processes put in place by UIDAI related to the Aadhaar Enrolment, Update and Authentication ecosystem has already been discussed in the foregoing paragraphs. The other important and related observations are discussed in the following paragraphs:

3.6.1 Data Archival Policy

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.

Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of older data that remains important to the organization for future reference or regulatory compliance reasons. It is a storage management best practice for efficient use of storage space and performance enhancement. UIDAI is maintaining one of the largest biometric databases in the world and hence it is vital for the Organization to have a policy on archiving the data collected.

It was seen in audit that during the Aadhaar enrolment process, data packets containing demographic and biometric information of the residents are subjected to various processes like Quality Checks (QC), Demographic de-duplication, Biometric de-duplication, Manual de-duplication (MDD) etc., to identify and weed out erroneous/ duplicate/ junk packets. Audit observed that packets rejected at QC stage remained present in the UIDAI database along with the accepted packets. So even where packets are rejected on account of de-duplication, UIDAI apparently will have more than one set of biometric data of the same resident - one with an Aadhaar number attached and others with all details except an Aadhaar number (new enrolment request) and all the data are retained in the CIDR. Retaining any data requires valuable resources, hence valid and necessary data should be only archived. In absence of a data archiving policy, UIDAI retains and preserves large volumes of redundant/ excess data for longer periods.

With a sound data archival policy, an organization like UIDAI, can not only have access to all classes of data whenever the need arises but also reduce the size of storage by disposing off redundant data regularly. It is therefore vital that UIDAI frames a Data Archival Policy and implements it strictly. UIDAI agreed (October 2020) with the audit recommendation and assured to work towards framing a suitable Data Archiving Policy. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

Recommendation: 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 .

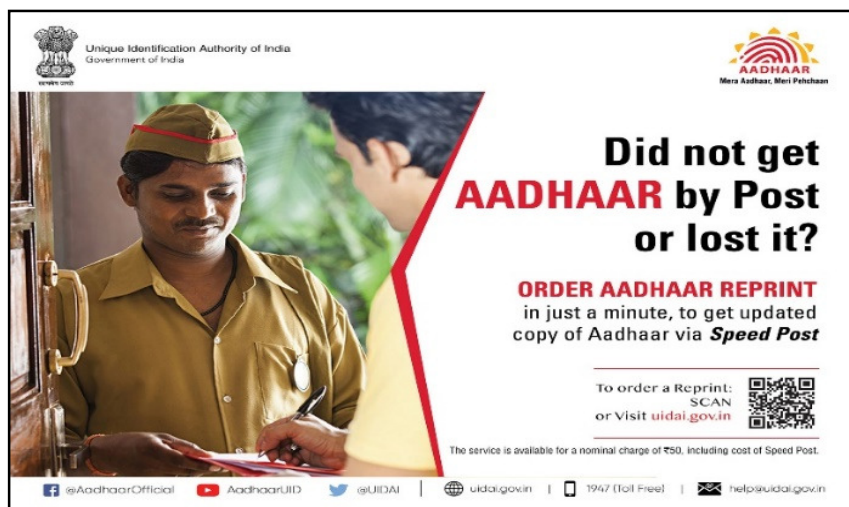
3.6.2 Delivery of Aadhaar Documents

UIDAI did not work out a customized delivery solution with DoP to ensure last mile successful delivery of Aadhaar letters.

Aadhaar cards in laminated form are printed and dispatched by UIDAI in all the cases of successful enrolments and updates. DoP is the logistic partner for delivery of Aadhaar letters as First-Class Mail (Ordinary Post). The ordinary post services of India Post do not provide any individual dispatch number or tracking facility.

As more than 250 welfare schemes of the Government require identification through Aadhaar, possession of Aadhaar assumes importance for residents to avail benefits from these schemes. An effective delivery mechanism is thus vital to ensure that Aadhaar letters are delivered to the intended individuals. Also as per the Aadhaar Act 2016, UIDAI is responsible for the security

of the identity information of the Aadhaar holder. In cases of non-receipt of Aadhaar letters by post, an individual can receive the original Aadhaar letter by approaching the Grievance Cell of UIDAI or by downloading e-Aadhaar. UIDAI also introduced an “Order Aadhaar Reprint” (OAR) service in December 2018.



(Image courtesy: UIDAI)

Audit observed that UIDAI received back 50 Lakh Aadhaar letters at its Bengaluru Centre till March 2019 due to non-delivery to residents. Residents also made complaints about non-delivery of Aadhaar letters at UIDAI Grievance Cell and through RTI requests.

Further, dumping/ abandoning of Aadhaar letters in bulk without delivering to the residents had been highlighted in various news media also.

As UIDAI has availed Ordinary Post Services from DoP, it was not in a position to track the receipt of the physical Aadhaar card by the addressee. In absence of any formal agreement or MoU as regards manner of delivery of Aadhaar letters with India Post, UIDAI had not ensured the confidentiality aspect of Aadhaar cards issued.

UIDAI informed (July 2020) that more than 122 Crore Aadhaar letters have been successfully delivered and DoP is regularly being addressed to ensure and strengthen the delivery of Aadhaar letters.

UIDAI further informed (October 2020) that it has requested DoP to develop a customized tracking system for Aadhaar letters to monitor their delivery and to sensitize their personnel/ staff in ensuring proper delivery to the residents. In addition, UIDAI has facilitated residents with an option to download their ‘e-Aadhaar’ or use official mobile app ‘m-Aadhaar’. Besides, UIDAI started (December 2018) Order Aadhaar Re-print (OAR) Service for residents by using which any Aadhaar holder could order online Aadhaar letter by paying ₹50 per order and get it through Speed Post service of DoP. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

In this regard, Audit noted the action taken by UIDAI but they could have negotiated with India Post for a customized delivery solution for delivery of Aadhaar letters. The options like ‘e-Aadhaar’, ‘m-Aadhaar’ and ‘OAR’ have several limitations requiring the residents to have additional resources and efforts, whereas a doorstep delivery of laminated Aadhaar letters has its own advantage for residents from all walks. Since a large number of Aadhaar cards/ letters were not actually delivered to residents, it raises doubts on the number of Aadhaar cards shown

as issued. Thus UIDAI should strengthen its last mile delivery mechanism to ensure effective delivery of the cards issued coupled with security of the identity information.

Recommendation: *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.*

CHAPTER 4

Management of Finances and Contracts

Chapter 4

Management of Finances and Contracts

4.1 Introduction-Budget and Finance

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, stipulates that the expenditure of UIDAI is to be met out of the Grants from the Central Government. The fees or revenue collected by the Authority is to be credited in the Consolidated Fund of India till the creation of separate UIDAI Fund. The expenditure of UIDAI is furnished below in **Table 4.1**.

Table 4.1: Budget (Revised) Estimates and Expenditure of UIDAI

(₹ in Crore)

Year	Budget (Revised) Estimates	Expenditure
2009-14	4,400.18	4,365.28
2014-15	1,617.73	1,615.34
2015-16	1,880.93	1,680.44
2016-17	1,135.27	1,132.84
2017-18	1,150.00	1,149.38
2018-19	1,344.99	1,181.86
2019-20	836.78	856.12 ²⁹
2020-21	613.00	892.67 ³⁰

(Data Source: Information Supplied by UIDAI and UIDAI website)

The expenditure of UIDAI is mainly on establishment and operational expenses. The budget and expenditure of UIDAI has reduced from 2009-14 to till date. As per Aadhaar (Amendment) Act 2019, a separate UIDAI Fund³¹ was created to which all grants, fees and charges received by the Authority were to be credited. The Fund so created was to be applied for meeting salaries and allowances and operations. Balance in this fund as on 31 March 2021 was ₹322.40 Crore.

Year-wise revenue earned, deposited in Consolidated Fund of India (CFI) and the balance utilised or lying with the UIDAI is shown below in **Table 4.2**:

²⁹ Excess expenditure met from unspent balance of 2018-19.

³⁰ Excess expenditure met from unspent balance of 2018-19 & 2019-20 and UIDAI Fund

³¹ The Aadhaar and Other Laws (Amendment) Ordinance 2019 (No.9 of 2019) (dated 02 March 2019) which become the Aadhaar and Other Laws (Amendment) Act (dated 23 July 2019)

Table 4.2: Statement showing Revenue earned and its utilisation

(₹ in Crore)

Year	Revenue earned	Deposited in Consolidated Fund of India ³²	Balance ³³
2009-17	The amount is not separately available as the UIDAI was working under Planning Commission and as an attached Office under MeitY.		
2017-18	160.76	160.76	0.00
2018-19	65.38	22.09	43.30
2019-20	224.59	21.82	202.77
2020-21	331.65	9.25	322.40

(Data Source: Information Supplied by UIDAI)

All the earnings of UIDAI including the interest and the unspent Grant-in-Aid were deposited in the CFI till 2017-18. From 2018-19 onwards, the entire revenue was deposited in UIDAI Fund and since then, they have deposited only the interest earned on Grants in Aid in the CFI.

4.2 Audit Observations on Revenue Management

The major source of Revenue for UIDAI comprises License Fee recoverable from ASAs and AUAs, Authentication Charges for biometric verifications in the shape of OTP, eKYC and financial disincentives levied on contractors/ partners etc for deficiencies in services. The audit observation on Revenue Resources is given below:

4.2.1 Non-Levy of charges for delivery of authentication services

UIDAI took three years from the enactment of the Aadhaar Act 2016 to decide the applicable fees for authentication services and allowed a large number of authentication transactions without charging any fees, in violation of their own Regulations, resulting in loss of revenue to the Government.

Section 8(1) of The Aadhaar Act 2016 and Section 12(7) of Aadhaar (Authentication) Regulations 2016 authorizes UIDAI to perform authentication of the Aadhaar number of an Aadhaar holder on payment of a fee. The conditions for providing the service and the fee applicable should be decided by UIDAI. Accordingly, UIDAI notified (March 2019), the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019 wherein, the charge for Aadhaar authentication services was fixed @ ₹20 (including taxes) for each e-KYC transaction and ₹0.50 (including taxes) for each Yes/ No authentication transaction from requesting entities. Government entities and the Department of Posts were exempted from authentication transaction charges. Levy of authentication transaction charges was to commence from 07 March 2019.

Audit observed that UIDAI took almost three years from the enactment of the Aadhaar Act 2016 to decide the applicable fees for authentication services. In the meantime, the Department of Telecommunication (DoT) permitted (March 2017) Telecom Service Providers (TSPs) to

³² From the year 2018-19 onwards only the amount of interest earned on the Grants-in-Aids received by UIDAI has been deposited in CFI.

