RFP No- IFCI/2024-25/IT-Advisory/002 **Dated-18/02/2025**

IFCI
LIMITED
आई एफ सी आई लिमिटेड
(A Government of India Undertaking)
(भारत सरकार का उपकम)

Request for Proposal (**RFP)**

For

Appointment of Consultant for UIDAI’s Compliances

To be submitted before
28/02/2025 – 5:00 PM

Addressed To
General Manage (IT-Advisory)
IFCI Limited
IFCI Tower, 61 Nehru Place
New Delhi – 110019

Disclaimer

This RFP is neither an agreement nor an offer and is only an invitation by IFCI to the interested parties for submission of bids. The purpose of this RFP is to provide the Vendor with information to assist in the formulation of their proposals.

This RFP does not claim to contain all the information each Vendor may require. Vendor(s) should conduct its own investigations and analysis and should check the accuracy, reliability, and completeness of the information in this RFP and wherever necessary, may obtain independent advice. IFCI makes no representation or warranty and shall incur no liability under any law, statute, rules, or regulations as to the accuracy, reliability, or completeness of this RFP. IFCI may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

This document is meant to provide information only and with an express understanding that recipients will use it only for the purposes set out above. It does not purport to be all inclusive or contain all the information about the requirement or form the basis of any contract. No representation or warranty, expressed or implied, is made regarding reliability, accuracy, or the completeness of any of the information contained herein. There may be deviation or change in any of the information mentioned herein.

While this document has been prepared in good faith, neither IFCI, nor any of their officers make any representation or warranty or shall have any responsibility or liability whatsoever in respect of any statements or omissions here from. Any liability is accordingly and expressly disclaimed by IFCI and any of their officers or subscribers, even if any loss or damage is caused by any act or omission on the part of IFCI or any of their officers or subscribers, whether negligent or otherwise.

By acceptance of this document, the recipient agrees that any information herewith will be superseded by any subsequent written information on the same subject made available to the recipient by or on behalf of IFCI. IFCI and any of their respective officers or subscribers undertake no obligation, among others, to provide the recipient with access to any additional information or to update this document or to correct any inaccuracies therein which may become apparent, and they reserve the right, at any time and without advance notice, to change the procedure for the selection of or any part of the interest or terminate negotiations or the due diligence process prior to the signing of any binding agreement.

This document has not been filed, registered, or approved in any Court of Competent jurisdiction.
Recipients of this document should inform themselves of and observe any applicable legal requirements.

****

1. Introduction

1.1 The **PM Electric Drive Revolution in Innovative Vehicle Enhancement (PM E-DRIVE) Scheme** is a landmark initiative by the Government of India aimed at addressing the pressing need for sustainable and environmentally friendly mobility solutions. Launched with a total budgetary outlay of ₹10,900 crores, the scheme emphasizes the fast-tracked adoption of electric vehicles (EVs) across various categories such as two-wheelers, three- wheelers, buses, trucks, and other emerging EV types. The scheme's timeline runs from 1st October 2024 to 31st March 2026 (with deliverable extending further), marking a crucial phase in India's transition towards electric mobility.

1.2 The government's intent with PM E-DRIVE is to drive significant reductions in the nation's carbon footprint by promoting EV adoption, while simultaneously fostering local EV manufacturing, improving energy efficiency, and enhancing air quality in urban areas. This ambitious scheme sets India on a path to becoming a global leader in the EV sector by addressing both consumer demand and the supply side through innovation, incentives, and infrastructure development.

2. Eligibility of Bidder/firm/External Agency

2.1 This is a limited tender and is being issued to perspective bidder / service provider.

2.2 Any bidder/ firm/ External Agency, which has been black-listed or debarred by the Government or its organizations/agencies, for executing such assignments will not be considered for appointment.

2.3 This tender is being issued to only vendors/bidders empaneled with IFCI and CERTIN Authorized Auditors.

3. Duration of Contract

3.1 The contract will be assigned for a period of One (01) months, which may be extended further, subject to the satisfactory performance of the service provider on the same terms & conditions and the requirements of IFCI.

4. Criteria for Evaluation

4.1 The bidder will be selected purely as per Least Cost Method (L1) as per the financial bid format

5. Security:

5.1 The Service Provider shall not disclose the details of this Contract with any third party at any point of time unless required by law. That the Service Provider and its employees/professionals/personnel are only authorized to access the information shared and or collected under this project and no third party shall have any access to any information either written or oral without the written consent of IFCI. The Service Provider shall ensure that all the data collected and processed and information received under this project or during the execution of this project and or required to be shared with IFCI, by the Service Provider under this Contract shall be in totally secure mode and that the Service Provider shall take all necessary steps to prohibit any unauthorized sharing/publishing of data in the public domain or with any other party or person who is not authorized by IFCI to receive such information and or data. That the Service Provider shall ensure that all the data collected, and information received under this contract shall be used only for the purpose of execution of this contract and once the purpose of this contract is fulfilled then all the papers, drawings, notes, memoranda, manuals, specifications, designs, devices, documents, diskettes, CD's, DVD's. Tapes, Trade Secrets and any other material on any media containing or disclosing any confidential or proprietary technical or business information shared during the course of execution of this contract shall be returned to IFCI.