³³ The balance amount includes the amount utilised by the UIDAI as well as the amount deposited in the UIDAI Fund

re-verify all their mobile subscribers through Aadhaar based e-KYC process and the Central Government in consultation with the Reserve Bank of India made (October 2017) linkage of Aadhaar number to bank account mandatory under the Prevention of Money-Laundering (Maintenance of Records) Second Amendment Rules, 2017. As such, the TSPs and banks updated their databases using the e-KYC services of UIDAI. Data on e-KYC and authentication showed that UIDAI performed nearly 637³⁴ Crore e-KYC transactions until March 2019, of which 598 Crore transactions (94 *per cent*) were for TSPs and banks alone. Besides, the increased acceptance of Aadhaar as a valid identity document led to an increase in the authentication transactions also and UIDAI performed 2,491 Crore authentication transactions (Yes/ No) during the same period. The belated decision of levying Fee for authentication services resulted in free services to parties even though the Aadhaar Act stipulated a fee to be charged for such services.

UIDAI stated (October 2019) that Aadhaar authentication was conceived as an enabler of good governance and not as a revenue generation measure and charging for authentication services would have “stifled government’s good governance efforts”. Further, since writ petitions challenging the constitutionality of the Aadhaar Act were being heard in the Apex Court, the Authority waited for clarity and stabilization of the policy framework before introducing authentication charges. As such, it was a conscious decision to introduce user fees in a staggered manner as the priority was to promote the usage of Aadhaar. UIDAI Management also took the view that they were the sole competent authority to decide on pricing for services and took a considered policy decision on charging of the requisite fees only when the statutory and legal landscape was mature enough.

Explaining the free e-KYC service to TSPs, it was stated that re-verification of mobile subscribers was mandated by Government policy and law, UIDAI was expected to enable re-verification by provisioning of e-KYC services and therefore levying any kind of fee for it would have been wrong and not in public interest. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

Audit does not agree with the views of UIDAI since in terms of the Aadhaar Act, UIDAI was mandated to specify fees for the service, and it was never the intention of the Government to provide free services for authentication facilities. Holding back levy of fees on the plea of the pending matter in the Court is also not acceptable as UIDAI had continued with the enrolment process and authentication services and had also prescribed a licence fee for the services utilised by REs and ASAs during the pendency of the Court case whereas only fees for authentication services were not levied. The response that the Competent Authority exercised its discretionary powers to levy the fees, is also not acceptable as it cannot override express provisions of an Act passed by Parliament. Besides the UIDAI did not produce any file or records to the audit in order to substantiate their statement that it was a “conscious decision” of the Organization to defer/not charge any fees for the authentication services rendered to TSPs and others.

³⁴ The e-KYC figure of 637 Crore represents the data from 12 September 2016 (date of effect of the Aadhaar Act 2016) to 06 March 2019 (Prior to the date of effect of Pricing of Aadhaar Authentication Service Regulations, 2019) with proportionate data for the respective years. The Authentication (Yes/ No) figures of 2,491 Crore have similarly been arrived.

The argument that levy of fee for e-KYC services given to TSPs was not in public interest, is not sound as verification of the credentials of a subscriber is compulsory for TSPs which in any case was incurring expenditure on the same by using other KYC methods. By offering free e-KYC service, UIDAI violated their own Regulations by facilitating the TSPs and banks an easy access to the Aadhaar database set up by the Government at considerable cost. In the process, a delayed decision has also resulted in a loss of revenue to the Government.

Recommendation: *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.*

4.3 Contract Management

The entire end-to-end technology infrastructure of UIDAI including data center operations, management of IT systems of UIDAI ROs, technical helpdesk etc., is managed by the Managed Service Provider (MSP) namely M/s HCL Infosystems Ltd.

Apart from the MSP contract, UIDAI has agreements for Project Management Unit (PMU) functions, supply of resources for offering handholding support to State Governments for roll out of Aadhaar, technical assignments, document management, printing and dispatch of Aadhaar letters etc.

4.3.1 Selection of Contracts

The contracts and agreements entered by the UIDAI were selected for scrutiny based on a statistical sampling technique. The 25 per cent of contracts valuing less than ₹100 Crore were selected by following random sampling. However, all the contracts of ₹100 Crore and above were selected for scrutiny. The brief description of the selected Contracts is placed as **Annexure-I**. Major contracts placed in a nutshell are as below:

Table 4.3: Statement showing brief description of Major Contracts

Contracts	Vendor and Cost of Contracts	Description
Managed Service Provider (MSP)	M/s HCL Infosystems Ltd (HCLI) ₹1,978.62 Crore	<ul style="list-style-type: none"> ✓ Expression of Interest (EoI) for selection of MSP was floated in June 2010 (Twelve Companies submitted EOI) and after evaluation Request for Proposal (RFP) was issued on 24 January 2011 to nine Companies. ✓ Six bidders submitted their bids and finally two bidders qualified on Technical Evaluation and Due diligence. M/s HCLI emerged successful after all sorts of evaluation³⁵ and a contract with a validity of seven years was entered on 07 August 2012. ✓ The contract was extended for nine months, from 07 August 2019 to 06 May 2020. The vendor moved to Arbitration Tribunal and under the directions of Tribunal the contract was extended for eleven months till 06 April 2021. Both the extensions were with the same terms and conditions of original contract.

³⁵ Technical Evaluation, Due Diligence, Commercial Evaluation and Quality and Cost Based Selection (QCBS) Evaluation

		<ul style="list-style-type: none"> ✓ The Contract extensions were managed from the unspent balance of the initial contract ✓ The arbitration proceedings were still under progress (September 2021)
Data Centre Development Agency (DCDA)	<p>M/s Wipro Ltd (WIPRO)</p> <p>The total cost involved, including the extension was ₹238.11 Crore (₹118.51 Crore for Bengaluru DC and ₹119.61 Crore for Manesar DC).</p>	<ul style="list-style-type: none"> ✓ Request for Quotation (RFQ) in respect of Selection of DCDA for the Bengaluru and Manesar Data centres was issued on 16 September 2011. Nine bidders participated and five bidders were shortlisted in the Request for Proposal (RFP) floated in April 2012. ✓ M/s Wipro Ltd emerged as the lowest bidder (L1) and the contract was made effective from 6 December 2012. ✓ The Capex contract was valid till 12 August 2014 for Bengaluru DC and till 30 September 2014 for Manesar DC. ✓ The OPEX contract was valid from 13 August 2014 to 14 August 2019 for Bengaluru DC and from 01 October 2014 to 30 September 2019 for Manesar DC. ✓ The OPEX contract was extended for six month each and the new validity was till 14 February 2020 and 31 March 2020 for the Bengaluru and Manesar Data centres respectively.
Governance Risk Compliance and Performance-Service Provider (GRCP)	<p>M/s Price Waterhouse Coopers (PwC)</p> <p>₹17.53 Crore</p>	<ul style="list-style-type: none"> ✓ RFP was issued on 03 November 2014 to six bidders. After Pre-qualification/ Technical and Financial Evaluation M/s PwC was awarded the contract on 06 October 2015 till 28 February 2018. ✓ The Contract was extended four times- <ul style="list-style-type: none"> • 1st extension for one year till 28 February 2019 • 2nd, 3rd and 4th extension each for three months till 31 May 2019, 31 August 2019 & 30 November 2019 respectively. • 5th extension was for one month and the contract was closed on 31 December 2019. ✓ The total amount released to the vendor including the extensions was ₹20.59 Crore.
Aadhaar Document Management System (ADMS)	<p>M/s HP India sales Private Ltd (HPISP)</p> <p>The cost of services for five years for 95.22 Crore EIDs was ₹278.61 Crore.</p>	<ul style="list-style-type: none"> ✓ RFP was issued on 15 January 2011. Pre-bid conference held with thirty organisations on 27 January 2011 and seven bids were submitted. ✓ Six bidders became eligible for opening of commercial bids after evaluation of technical Committee and M/s HPISP emerged successful after completion of the tender evaluation process. ✓ The contract was signed on 07 June 2011 and was valid for five years. The cost of services will change annually depending on the number of Enrolment IDs (EIDs) to be picked up. ✓ The contract was given an extension on 16 September 2016 for further EIDs of 15 Crore for ₹49.37 Crore. Total cost for 110.22 Crore documents was ₹327.98 Crore. The contract was successfully closed on 07 June 2021.

4.4 Audit Observations on Contract Management

Since the complete files relating to award of contract of the above were not made available, audit could not provide a reasonable assurance on these contracts. However, audit observations on the management of the various contracts by UIDAI are brought out in the succeeding paragraphs:

4.4.1 Liquidated damages (LD) for deficient performance of biometric solutions not levied

UIDAI did not penalize deficient Biometric Service Providers (BSPs) despite shortcomings in their services.

The Service Level Agreement (SLA) conditions of the MSP contract prescribe the expected service levels to be provided by the service provider including the performance of the biometric solutions. Wrong decisions by the biometric solutions would lead to issue of multiple Aadhaars (FNIR³⁶) to the same resident or denial of Aadhaar to a genuine applicant (FPIR)³⁷. Similarly, wrong outcomes of authentication transactions, will result either in a genuine person not getting the intended benefit (FNMR)³⁸ or a wrong person is availing the undue benefit (FMR)³⁹. Thus, it was imperative that the biometric solution related levels are maintained as close to the defined threshold levels as possible. Non-compliance with the performance benchmarks would attract liquidated damages (LD), as per the Agreements depending on the severity level. The cumulative LD i.e. LD applicable of all the SLAs was limited to 20 *per cent* of the fee payable for each quarter and the quarterly payments comprised of the amortized cost of cell⁴⁰ payable in that quarter and the cost of managed services for that quarter.

As per the contract, the MSP was responsible for selection and evaluation of biometric solutions meeting UIDAI's requirements and implementation of three biometric solutions⁴¹.

Audit observed that there were regular breaches of FMR and FNMR targets in the authentication transactions to levels that attracted LD of two *per cent* in every quarter. Accordingly, the Technical Centre, Bengaluru had recommended imposition of LD amounting to ₹13.29 Crore on the MSP for the period up to January 2019. However, UIDAI finally did not impose any LD on the MSP for deficient performance.

UIDAI stated (February 2020) that as per the MSP contract, biometric payments do not form part of the quarterly payment on which LD could be applied. Further, it was indicated that deviations in biometric SLA are factored in the LD computed for a quarter, by including the LD *per cent* for biometric track SLAs in the overall LD *per cent* calculated for the quarter and the maximum rate of 20 *per cent* is being imposed on the vendor every quarter.

³⁶ FNIR- False negative identification is an incorrect decision of the biometric system that an applicant for a UID, making no attempt to avoid recognition, has not previously enrolled in the system, when in fact he/ she has. FNIR is the ratio of the number of false negative identification decisions to the total number of enrolment transactions by enrolled individuals.

³⁷ FPIR-False positive identification is an incorrect decision of the biometric system that an applicant has already enrolled in to Aadhaar when he/ she has not. FPIR is the ratio of the number of false positive identification decisions to the total number of enrolment transactions by unenrolled individuals.

³⁸ FNMR-The ratio of the number of authentication transactions conducted by data subjects resulting in a false non-match to the total number of transactions.

³⁹ FMR-The ratio of number of authentication transactions conducted by authentication subjects resulting in false match to the total number of transactions.

⁴⁰ Cell means any set of technology and physical components which collectively hosts the software programs that performs/enables the set of UIDAI's business requirements. As per MSP agreement with M/s HCL, one cell denotes two Crore Aadhaar enrolment. 'Amortized cost of Cell' has been considered as balance 30 *per cent* cost of cell components which is being paid to MSP in equal installments in every quarter.

⁴¹ The biometric solution is primarily comprised of the multi modal "Automatic Biometric Identification Subsystem (ABIS) for De-duplication and the software Development Kit (SDK). Multiple multi-modal solutions from three vendors (known as BSP-Biometric service Provider) are being used to ensure a vendor independent & technology Neutral solution.

The response was not acceptable, because there was a capping of 20 *per cent* for LD to be imposed which had already reached the maximum due to the failure to meet other SLA parameters. In fact, the LD recommended by the Tech Center in respect of deviation in Biometric SLAs never came to reckoning as evident from the fact that the quantum of LD to be applied was only on the sum of Amortised cost of ‘Cell Payable’ & ‘Cost of Managed Services’ in a quarter. The Cost of Biometric Solution was never considered for levying the LD based on agreement. Success of Aadhaar hinges upon the efficiency of the biometric de-duplication services and hence it was important to ensure that the biometric service providers (BSPs) are accountable for any deficiency in service. When the payments for biometric services are kept out of the purview of LD, the shortcomings in the services provided by BSP were not adequately covered in the MSP contract.

We further observed that as per the agreement (June 2013) between the MSP and the BSPs, the MSP could levy LD on the BSPs for deficient performance of biometric solutions. However, the said condition was amended (November 2016), with the consent of UIDAI to the effect that the MSP will waive off all SLAs, if the same were waived off by UIDAI for the MSP under the MSP contract. With UIDAI keeping payments for biometric services out of the purview of its quarterly payments to the MSP, the MSP waived off the LD due from BSPs for deficiencies in the performance of biometric services. Thus, breaches in the performance benchmarks for biometric services were never penalized either by UIDAI or by the MSP, which gave undue advantages to the MSP/ BSPs.

UIDAI further intimated (October 2020) that the matter was under arbitration and counter claims including the LDs to be recovered from the biometrics’ payments was submitted in September 2020 to the Tribunal. UIDAI further submitted that it has engaged three new BSPs through exclusive contracts signed directly between UIDAI and BSPs, having provision of biometric SLAs and LD which would be levied on BSPs for any breach of these SLAs. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

Recommendation: 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

4.4.2 Deficiencies in monitoring contracts with NISG

UIDAI had partnered with the National Institute for Smart Governance (NISG)⁴² for setting up a professionally managed team for project management, operations management, technology support, handholding support to State Governments for implementation of Aadhaar project etc. Details of assignments handled by NISG for UIDAI are in **Table 4.4**.

⁴² NISG is a non-profit company setup in PPP in 2002 with 51 *per cent* equity contributed by the private sector and 49 *per cent* by the public sector. It assists Central and State Governments in e-governance initiatives to improve services to citizens, businesses and all sections of society.

Table 4.4: Assignments handled by NISG

Agreement	Date of Agreement	Agreement period	Contract value (₹ Crore)	Amount released (₹ Crore)	Amount utilized (₹ Crore)
1. Establishment of Project Management Unit (PMU)	30 Nov 2009	Up to Nov 2014	47.91	110.20	107.74
	Addendum-I 18 Dec 2013	Up to Mar 2017	40.68		
	Addendum-II 01 Apr 2017	Up to Mar 2020	28.10		
2. Project management resource (SRP) for assisting State Registrars	22 Nov 2010	Up to Nov 2013	Value of contract not specified in the agreement	17.23	17.23
	Addendum-I	Up to Nov 2016			
	Addendum-II	Up to Mar 2017			
	Addendum-III 01 Apr 2017	Up to Mar 2020			
3. Aadhaar Enabled Applications Group (AEAG)	18 Apr 2011	Up to Mar 2016	28.50	22.71	22.71
	Addendum-I 08 July 2015	Up to Mar 2017	*		
	Addendum-II 01 Apr 2017	Up to Mar 2020	16.50		
4. Establishment of Technology Services Unit (TSU) for UIDAI	22 May 2013	Up to May 2018	62.30	31.20	30.47
	Addendum-I 01 Apr 2017	Up to Mar 2020	*		
5. Establishment of Field Support Engineer PMU for UIDAI	31 Aug 2012	Up to Aug 2014	5.43	23.34	23.34
	28 Aug 2014	Up to Mar 2017	19.21		
	Addendum-I 01 Apr 2017	Up to Mar 2020	9.90		

(* The amount of contract of Addendum -I to the original Contract was met from the savings of Original Contract)
(Data Source: Copies of agreement and fund utilisation statements of UIDAI)

Thus, till the end of March 2020, UIDAI had released payment amounting to ₹204.68 Crore to the NISG out of which NISG utilised a sum of ₹201.49 Crore.

This is pertinent to mention here that UIDAI does not has its own personnel resources. While it employed Government staff on deputation to manage the works that are mostly administrative and financial in nature, the technical support resources were hired from NISG. UIDAI has not made any serious attempt to have its own dedicated staff especially in technical cadre. A notification for appointment of officers and employees was issued in recent past only (January 2020) but no selection of resources could be finalised till March 2021. It is a cause of concern that UIDAI has continuously relied on outsourced people at the cost of building their own expertise and competence in the designated areas.

Audit observations on the management of the agreements with NISG by UIDAI are in succeeding paragraphs:

4.4.2.1 State Resource Personnel (SRP) contract with National Institute of Smart Governance (NISG) extended beyond the period envisaged in the ICT guidelines

The support services to States by way of a State Resource Personnel to be provided by 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.

The services from NISG for providing skilled project management resource persons (SRP) to the states seeking for such resources was part of the financial assistance for Information & Communication Technology (ICT) infrastructure to states. As per the agreement with NISG, each SRP would be engaged at a consolidated remuneration of ₹1 Lakh per month on a one-year contract with an option for extension. NISG would be paid 15 per cent of actual manpower cost over and above the resource cost as fees for their services. All costs related to the recruitment process, such as travel costs of candidates, panel members and cost of advertisements, if any required, would be met by UIDAI at actuals. It was seen that indicative cost of SRP, which was important for exercising control over expenditure, was not estimated for the services provided by NISG.

The agreement, which was initially for a period of three years, was extended initially for three years i.e. up to November 2016 and again up to March 2017 and finally up to March 2020. Thus, an assistance that was envisaged for only one year as per the guidelines for ICT infrastructure assistance, continued for more than nine years by which time Aadhaar saturation had crossed 98 per cent of the adult population in the country or in terms of numbers, more than 125 Crore (March 2020) Aadhaar letters were issued. The agreement which was initially envisaged for only one year was repeatedly extended for years together.

UIDAI intimated (October 2020) that SRPs were deployed in the states mainly to assist state departments/ agencies for implementing their schemes with Aadhaar authentication. It justified the continued engagement of SRP for liaisoning with state/ UT departments/ agencies based on project requirement as UIDAI did not have its own office in all the states/ UTs. Eventually the SRPs were made part of PMU which could not be foreseen. It added that the cost for this service depended on progress made by the State Governments in integrating their schemes with Aadhaar and the cost of SRP was subsumed in the overall ICT assistance to the state. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

The reply is not convincing as the ICT guidelines envisaged this support only for a one-year period to be met out of ICT assistance provided to the state. The contract value was not mentioned as it depended on the requisitions placed by the respective states/ UTs. No separate approval for funding was sought apparently on the plea that the assistance for ICT was approved by the Cabinet Committee on UIDAI. It was observed that UIDAI was keen on utilizing the resources for various additional works other than the intended handholding and now the resources have been made part of PMU which clearly supports the view that SRP services were being continued for one reason or another. UIDAI had not even made any amendment related to resource persons despite releasing subsequent guidelines on ICT.

In light of the fact that Aadhaar numbers are nearing saturation limits for the country as a whole, continued assistance to the States by way of State Resource Personnel and consequential payments to NISG on this count including their service charges needs to be reviewed. The

UIDAI have to accept their own responsibility for issue of Aadhaar and limit their continued reliance on other agencies for support.

Recommendation: *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.*

4.4.2.2 Deficiencies in engagement of Field Service Engineers (FSE)

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.

UIDAI added an addendum to the PMU Agreement (August 2012) for engagement of Field Service Engineers (FSEs) team at UIDAI ROs for a period of two years with an additional indicative value of ₹5.43 Crore. On completion of the two years period (August 2014) a fresh agreement was signed for the period up to March 2017 for an indicative cost of ₹19.21 Crore which was further extended up to March 2020 at an additional cost of ₹9.90 Crore taking the total cost to ₹29.11 Crore.

We noticed that UIDAI released (May 2014) ₹1.5 Crore to NISG as advance for the last quarter of the agreement while the utilization for FSE never exceeded ₹34 Lakh in any of the previous quarters leading to an unspent balance of ₹1.28 Crore available with NISG at the end of the agreement period in August 2014. Instead of refunding the unspent balance to the Government, NISG was allowed to utilize it against a fresh agreement signed in August 2014. We also noticed that the sanctioned cost for FSE agreements was always on the higher side than the actual expenditure throughout the period as indicated in the **Table 4.5**.

Table 4.5: Details of utilization for Field Service Engineers

Agreement type & Effective Period	Amount		(₹ in Crore)
	Sanctioned	Released	Utilised
Old Addendum 31 August 2012 to 30 August 2014	5.43	3.02	1.75
Fresh Agreement 31 August 2014 to 31 March 2017	19.21	7.43	7.03
Addendum to fresh agreement 01 April 2017 to 31 March 2020	9.90 ⁴³	12.89	14.57

The above indicated deficiency in assessing the requirements for resources to be hired from NISG and in monitoring the payments made to them.

UIDAI replied (June 2020) that funds were sanctioned to NISG on the basis of estimates provided by NISG and are indicative values depicting the maximum allowable expenditure. Further, it was added that the actual expenditure depends on the actual deployment of resources. The differences in the actual expenditure and amount utilized were on account of proactive polices taken by UIDAI for regulating the CTC of outsourced resources. It was further stated that UIDAI's endeavor is to reduce costs and promote propriety in expenditure.

UIDAI further informed (October 2020) that deficiency pointed out by the audit has already been taken into cognizance and accordingly they were in a better position to assess the

⁴³ Cumulative total from 31 August 2014 is ₹29.11 Crore (₹29.10- ₹19.21= ₹9.90)

requirements of PMUs and TSUs. The estimates provided by the NISG at the time of latest extension of agreement have already been rationalized. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

The response was not convincing because there was consistent release of excess funds to a service vendor despite being aware of the fact that the actual expenditure was constantly below the funds released. This was against financial propriety and tantamount to parking of funds with agencies. Moreover, as discussed in para 4.4.2.1 above, there was continuous dependence on the outsourced personnel without any corresponding creation of expertise within the organization.

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

4.4.3 Rebate on Franking Values on dispatch of Aadhaar not availed

Deficiency in the contract with the DoP for delivery of Aadhaar Letters, deprived UIDAI of rebate on postage charges loaded in franking machines, despite UIDAI meeting the cost for franking.

Aadhaar letters, in respect of new enrolments and update or modification of resident details are dispatched and delivered to the residents in the form of laminated document through the Department of Posts (DoP) as First-Class Mail⁴⁴. UIDAI has agreements with three Print Service Providers⁴⁵ (PSPs) located at Manipal, Mumbai and Sangareddy (Telangana) for printing Aadhaar documents. As per the agreements, the PSPs were to bundle and bag Aadhaar documents on pin code basis after digitally franking them with the required postage. The postage charges are borne by UIDAI by loading the franking machines with the required funds. The bundled and bagged documents were then to be presented to the DoP for dispatch. For franking operations, PSPs were required to hold a valid commercial license issued by DoP.

DoP allowed a rebate of three *per cent* on the franked value, whenever the meter is reset i.e. credit is uploaded in the machine. Further, an additional two *per cent* rebate was also available on presentation of pin-code wise sorted mails. UIDAI released ₹648 Crore from the year 2012-13 to 2018-19 to Karnataka (Manipal), Maharashtra (Mumbai) and Andhra Pradesh/Telangana (Sangareddy) Postal Circles to replenish the postage loaded in franking machines for delivery of Aadhaar letters, of which the Circles utilized ₹603.84 Crore.

The rebate available as refund on the franked value for the above period @ three *per cent* amounted to ₹18.12 Crore and as Aadhaar documents capture pin-code and present them sorted on pincode wise to DoP, an additional two *per cent* rebate amounting to ₹12.08 Crore was also available. Thus, the total rebate available on the franked value was ₹30.19 Crore.

We observed that since UIDAI had signed Agreements with the PSPs, which did not contain any clause binding the PSPs to pass on the benefits to them, the deficient contracts deprived

⁴⁴ First class mail is a service offered by DoP with free air transmission within India for letters, post cards and letter cards.

⁴⁵ M/s Manipal Technologies Ltd, Manipal, M/s Sessaasai Business Forms (P) Limited, Mumbai and M/s K.L. Hi-tech Secure Print Limited, Sangareddy, Telangana.

UIDAI of rebate amounting to ₹30.19 Crore during the years 2012-13 to 2018-19 despite meeting the entire franking cost.

Responding to our observation, UIDAI management stated (March 2020) that the matter was referred to the DoP authorities for getting the admissible discount/rebate retrospectively and for future. However, DoP has clearly stated (July 2020) that the rebates were given to the PSPs as they were the license holder of franking machines.

UIDAI accepted (October 2020) its ignorance about the rebate being utilized by the print partners. The recommendation of audit was noted for compliance in future agreements and the matter was being followed up in accordance to the provisions of the existing contract with the print partners to pass on the rebates availed by them to UIDAI. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

Recommendation: 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.

4.4.4 Monitoring of Information & Communication Technology (ICT) Assistance to States

Improper management of Grants-in-Aid and utilizing ICT assistance for creating infrastructure.

The Cabinet Committee on UIDAI approved (September 2010) ₹ 350 Crore as assistance to the Registrars/other departments in the states and union territories for setting up Information & Communication Technology (ICT) infrastructure for making their systems UID compliant. Guidelines for regulating the assistance for ICT infrastructure was developed (September 2010) by UIDAI. Initially a normative amount of ₹ 10 Crore was approved as assistance to each state which would be released in five tranches. The quantum of each tranche was linked to the deliverables/ milestones to be achieved by states.

Under Phase-I of the assistance, Grants-in-Aid (GIA) amounting to ₹147.80 Crore was released to 38 agencies (States/ Departments/ Ministries) for ICT infrastructure during the years from 2010-11 to 2018-19. Subsequently ten more agencies were granted the ICT assistance amounting to ₹19.50 Crore during the years 2019-20 to 2020-2021.

It was seen in audit that, once the Aadhaar generation crossed the 100-Crore mark and the saturation of adult population reached 98 *per cent*, a new stream of ICT assistance was introduced (September 2016) by modifying the existing Phase-I guidelines of September 2010. The unspent amount from the normative amount of ₹10 Crore was given as additional support for procurement of enrolment kits. These kits were to be primarily used for targeted enrolments especially of new born and school going children covering their enrolment and mandatory biometric update at age five and 15 years. In addition, the kits were to be used for enrolment of adult beneficiaries of direct benefit programs who had not been earlier enrolled into the Aadhaar database. The quantum of the ICT assistance was fixed at a maximum 50 *per cent* of the total ICT assistance of the State viz., ₹5 Crore which were to be released in two tranches of ₹2.5 Crore each. Other than procurement of equipment from the assistance, the ancillary

costs like infrastructure, deployment of personnel, operating expenses, maintenance etc. were to be borne by the States.

Subsequently, (August 2018) UIDAI considered that the requirement of enrolment of newborn or children between the age 0-5 years and mandatory requirement of biometric updates at ages five & 15 years would be continuous. As such new ICT guidelines (Phase-II) were issued (September 2018) for providing assistance to State Governments, Kendriya Vidyalaya Sangathan (KVS) and Navodaya Vidyalaya Samiti (NVS) for provisioning of Aadhaar Enrolment Kits (AEKs) to be deployed dedicatedly for this category of residents. These revised guidelines also provided for assistance to BSNL to set up two AEKs in each of its Customer Service Centers to provide enrolment and update services. The total support on this account was estimated at ₹315 Crore. Financial assistance under the scheme was ₹1.5 Lakh per kit. Accordingly, UIDAI released ₹280.31 Crore to 33 agencies during 2018-19 for procurement of AEKs. A further sum of ₹0.3 Crore and ₹7.5 Crore was released to one more agency in each years of 2019-20 and 2020-21 respectively. These funds were over and above the assistance provided to states under Phase-I. The Phase II guidelines envisaged that savings if any, after procurement of two kits per block, were to be refunded.

A review of the release and utilization of the ICT assistance to various entities by UIDAI under different phases revealed the following:

- a. General Financial Rules 2005 stipulates that in respect of non-recurring Grants to an Institution or Organization, the authority sanctioning the Grants-in-Aid should insist upon a certificate in the prescribed form, of actual utilization of the Grants for the purpose for which it was sanctioned. The Institution/ Organization should submit the Utilization Certificate (UC) within twelve months of the closure of the financial year. It was seen that UIDAI had released grants of ₹147.80 Crore till 2018-19 and an additional GIA of ₹19.50 Crore in 2019-20 under Phase I, of which UCs for ₹25.34 Crore were pending from States till 31 March 2021.
- b. It was also seen that UCs for grants released as far back as February 2014 were pending submission. Seven (7) agencies, out of the 38 agencies had not even submitted partial UCs including for assistance released in the years 2013-14 and 2014-15.
- c. As per GFR conditions interest earned on unutilized funds should also be made part of the assistance. However, accrued interest earned on the ICT grants were accounted for in the UCs only by the States of Jammu & Kashmir and Himachal Pradesh. The other States neither had shown the interest earned nor had UIDAI taken review of the same.
- d. In the Phase-II ICT guidelines the entire fund was released in one lump sum to the entities instead of in installments based on submission of UCs. Audit noted that the grantee entities were erratic/ inconsistent in furnishing UCs or in refunding unspent balances. In this scenario, the possibility of the fund remaining parked or being diverted for other use cannot be ruled out. As an example, it is pointed out that the NVS Regional Office, Pune had procured 20 AEKs @ ₹1,19,068 per AEK while the assistance provided to them was @ ₹1.5 Lakh per AEK. This shows that this entity had unspent balances/ excess funds with it.

- e. The prime intention of providing ICT assistance under Phase-II guidelines was to capture the un-enrolled population belonging to the age group of less than five years. The assistance however was issued to the schools or to the State Registrars with an instruction to utilize the AEKs in Schools. As the age of school-going children is above five years the decision of funding purchase of AEKs in schools for enrolment of new-born or children between 0-5 years of age was ab-initio flawed.

Further, as mentioned in Para 3.2.3 of this Report, the issue of Baal Aadhaar without biometrics of the child, itself is not in keeping with the basic conditions of uniqueness of the identity envisaged under the Aadhaar Act. Therefore, the expenditure by way of grants for ICT assistance (Phase-II) given to States to enroll children below five years was avoidable.

UIDAI justified the release of Phase II ICT assistance in one tranche on the grounds that this was a one- time assistance as also the decision to provide AEKs to schools in view of less saturation in age groups 0-5 years and 5-18 years. They further stated (July 2020) in response that efforts were underway to obtain UCs from the nodal agencies and the non-submission of UCs have been raised with Chief Secretaries of defaulting states. It also stated that it was obtaining inputs on interest accrued on funds parked by states /UTs. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

The replies relating to UCs shows that UIDAI has not monitored utilization of the funds released as ICT assistance to States regularly and needs to take remedial action in financial management issues.

Recommendation: 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.

CHAPTER 5

Security of Aadhaar Information System

Chapter 5

Security of Aadhaar Information System

5.1 Introduction

Aadhaar authentication framework comprises of REs and ASAs. These entities collect the biometric information of the Aadhaar holder for validation purposes. Their interaction with Aadhaar number holders and UIDAI is through the digital mode. Aadhaar (Authentication) Regulation 2016 and other directions of UIDAI notified from time to time, contain instructions on the arrangements which all the entities involved in the authentication ecosystem should follow for ensuring the security of data of the residents. The regulation also specifies the responsibilities of UIDAI in monitoring e-compliance with its instructions by the ecosystem partners' viz. ASA, AUA, KUA etc.

Audit observations on compliance with provisions of the Regulation and the processes put in place by UIDAI to monitor the activities of the REs and ASAs are given in the succeeding paragraphs.

5.2 Monitoring of the activities of authentication ecosystem partners of UIDAI

Aadhaar enabled services are provided to the Aadhaar holders through the Authentication User Agencies (AUAs) or the e-KYC User Agencies (KUAs). In addition to AUAs/ KUAs, there are sub-AUAs who use Aadhaar authentication to enable their services through an existing Requesting Entity (RE). The Aadhaar Act 2016, Aadhaar (Authentication) Regulations, 2016, Aadhaar (Data Security) Regulations 2016 and other instructions/ directions issued by UIDAI govern the responsibilities and activities of these entities. Since the authentication facility uses the demographic and biometric information of the Aadhaar holder, it was imperative to put in place a strong and effective monitoring mechanism to ensure that these entities comply with the standards prescribed by UIDAI while operating and maintaining their information systems.

Audit comments on the monitoring of the activities of the authentication ecosystem partners by UIDAI are in the following paragraphs.

5.2.1 Annual Information System audit of the operations of REs and ASAs

UIDAI was neither able to derive required assurance that the entities involved in the authentication ecosystem had maintained their information systems which were compliant with the prescribed standards nor did it ensure compliance of Information Systems Audit by the appointed entities.

As per UIDAI Regulations on Authentication, REs and ASAs should ensure that their operations and systems are audited by an Information Systems Auditor duly certified by a recognized body, on an annual basis to ensure compliance with UIDAI's standards and specifications. The report of these auditors should be on request, shared with the Authority. Further, the REs will be responsible for the authentication operations of their sub-contractors and would be responsible for ensuring that the authentication related operations of such third-party entities comply with standards and specifications set by UIDAI. The operations of all the entities are to be regularly audited by approved independent audit agencies.

Important Information System (IS) audit requirements are summarized in **Table 5.1**.

Table 5.1: Information System Audit requirements

RE	ASA	UIDAI
<ul style="list-style-type: none"> • Ensure audit of its operations and systems by information systems auditor certified by a recognized body on an annual basis. • Share the audit report with the Authority upon request. • Responsible for the authentication operations and results of its sub-contract by third parties. • Ensure the authentication related operations of such third-party entities comply with Authority standards and specifications and they are regularly audited by approved independent audit agencies. 	<ul style="list-style-type: none"> • Ensure that an information systems auditor certified by a recognized body audits its operations annually. 	<ul style="list-style-type: none"> • Audit of the operations, infrastructure, systems and procedures of requesting entities, including the agencies or entities with whom they have shared a license key or the entities on whose behalf they performed authentication, and authentication Service Agencies, either by itself or through audit agencies appointed by it. • The Authority may conduct the above either by itself or through an auditor appointed by the Authority and the cost of audits shall be borne by the concerned entity.

Certified audit reports are to be submitted to the Authority upon request or at time-periods specified by the Authority. In addition to the above audits, the Regulation empowers the Authority to conduct audits of the operations and systems of such entities or persons, either by itself or through an auditor appointed by the Authority.

Thus, the Regulation mandates all the entities, involved in the authentication ecosystem, to keep their information systems in complete compliance with UIDAI standards and UIDAI in its turn should monitor the conformity through independent audits.

Further, Aadhaar (Data Security) Regulations stipulates that UIDAI should specify the security measures to be adopted by the Registrars, EAs, REs, and ASAs and should monitor compliance of security requirements through internal audits or through independent agencies. UIDAI empaneled (April 2018) M/s Deloitte Touché Tohmatsu India LLP (DTTILLP) as the agency to perform Information Security Assessment of all UIDAI Authentication Ecosystem Partners for a period of three years. As per the arrangement, the Authentication Ecosystem Partners would reach out to DTTILLP individually to initiate Information Security Assessment stipulated in the Aadhaar Authentication Regulations 2016. The agency will perform the Information Security Assessment once in a year and submit its Audit Report to the entity concerned. DTTILLP was to communicate to UIDAI at the end of every month the names of the audited partner.

Details of the audit of the REs and ASAs conducted during the five years of audit coverage are in **Table 5.2**.

Table 5.2: Details of IS audit of REs and ASAs

Year	Requesting Entities			Authentication Service Agencies		
	Agencies	Agencies whose audit was done by IS auditor	Agencies whose audit was done by UIDAI	Agencies	Agencies whose audit was done by IS auditor	Agencies whose audit was done by UIDAI
2014-15	92	NA ⁴⁶	NA	16	NA	NA
2015-16	223	2	NA	23	NA	NA
2016-17	355	121	8	27	3	1
2017-18	308	110	29	26	3	3
2018-19	204	106	8	27	9	1

Analysis of the above data showed that no REs or ASAs had their operations audited annually either by themselves through a certified Information Systems auditor or by UIDAI.

Thus, it was evident that while UIDAI regulations stipulated annual audit of the operations and systems of both REs and ASAs by Information Systems auditor, compliance was very poor. UIDAI also failed to invoke its prerogative to audit the operations, infrastructure, systems and procedures of the REs and ASAs, either by itself or through audit agencies appointed by it. As such it was unable to derive required assurance that the entities involved in the authentication ecosystem, are maintaining their information systems in complete compliance with UIDAI standards.

UIDAI informed (January 2020) that the MoUs between UIDAI and Registrars contain provisions for periodic audit of enrolment processes. It stated that the ROs carry out audit and inspection of enrolment operation of Registrars, EAs and audit of the Self-Service Update Portal (SSUP) and back end services rendered by BPO. The reply was not relevant to the observation as it deals with MoUs between UIDAI and Registrars and relates to the adherence to enrolment processes whereas, the audit observation relate to requirement for IS audits under the Authentication Regulations, of authentication related operations of the REs and ASAs.

UIDAI further intimated (October 2020) that there had been a steady increase in submission of IS Audit Reports by AUAs i.e., from about 35 per cent in 2016-17 and 2017-18 to 52 per cent in 2018-19 and that it was pursuing this aspect with the REs and sensitizing them about the significance of the audits through training sessions.

UIDAI accepted the recommendation for conducting audit of existing REs and ASAs by the auditor appointed by it within a cycle of three years subject to the present constraints posed by Covid-19 pandemic. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

Recommendation: UIDAI may ensure that each of the existing REs & ASAs are audited by UIDAI or by the Auditor appointed by it within a cycle of three years so as to provide adequate assurance about compliance to its Regulations.

⁴⁶ NA means- Data not available at UIDAI.

5.2.2 Information System Audit of Client Applications' Systems storing biometric data not ensured

UIDAI could not provide adequate assurance that REs & ASAs accessing and storing the personal information of Aadhaar holders through the Non-Registered Biometric Devices, used prior to April 2018, had been addressed by them despite issue of directions (June 2017) mandating IS audits of client systems.

UIDAI directed (January 2017) all AUAs/ASAs that with effect from 1 June 2017, authentication requests would be accepted only through “Registered Devices⁴⁷” certified by STQC (Standardization Testing and Quality Certification). An important feature of the Registered Device was that it could encapsulate activities like biometric capture, signing and encryption of biometrics etc. within it. Hence, use of Non-Registered Devices will be putting resident’s privacy at risk. UIDAI further instructed (February 2017) that all AUAs/ KUAs should ensure that the client applications used by sub-AUAs or other entities providing authentication services, are not capable of storing biometric data of the Aadhaar holder and the biometrics/PID block is encrypted at the frontend device/client level. The AUAs/ KUAs were to ensure that the client application does not replay any authentication request with stored biometric data under any circumstance and an information systems auditor(s), certified by STQC/ CERT-IN⁴⁸ should audit the client application. The compliance audit report was to be submitted to UIDAI and the sub-AUAs would access authentication services only through duly audited client applications. The AUAs/ KUAs were to ensure compliance to the directions and submit audit report along with a certificate duly signed by their Chief Executive Officer to UIDAI by 31 March 2017. Ensuring adherence to these directions was critical because use of Non-Registered Devices would be putting resident’s privacy at risk. The timeline to complete the upgrade of applications to Registered Device for AUAs/ KUAs was initially up to May 2017 and further extensions were granted till April 2018 when all the Non-Registered Devices were deactivated.

Audit was informed (July 2020) that UIDAI had not received any audit reports from any AUAs/ ASAs within the stipulated date, in compliance of their instructions of February 2017. Further, to our query on how UIDAI ensured that the front-end devices used for e-KYC were not capable of storing biometric/PID, Audit was informed that Aadhaar (Authentication) Regulation stipulates that the client application should package and encrypt the input parameters (Aadhaar number or any other identifiers provided by the requesting agency), into PID block before transmission. Therefore, it was mandatory for the requesting agencies to ensure compliance to the provisions of the Aadhaar Act and associated regulations and instructions issued by UIDAI.

⁴⁷ Public devices are biometric capture devices that provide Aadhaar compliant biometric data to the application, which, in turn encrypts the data before using for authentication purposes. A registered Device is a public device with additional features compared to public device like Device identification, eliminating use of stored biometrics and having a standardized RD service. Registered devices MUST ensure that; i.) there should be no mechanism for any external program to provide stored biometrics and get it signed and encrypted and ii.) There should be no mechanism for external program/probe to obtain device private key used for signing the biometrics.

⁴⁸ Indian Computer Emergency Response Team is a functional organization of the Ministry of Electronics and Information Technology. Apart from the objective of securing the Indian cyber space CERT-In provides Security Quality Management service also.

UIDAI further stated (October 2020) that implementing a significant technical change across the country without disrupting ongoing services required a calibrated approach and could take longer time than envisaged initially. UIDAI completed implementation of biometric registered devices for the authentication system by April 2018 thereby ensuring that the biometrics were encrypted at the device itself before sending it to client application. No RE could perform authentication using non-registered device. Thus, there was no risk of the client application storing biometric data, thereafter. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

Audit noted that during the period April 2017 to March 2018, nearly 385 Crore e-KYC transactions were undertaken by UIDAI. This was more than 76 per cent of the cumulative e-KYC transactions done since the year 2013-14. There is no assurance that many of these transactions were done using client applications that were capable of storing biometric data of residents.

Though UIDAI had claimed that it had completed implementation of biometric registered devices for the authentication system by April 2018, there was no system to confirm that the client applications used by authentication ecosystem partners for providing authentication services prior to April 2018, were not capable of storing biometric data of the Aadhaar number holders. As such, there was inadequate assurance that the risk of ASA/ AUAs/ sub-AUAs accessing and storing the personal information of Aadhaar holders through the earlier Non-Registered Devices, was addressed by UIDAI despite issuing directions in June 2017 mandating IS audits of client systems.

Recommendation: 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.

5.2.3 Security and safety of data in Aadhaar vaults

Aadhaar numbers and any connected Aadhaar data were to be stored mandatorily on a separate Aadhaar Data Vault. UIDAI could not provide reasonable assurance that the entities involved adhered to the procedures.

Security of CIDR information requires highest importance for safeguarding resident data. The confidentiality, integrity and availability of the information should be in controlled manner. UIDAI has obtained ISO 27001:2013 certification from STQC by establishment of Information Security Management System. UIDAI-CIDR has also been declared as “Protected System” by National Critical Information Infrastructure Protection Centre (NCIIPC) adding another layer of IT security assurance. However, safeguarding the Aadhaar data with the same level of security measures has to be maintained throughout the Aadhaar Ecosystem, including the authentication partners.

With a view to enhance the security level for storing the Aadhaar numbers, UIDAI mandated (July 2017) all AUAs/KUAs/Sub-AUAs and other entities who are collecting and storing the Aadhaar numbers for specific purposes, to implement Aadhaar vaults⁴⁹. UIDAI also prescribed

⁴⁹ Aadhaar Data Vault is a centralized storage for all the Aadhaar numbers collected by the AUAs/ KUAs/ Sub-AUAs/ or any other agency for specific purposes under Aadhaar Act and Regulations, 2016. It is a secure system inside the respective agency’s infrastructure accessible only on need-to-know basis.

the procedure for implementation of Aadhaar vaults and non-compliance would attract general penalty provisions of the Aadhaar Act. In addition, UIDAI could also levy financial disincentives as per the conditions provided in the AUA/ KUA agreement. Since the entities were permitted to store Aadhaar numbers along with the demographic information and photo of the Aadhaar holder, UIDAI had stipulated security and safety measures, which the entities were required to comply with while implementing Aadhaar vaults.

For verification of compliance to the above mentioned requirements and systems put in place to monitor compliance with directions by user agencies/ entities on implementing Aadhaar Data Vaults, UIDAI informed Audit (July 2020) that REs were to ensure that the objective of secure storage of Aadhaar numbers is met. UIDAI has not specified any encryption algorithm or key strength for the encryption of Aadhaar Data Vault. It further mentioned (October 2020) that Aadhaar Data Vault (ADV) was not a specific product but a process and a concept for storage of Aadhaar numbers in a secure manner and its implementation was monitored through Audit Reports submitted by the REs. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

The above position indicated that UIDAI had not established any measures /systems to confirm that the entities involved adhered to procedures and was largely dependent on Audit Reports submitted to them. They had not independently conducted any verification of compliance to the process to derive a satisfactory assurance.

Aadhaar number is a lifetime identity for Indians and is used to avail various services involving financial transactions, as such unauthorized access to Aadhaar number can be misused in many ways. Hence UIDAI may ensure the implementation of Aadhaar Data Vault by instituting periodic audit to enhance the security for the data stored by user organizations. It should deal with non-compliance strictly as per the Act and as per conditions in the agreement with AUAs/ KUAs

Recommendation: 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)

CHAPTER 6

Redressal of Customers Grievances

Chapter 6

Redressal of Customer Grievances

6.1 Introduction

UIDAI caters to the entire population of India and hence Customer Relationship Management (CRM) is an important aspect of its functioning. Aadhaar (Enrolment & Update) Regulation 2016 provides for setting up of contact centre to act as a central point for resolution of queries and grievances of residents. The contract centre should be accessible to residents through toll free number(s) and/ or e-mail. Accordingly, UIDAI has set up a grievance redressal mechanism centrally to receive grievances through the following channels:



Image courtesy: UIDAI

- a. **Through Contact Centre:** UIDAI has set up a contact centre with a toll-free number and email id being 1947 and help@uidai.gov.in respectively.
- b. **By Post:** Grievances are received at the UIDAI HQ through Post/hardcopy.

- c. **Through Public Grievance Portal of GoI:** Grievances which are lodged at the Public Grievance Portal of Government of India (pgportal.gov.in) are received from Government agencies for redressal.
- d. **Other Channels:** Sometimes grievances are received by UIDAI officials through emails, walk-in residents, phone, website, RTI etc.

The CRM partners⁵⁰ handle the grievances received at the Contact Centre (CRM Channel). The grievances received through other than CRM mode are examined and forwarded to the concerned Regional Offices/ Sections for redressal. The Regional Office/ Section concerned dispose the grievances by replying directly to the complainants under intimation to the grievance cell of UIDAI HQ. Apart from the central CRM system, the Regional Offices of UIDAI also have a system of receiving complaints/ grievances directly.

Total number of complaints registered in CRM channel during the period 2014-15 to 2018-19 is shown in **Table 6.1**.

⁵⁰ M/s Tata Business Support Services Ltd and M/s Strategic Marketing Pvt Ltd were the CRM partners till June 2018 and M/s CBSL & M/s Tech M are the current CRM partners.

Table 6.1: Year-wise and category-wise complaints received by CRM

Year	Complaints received –category wise						Complaints resolved-category wise		
	Enrolment		Update		Authentication		Enrolment	Update	Authentication
	OB	New	OB	New	OB	New	Resolved	Resolved	Resolved
2014-15	20,315	4,03,014	0	1,94,629	17	1,965	3,05,665	1,93,831	1,133
2015-16	1,17,664	6,08,553	798	9,79,695	849	20,981	7,24,133	9,79,045	21,710
2016-17	2,084	5,78,855	1,448	7,82,502	120	20,684	5,79,494	7,71,400	20,525
2017-18	1,445	10,59,107	12,550	19,51,611	279	48,041	10,57,171	19,54,305	47,002
2018-19	3,381	9,66,975	9,856	56,66,501	1,318	4,46,269	9,66,975	56,66,501	4,46,269

(Data Source: Information furnished by UIDAI)

Audit observation on the complaint redressal mechanism of UIDAI in succeeding paragraphs.

6.2 Audit Observations

6.2.1 Data on complaints and their redressal

Capture of grievances/ complaints have not been streamlined and does not display a clear picture for analysis.

UIDAI ROs apart from the centrally available CRM channels, have their own arrangements/ additional channels for receiving Grievances/complaints through phone and email. ROs also entertain complaints through Post, e-mail, phone, in person and through RTI applications. Grievances/ complaints received at the ROs of UIDAI are not captured by the CRM system and are thus, not centrally recorded and monitored. It was observed that number of grievances received at the ROs and not captured through its CRM mechanism, was significantly high. The present system does not escalate the complaints not resolved at the RO level to the next level for redressal thereby compelling the complainants to register a new complaint. As a result, UIDAI cannot track the history of complaints and assess the efficiency of the grievance redressal system.

UIDAI stated (October 2020) that up-gradation/ replacement of the existing old system was under process. The new CRM system has been designed as a single centralized system with state-of-the-art technology available for effective and comprehensive disposal and monitoring of grievances as centralized system. MeitY agreed (June 2021) with replies of UIDAI to the audit observations.

6.2.2 Grievances received through CRM

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.

An age wise pendency report is auto generated daily in respect of the cases lodged through CRM. On analysis of such pendency report for 31 December 2019, it was noticed that 58,697 grievances were pending for disposal at the various ROs/ Divisions. Of these 6,326 cases were pending for more than 30 days for redressal of which 960 cases were pending for more than 90 days.

We observed that a majority of pending cases related to Technical Support. Out of a total of 28,276 grievances relating to Technical Support 23,426 cases (82.85 *per cent*) were pending at CIDR. Further, 26,247 cases (92.82 *per cent*) had a pendency of more than one month and 202 cases were pending for more than nine months.

UIDAI stated (October 2020) that resolution/ redressal of grievances was an ongoing process and efforts had been made to bring down pendency from 58,697 cases to 27,654 cases (as on 14 September 2020). Further, pendency of 6,326 cases beyond 30 days including 960 cases beyond 90 days has been brought down to 2,609 cases and 442 cases respectively (as on 14 September 2020). There are some cases which require proper enquiry/ investigation on account of corruption and fraud, and these need adequate time for resolution. MeitY agreed (June 2021) with replies of UIDAI to the Audit Observations.

The pendency Report as on 31 March 2021, however reveals 48,000 cases were pending for resolution. Out of these total pending cases, 7,020 cases were pending for more than 30 days for redressal of which 496 cases were pending for more than 90 days.

It emerges from the above facts that the time taken for grievance redressal was high and since complaints lodged at the RO level, do not get the attention of UIDAI HQ, this compromises the effectiveness of the grievance redressal mechanism.

Recommendation: 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.



CHAPTER 7

Conclusion



Chapter 7

Conclusion

Aadhaar, the unique ID programme for India was conceived as a voluntary identity system for the residents of the country and UIDAI was formed to pilot the project with mandate to develop appropriate strategies and plans. Till March 2021, UIDAI had generated more than 129 Crore Aadhaar cards since the issue of the first Aadhaar in September 2010. The project uses a complex state-of-the-art technology for its operations and runs on one of the largest biometric databases in the world. The technology is based on biometrics to establish unique identity of the resident applicant. Authentication of the biometric identity of the resident, using Aadhaar helps the government to position it and utilise it as a major tool in its efforts to plug leakages in the delivery of government services to beneficiaries. Voluntary use of Aadhaar identity also enables other Agencies such as banks and telecom operators to verify the identity of the applicants for delivery of services to them.

The Performance Audit of UIDAI of the selected Enrolment and Authentication system revealed certain deficiencies in their functioning and delivery of services and several areas where there is scope for improvement in the functioning of the Authority.

It was seen that UIDAI had generated Aadhaar numbers with incomplete information/ documents of the holder, non-establishment of residence status of applicants with proper documents, non-review/ matching of documents of the resident with the Aadhaar database and acceptance of poor-quality biometrics resulting in multiple/ duplicate Aadhaar numbers to the same individual. Aadhaar numbers with poor quality biometrics induces authentication errors. UIDAI takes no responsibility for it and transfers the onus of updating the biometrics to the resident and also charges fees for it. Issue of Bal Aadhaar to minor children below five years was largely focused towards expanding the Aadhaar footprint, without establishing uniqueness of identity of the children. Costs to the Government for issue of these Bal Aadhaar numbers were at best avoidable

The control mechanism instituted by UIDAI to ensure that all the authentication ecosystem partners adhere to the prescribed standards in the maintenance of their IT infrastructure, needed strengthening as it was seen that Information System Audit of the operations of a large percentage of REs and ASAs was never done despite UIDAI regulations prescribing annual IS audits. Moreover, UIDAI had not ensured that the client applications used by its authentication ecosystem partners were not capable of storing the personal information of the residents, which put the privacy of residents at risk. The Authority had not ensured security and safety of data in Aadhaar vaults. They had not independently conducted any verification of compliance to the process involved.

UIDAI's compliance to its own Regulations were found wanting due to belated levy of fees for authentication services, which deprived the government of its due revenues upto March 2019, though the Aadhaar database was used extensively by Banks and Mobile operators for authentication of identity of the applicants. The fees chargeable were determined thereafter.

There were flaws in the management of various contracts entered into by UIDAI. The decision to waive off penalties for biometric solution providers was not in the interest of the Authority giving undue advantage to the solution providers, sending out an incorrect message of acceptance of poor quality of biometrics captured by them.

The logistics arrangements with the Department of Posts were not effective for ensuring actual delivery of Aadhaar letters to the correct addressee pointing to the need for fine-tuning the last mile management of enrolment process for improving the efficiency of the Aadhaar delivery mechanism.

The grievance redressal system at the UIDAI Hqrs and Regional Offices was ineffective and was plagued with delays in redressal of grievances.

Observations emanating out of the Performance Audit show that UIDAI was successful in issuing a large majority of residents with an identity document, based on unique identity established through biometrics. This has undoubtedly helped Government as well as private Agencies in establishing identity of the residents before delivery of services.

The issue of Aadhaar to residents is an ongoing project and the UIDAI would do well to proactively accept its role and responsibility bestowed upon them by the Government by various statutory enactments and reduce its continued dependence on outsourced Agencies and instead partner with State Governments for the enrolment process.


The audit observations and Recommendations could assist the UIDAI Management to identify areas that require fine-tuning, improvements in its functions, reviewing the existing systems for ensuring compliance to its own regulations and securing the information in the Aadhaar database maintained by them.

New Delhi
Dated: 03 January 2022


(MANISH KUMAR)
Director General of Audit
Finance & Communication

Countersigned

New Delhi
Dated: 31 January 2022


(GIRISH CHANDRA MURMU)
Comptroller and Auditor General of India



Appendices and Abbreviations

Appendix-I

Provisions of Aadhaar Act, 2016

(Refer Paragraph no. 1.4)

Sl. No.	Section no. of Aadhaar Act 2016	Act particulars	Whether regulation exists?	Regulation Particulars	Ecosystem
1	2(aa)*	“Aadhaar ecosystem” includes enrolling agencies, Registrars, requesting entities, offline verification-seeking entities and any other entity or group of entities as may be specified by regulations;	Partial	Aadhaar (Enrolment and Update) Regulations 2016 & Aadhaar (Authentication) Regulation 2016 No amendments in Regulation for offline verification	Enrolment & Update (E&U) and Authentication
2	2(pa)*	“Offline verification” means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations	No	No amendments in Regulation for offline verification	Authentication
3	2(g) 54(2)(a)	“biometric information” means photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by regulations	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016)	E&U
4	2(j)	“core biometric information” means finger print, Iris scan, or such other biological attribute of an individual as may be specified by regulations	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016)	E&U
5	2(k) 54(2)(a)	“demographic information” includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016)	E&U
6	2(m) 54(2)(a)	“enrolment” means the process, as may be specified by regulations, to collect demographic and biometric information from individuals by the enrolling agencies for the purpose of issuing Aadhaar numbers to such individuals under this Act	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016)	E&U

Sl. No.	Section no. of Aadhaar Act 2016	Act particulars	Whether regulation exists?	Regulation Particulars	Ecosystem
7	3(2)	The enrolling agency shall, at the time of enrolment, inform the individual undergoing enrolment of the following details in such manner as may be specified by regulations, namely: — (a) the manner in which the information shall be used	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016)	E&U
8	3(3) 54(2)(b)	On receipt of the demographic information and biometric information under sub-section (1), the Authority shall, after verifying the information, in such manner as may be specified by regulations, issue an Aadhaar number to such individual	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016) [Clause 10&13(2)] & 6 th Amendments	E&U
9	3(4) * 54(2) (be)	The Aadhaar number issued to an individual under sub-section (3) shall be a twelve-digit identification number and any alternative virtual identity as an alternative to the actual Aadhaar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations.	Yes	The term Aadhaar number to include virtual id also	Aadhaar
10	3A (2) * 54(2) (bb)	A child who is an Aadhaar number holder may, within a period of six months of attaining the eighteen years of age, make an application to the Authority for cancellation of his Aadhaar number, in such manner as may be specified by regulations and the Authority shall cancel his Aadhaar number	Yes	Aadhaar (Enrolment and Update) (eighth Amendment) Regulations 2020. (3 of 2020 dated 30th June 2020)	E & U
11	4(3) 54(2)(c)	An Aadhaar number, in physical or electronic form subject to authentication and other conditions, as may be specified by regulations, may be accepted as proof of identity of the Aadhaar number holder for any purpose <i>*Substituted as</i> <i>Every Aadhaar number holder to establish his identity, may voluntarily use his Aadhaar number in physical or electronic form by way of authentication or offline verification, or in such other form as may be notified, in such manner as may be specified by regulations</i>	Yes	Aadhaar (Authentication) Regulation 2016 (No. 03 of 2016 (12/09/16)) No amendments in Regulation for offline verification	Authentication
12	4(4) * 54(2) (ca)	<i>An entity may be allowed to perform authentication, if the Authority is satisfied that the requesting entity is— (a) compliant with such standards of privacy and security as may be specified by regulations;</i>	Yes	Aadhaar (Authentication) Regulation 2016 (No. 03 of 2016 (12/09/16))	Authentication

Sl. No.	Section no. of Aadhaar Act 2016	Act particulars	Whether regulation exists?	Regulation Particulars	Ecosystem
13	4(5) * 54(2) (cob)	<i>The Authority may, by regulations, decide whether a requesting entity shall be permitted the use of the actual Aadhaar number during authentication or only an alternative virtual identity</i>	Yes	No regulation for use of only an alternate virtual number. However, use of Aadhaar no allowed under authentication regulations & Aadhaar no include virtual no (as per amendments)	Authentication
14	5 54(2)(d)	The Authority shall take special measures to issue Aadhaar number to women, children, senior citizens, persons with disability, unskilled and unorganized workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and such other categories of individuals as may be specified by regulations	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016)	E&U
15	6 54(2)(e)	The Authority may require Aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations, so as to ensure continued accuracy of their information in the Central Identities Data Repository.	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016) only bio of children	E&U
16	8(1) 54(2)(f)	The Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder submitted by any requesting entity, in relation to his biometric information or demographic information, subject to such conditions and on payment of such fees and in such manner as may be specified by regulations	Yes	Aadhaar (Authentication) Regulation 2016 (No. 03 of 2016) (Clause 12(7))	Authentication
17	8(2)(a) 54(2)(f) *	A requesting entity shall—unless otherwise provided in this Act, obtain the consent of an individual <i>or in the case of a child obtain the consent of his parent or guardian</i> before collecting his identity information for the purposes of authentication in such manner as may be specified by regulations	Yes	Aadhaar (Authentication) Regulation 2016 (No. 03 of 2016) (Clause 16)	Authentication

Sl. No.	Section no. of Aadhaar Act 2016	Act particulars	Whether regulation exists?	Regulation Particulars	Ecosystem
18	8(2)(b) * 54(2) (fa)	<i>“Provided that the requesting entity shall, in case of failure to authenticate due to illness, injury or infirmity owing to old age or otherwise or any technical or other reasons, provide such alternate and viable means of identification of the individual, as may be specified by regulations</i>	No	No amendment in regulations found to provide for alternate and viable means of identification of an individual	Authentication
19	8(3) 54(2)(f)	A requesting entity shall inform, in such manner as may be specified by regulations, the individual submitting his identity information for authentication, the following details with respect to authentication, namely:— (a) the nature of information that may be shared upon authentication; (b) the uses to which the information received during authentication may be put by the requesting entity; and (c) alternatives to submission of identity information to the requesting entity	Yes	Aadhaar (Authentication) Regulation 2016 (No. 03 of 2016)	Authentication
20	8A(2)(a) *	<i>Every offline verification-seeking entity shall, — (a) before performing offline verification, obtain the consent of an individual, or in the case of a child, his parent or guardian, in such manner as may be specified by regulations</i>	Partial	No amendments in Regulation for offline verification however in other cases it is available in Authentication Regulation	Authentication
21	8A (3) *	<i>An offline verification-seeking entity shall inform the individual undergoing offline verification, or in the case of a child, his parent or guardian, the following details with respect to offline verification, in such manner as may be specified by regulations,</i>	Partial	No amendments in Regulation for offline verification however in other cases it is available in Authentication Regulation	Authentication
22	8A(4)(c) *	<i>No offline verification-seeking entity shall— (c) take any action contrary to any obligation on it as may be specified by regulations.</i>	No	No amendments in Regulation for offline verification	Authentication
23	10 54(2)(g)	The Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations.	Yes	Aadhaar (Data Security) Regulations, 2016 (No. 04 of 2016)	IS /Tech
24	18(2)(e)	The chief executive officer shall be the legal representative of the Authority and shall be responsible for— (e) performing such other functions, or exercising such other powers, as may be specified by regulations	Yes	UIDAI (Transaction of Business at Meetings of the Authority) Regulations, 2016 (No. 1 of 2016)	Administration

Sl. No.	Section no. of Aadhaar Act 2016	Act particulars	Whether regulation exists?	Regulation Particulars	Ecosystem
30	23(2)(g) 54(2)(l)	Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include— (g) omitting and deactivating of an Aadhaar number and information relating thereto in such manner as may be specified by regulations	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016) (Clause 27, 28)	E&U
31	23(2)(i) 54(2)(n)	Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include—(i) specifying, by regulations, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016) and 2 nd & 4 th Amendments	E&U
32	23(2)(k) 54(2)(o)	Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include—sharing, in such manner as may be specified by regulations, the information of Aadhaar number holders, subject to the provisions of this Act	Yes	Aadhaar (Sharing of Information) Regulations, 2016 (No. 05 of 2016)	IS
33	23(2)(m) 54(2)(p)	Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include— (m) specifying, by regulations, various processes relating to data management, security protocols and other technology safeguards under this Act	Yes	Aadhaar (Data Security) Regulations, 2016 (No. 04 of 2016)	IS
34	23(2)(n) 54(2)(q)	Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include— (n) specifying, by regulations, the conditions and procedures for issuance of new Aadhaar number to existing Aadhaar number holder	No	<i>The enrolment and update division of UIDAI informed that the purpose of the provision in the Act was not known to them</i>	E&U
35	23(2)(o) 54(2)(r)	Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include—(o) levying and collecting the fees or authorising the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act in such manner as may be specified by regulations	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016)	E&U
36	23(2)(r) 54(2)(s)	Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include—(r) evolving of, and specifying, by regulations, policies and practices for Registrars, enrolling agencies and other service providers	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016)-	E&U

Functioning of Unique Identification Authority of India

Sl. No.	Section no. of Aadhaar Act 2016	Act particulars	Whether regulation exists?	Regulation Particulars	Ecosystem
37	28(3)	The Authority shall take all necessary measures to ensure that the information in the possession or control of the Authority, including information stored in the Central Identities Data Repository, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage	Yes	Aadhaar (Data Security) Regulations, 2016 (No. 04 of 2016)	IS
38	28(5) * 54(2)(t)	Provided that an Aadhaar number holder may request the Authority to provide access to his identity information excluding his core biometric information in such manner as may be specified by regulations	Yes	Aadhaar (Authentication) Regulation 2016 (No. 03 of 2016) [clause 28]	Authentication
39	29(2) 54(2)(u)	The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations.	Yes	Aadhaar (Sharing of Information) Regulations, 2016 (No. 05 of 2016)	IS
40	29(4)	No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.	Yes	Aadhaar (Sharing of Information) Regulations, 2016 (No. 05 of 2016) [Clause 6]	IS
41	31(1) 54(2)(v)	In case any demographic information of an Aadhaar number holder is found incorrect or changes subsequently, the Aadhaar number holder shall request the Authority to alter such demographic information in his record in the Central Identities Data Repository in such manner as may be specified by regulations	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016) and Amendments (7 th , 6 th)	E&U
42	31(2) 54(2)(v)	In case any biometric information of Aadhaar number holder is lost or changes subsequently for any reason, the Aadhaar number holder shall request the Authority to make necessary alteration in his record in the Central Identities Data Repository in such manner as may be specified by regulations.	Yes	Aadhaar (Enrolment and Update) Regulations 2016 (No. 02 of 2016) and Amendments (7 th , 6 th)	E&U
43	31(4)	No identity information in the Central Identities Data Repository shall be altered except in the manner provided in this Act or regulations made in this behalf	Partial	No amendments in Authentication Regulations (cl 26) found to include the change.	Authentication

Sl. No.	Section no. of Aadhaar Act 2016	Act particulars	Whether regulation exists?	Regulation Particulars	Ecosystem
44	32 (1) 54(2)(w)	The Authority shall maintain authentication records in such manner and for such period as may be specified by regulations	Yes	Aadhaar (Authentication) Regulation 2016 (No. 03 of 2016)	Authentication
45	32 (2) 54(2)(w)	Every Aadhaar number holder shall be entitled to obtain his authentication record in such manner as may be specified by regulations	Yes	Aadhaar (Authentication) Regulation 2016 (No. 03 of 2016)	Authentication
46	37	Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorised under this Act or regulations made there under or in contravention of any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one Lakh rupees or with both.	Yes	<i>Part of the act and covered in Authentication Regulations, Data Sharing Regulations and Sharing of Information Regulations</i>	IS
47	54(2)(x)	any other matter which is required to be, or may be, specified, or in respect of which provision is to be or may be made by regulations	Yes	Aadhaar (Enrolment and Update) Regulations 2016 Regulation no 10(2) and 7 th Amendments	E & U

Appendix-I shows the requirements of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, (“**Aadhaar Act 2016**”) including **the Aadhaar and Other Laws (Amendment) Act** (dated 23 July 2019)⁵¹ and corresponding provisions in the various Regulations issued by the UIDAI as on 31 March 2020.

* denotes the requirement of regulations as per the amendment to the Aadhaar Act 2016 by **The Aadhaar and Other Laws (Amendment) Ordinance 2019** (No. 9 of 2019) (dated 02 March 2019) which become **the Aadhaar and Other Laws (Amendment) Act** (dated 23 July 2019)

⁵¹ The Aadhaar and Other Laws (Amendment) Ordinance 2019 (No.9 of 2019) (dated 02 March 2019)

Annexure-I

(Refer Paragraph no. 4.3.1)

Based on the decided sample size six out of six contracts having value of ₹100 Crore and above and seven out of twenty-six contracts having value less than ₹100 Crore were selected for scrutiny. The selected list of contracts is furnished below:

A. Contracts > ₹100 Crores entered by UIDAI					
Sl. No.	Particulars	Name of the firm	Period	Value (₹ in Crore)	Remarks
I	II	III	IV	V	VI
1	Agreement with Data Centre Development Agency (DCDA), Bengaluru	M/s Wipro Ltd,	06-12-2012 to 05-12-2017	116.06	The file related to AMC part was only provided for scrutiny. The file related to selection process of the vendor was not made available. Since the contract involved technical issues, the same was out of the scope of the Audit for scrutiny.
2	Agreement with DCDA, Manesar			117.18	
3	Managed Service Provider (MSP)	M/s HCL Infosystems Ltd	20-6-2012 to 19-6-2019	1,978.62	The tender/contract files related to MSP was denied citing confidentiality. The file related to invoices and payments were subsequently provided for scrutiny. The file related to selection process of the vendor was not made available. The same was also out of audit coverage period. Further the detailed scrutiny was not done as the issues of technical nature was kept out of scope of audit. The observations made by audit is presented in the Chapter-4 of the Report.
	A 1 Cost of 35 Cells - Value-1			585.91	
	A 2 Cost of Non-Cell Comp. - Value-2			325.49	
	B 1 Staff cost for managed service - Value-3			347.38	
	B 2 AMC for Cell comp - Value-3			210.85	
	B 3 AMC for Non-Cell comp - Value-3			144.86	
	B 4 N/work connectivity cost - Value-3			21.22	
	C Software development - Value-4			27.91	
	D Cost of Biometric solution - Value-5			315.00	
4	Aadhaar Document Management System (ADMS)	M/s Hewlett-Packard India Sales Pvt. Ltd.	7-06-2011 to 6-06-2016	327.98	The management did not produce the file for audit scrutiny during the presence of audit team in the premises. Observations were made based on the reports of ROs and information collected through replied memos. However, they agreed to provide the same later on.

5	Professionals Recruitment (NISG)	M/s National Institute of Smart Governance (NISG), Hyderabad	up to 31-03-2020		The files were furnished to audit for scrutiny. The observations made on the contracts related to supply of executives by NISG has been brought out in the Report. The finance cost of SRP was to be met from the ICT assistance paid to the States.
	Field Support Engineers (FSE)		30-11-2009	5.43	
	Project Management Unit (PMU)		30-11-2009 & 18-12-2013	40.68	
	Aadhaar Enabled Applications Group (AEAG)		18-04-2011	28.50	
	Project Management Resources (SRP)		22-11-2013		
	Technology Services Unit (TSU)		22-05-2013	62.30	
6	Hiring of accommodation on rent at Jeevan Bharti Building, Connaught Circus, New Delhi	M/s Life Insurance Corporation of India (LIC)	01-11-2009 to 31-10-2014 & 01-11-2014 to 31-10-2019		No file was made available to PA Team during their presence at the premises. However, the files were subsequently provided to the Compliance Audit Team/ LAP during December 2020.

B. Contracts < ₹ 100 Crores entered by UIDAI					
Sl. No.	Particulars	Name of the firm	Period	Value (₹ in Crore)	Remarks
I	II	III	IV	V	VI
1	Governance Risk Compliance and Performance (GRCP) Service Provider	M/s Price Water House - Cooper	06-10-2015 to 05-10-2018	17.53	The file was not provided to audit. GRCP reports on for few periods shared under their watch and ward in separate chamber.
2	Processing of update requests of the residents, back-end work of self-service update, etc.	M/s Karvy Data Management Services Ltd.	28-05-2017 to 02-07-2018	16.52	The RFP file was provided but nothing substantial worth reporting was found.
3	Operating of Contact Centre Services of UIDAI	M/s TATA Business Support Services Ltd.	06-04-2016 to 05-04-2017 & 06-04-2017 to 05-04-2018	24.93	The files related to selection process and correspondences was made available to audit but nothing substantial worth reporting was found.
4	Augmentation of outbound SMS capabilities at UIDAI HQrs	M/s Value First Digital Media Pvt. Ltd.	23-03-2013 to 22-03-2016 & 23-03-2016 to 22-03-2017	4.86	The RFP file was provided but nothing substantial worth reporting was found.

Functioning of Unique Identification Authority of India

5	Printing and Franking of Aadhaar documents	M/s Manipal Technologies Ltd., Manipal	01-07-2013 to 31-10-2016 & 15-12-2016 to 14-12-2018	74.29 50.47	The RFP files was provided. The invoices along with GRCP reports on meeting the SLA parameters and sanction for payments were provided. The observations emanating from it has been brought out in the report.
6	Printing and Franking of Aadhaar documents	M/s Sessaasai Business Forms (P) Ltd., Wadala, Mumbai	21-06-2013 to 21-10-2016 & 20-12-2016 to 19-12-2018	44.57 25.24	
7	De-duplication of Data Monitoring Services	M/s HCL Infosystems Ltd.	01-11-2017 to 31-10-2018	22.63	The files were not supplied.

Abbreviations

List	Description
ABIS	Automatic Biometric Identification Systems
ADMS	Aadhaar Document Management System
AEAG	Aadhaar Enabled Applications Group
AEK	Aadhaar Enrolment Kit
ASA	Authentication Service Agency
ASK	Aadhaar Seva Kendra
AUA	Authentication User Agency
BSP	Biometric Service Provider
CEO	Chief Executive Officer
CERT-IN	Indian Computer Emergency Response Team
CIDR	Central Identities Data Repository
CRM	Customer Relationship Management
DC	Data Center
DDG	Deputy Director General
DEITY	Department of Electronics & Information Technology
DMS	Document Management System
DoB	Date of Birth
DoP	Department of Posts
EA	Enrolment Agency
EFC	Expenditure Finance Committee
EID	Enrolment ID
e-KYC	Electronic Know Your Customer
FMR	False Match Rate
FNIRA	False Negative Identification Rate for Anomalous matches
FNMR	False Non-Match Rate
FPIR	False Positive Identification Rate
FSE	Field Service Engineer
GFR	General Financial Rules
GRCP	Governance Risk Compliance and Performance
HQ	Head Quarters
ICT	Information & Communication Technology
ID	Identity Document
IS	Information Security
IT	Information Technology
KUA	e-KYC User Agency
LD	Liquidated Damages
LLP	Limited Liability Partnership
MDD	Manual De-duplication

MEITY	Ministry of Communications and Information Technology
MoU	Memorandum of Understanding
MSP	Managed Service Provider
NISG	National Institute for Smart Governance
NVS	Navodaya Vidyalaya Samiti
OAE	Other Administrative Expense
OAR	Order Aadhaar Reprint
OTP	One Time Pin
PAN	Permanent Account Number
PII	Personally, Identifiable Information
PID	Personal Identity Data
PMU	Project Management Unit
PoA	Proof of Address
PoI	Proof of Identity
PoR	Proof of Relationship
PSP	Print Service Provider
QC	Quality Check
RE	Requesting Entity
RO	Regional Office
RTI	Right To Information
SLA	Service Level Agreement
SRP	State Resource Person
STQC	Standardization Testing and Quality Certification
TSP	Telecom Service Providers
TSU	Technology Service Unit
UC	Utilization Certificate
UID	Unique Identification
UIDAI	Unique Identification Authority of India
UT	Union Territories

© COMPTROLLER AND
AUDITOR GENERAL OF INDIA
www.cag.gov.in

UPDATE YOUR CHILD'S BIOMETRICS AT AGE OF 5 & 15 YEARS

These Biometric Updates are **FREE** and can be done only at an Aadhaar Kendra.

Aadhaar Enrollment & Update facilities are available at East Branches & Post Offices only.

Learn an Aadhaar Kendra is **सहयोगी केंद्र**

Unique Identification Authority of India
Department of India

AADHAAR
सहयोगी केंद्र

Facebook, YouTube, Instagram, Twitter, LinkedIn, WhatsApp, Telegram, Messenger, Email, Website

Did not get AADHAAR by Post or lost it?

ORDER AADHAAR REPRINT in just a minute to get updated copy of Aadhaar via **Speed Post**

To order a Reprint, visit **www.uidai.gov.in**

The service is available for a nominal charge of ₹25 including cost of Speed Post.

Unique Identification Authority of India
Department of India

AADHAAR
सहयोगी केंद्र

Facebook, YouTube, Instagram, Twitter, LinkedIn, WhatsApp, Telegram, Messenger, Email, Website

UPDATE YOUR ADDRESS IN AADHAAR, ONLINE

To know more, visit **www.uidai.gov.in**

UIDAI services can be updated online. For any other updates, visit an Aadhaar Kendra.

Remember to **Mumkin Hai**

Unique Identification Authority of India
Department of India

AADHAAR
सहयोगी केंद्र

Facebook, YouTube, Instagram, Twitter, LinkedIn, WhatsApp, Telegram, Messenger, Email, Website