6. Key Information to Bidders:

Sl. No.	Particulars	Details
1	RFP No	IFCI/2024-25/IT-Advisory/002
3	Tender Name	RFP for Appointment of Consultant for UIDAI's Compliances for PM EDRIVE Portal of MHI
4	Date of Issue	18/02/2025
5	Pre-Bid Meeting	24/02/2025 2:00pm
6	Last date & time of submission of financials	28/02/2025 12:00pm
7	Date & time of opening of the bid	03/03/2025 12:00pm
8	Mode of Submission of Financial Bid	The financial bid must be provided in password protected PDF format at the mentioned email address. The password must be shared once asked from IFCI officials on bid opening date and time.
8.	Name of the contact person for any clarification	Mr. Shivam Kumar Yadav - 011-41732167 Ms. Sandhya Singh -011 41732228
9	e-mail Address	itadvisory.services@ifciltd.com
10	Validity of Proposal	15 days from the date of bid submission.

SCOPE OF WORK

The **PM Electric Drive Revolution in Innovative Vehicle Enhancement (PM E- DRIVE) Scheme** is a landmark initiative by the Government of India aimed at addressing the pressing need for sustainable and environmentally friendly mobility solutions. Launched with a total budgetary outlay of ₹10,900 crores, the scheme emphasizes the fast-tracked adoption of electric vehicles (EVs) across various categories such as two-wheelers, three- wheelers, buses, trucks, and other emerging EV types. The scheme's timeline runs from 1st October 2024 to 31st March 2026 (with deliverable extending further), marking a crucial phase in India's transition towards electric mobility.

The scheme requires e-KYC to be carried out for which the ministry has been appointed as a Sub-KUA/AUA. In terms of the requirements stipulated by UIDAI, certain compliances need to be adhered to.

IFCI has been appointed as a project management agency (PMA) for the above scheme which entails compliance requirements to be addressed by the appointed PMA.

The Scope of work would involve compliance requirements to be adhered to for being a Sub-AUA/KUA as per requirements of UIDAI.

Reporting & Key Deliverable Requirement:

Detailed policy framework at the end of each requirement mentioned above, providing observations, evidence and document details.

Payment Terms:

100% payment will be made after successful acceptance of the compliance report and policies by IFCI, MHI and UIDAI as mentioned in Annexure-1

Financial Bid Format

S No	Item Description/Services	Total Cost (In INR – Inclusive of all taxes)
1	Completion of all tasks as defined in the document – Annexure-1	

Annexure-1

UIDAI's Compliances

Sr. No.	Control No.	Short Title	Control Description
1	3	Information security policy and procedure	Sub AUA/ Sub KUA should have an information security policy and information security procedures in accordance with industry leading standards, such as ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework and ISO27701 (PIMS). The entity's information security policy should also address the security aspects of Aadhaar, as provided under the Aadhaar Act, regulations and specifications.
2	6	Risk assessment	Sub AUA/ Sub KUA should implement process and procedure to perform periodic (at least annual) information security risk assessment of its ICT infrastructure supporting the authentication application. Further, entity should also perform risk assessment of its third party suppliers / vendors having access to the Aadhaar application and the data of Aadhaar number holders. Security risks should be documented and reviewed periodically by Security Officers / CISO / those in charge of the security governance of the Sub-AUAs and Sub-KUAs.
3	7	Third party information security policy	Sub AUA/ Sub KUA should ensure that it has a third party information security policy that lays down the security controls and compliances that its third party vendors, suppliers, ICT service providers and ICT support vendors (e.g., third party / outsource application developers, infrastructure support vendors, data centre hosting agency, cloud service providers etc.) are obligated to adhere to.

4	8	Annual information security audit by CERT-In- empaneled auditor	Sub AUA/ Sub KUA should ensure that its operations and systems are audited by an information systems auditor certified by a recognized body on an annual basis and on need basis to ensure compliance with UIDAI's standards and specifications. The audit report should be shared with UIDAI. If any non-compliance is found as a result of the audit, Sub AUA/ Sub KUA should— (a) determine the causes of the non- compliance; (b) evaluate the need for actions to avoid recurrence of the same; (c) determine and enforce the implementation of corrective and preventive actions; and (d) review the corrective actions taken. The annual audit should cover all security controls applicable under the Aadhaar (Data Security) Regulations, 2016.
5	9	Data protection policy	Sub AUA/ Sub KUA should establish a data protection policy addressing, inter alia, data protection related aspects under— (a) the Aadhaar Act, the regulations made thereunder and the standards and specifications issued by UIDAI from time to time; (b) the Information Technology Act, 2000 ("IT Act"); and (c) till the coming into force of the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") and, on and from the date of coming into force of the DPDP Act, the said Act and the rules made thereunder. Such policy should be published on the website of Sub AUA/ Sub KUA and the URL for the same should be mentioned.
6	14	Consent communication in local language	The Sub AUA/ Sub KUA should ensure that the consent information is communicated in local language. The Sub AUA/ Sub KUA should also ensure that, on and from the date of coming into force of sub-section (3) of section 5 of the DPDP Act, the Aadhaar number holder has the option to access the contents of the notice referred to in sub-sections (1) and (2) of the said section and the request for consent referred to in sub-section (3) of section 6in English or any language specified in the Eighth Schedule to the Constitution.
7	15	Communication of consent related information to persons with visual/hearing disability	The Sub AUA/ Sub KUA should make provisions for communication of consent related information to persons with visual/hearing disability in an appropriate manner.
8	23	Security hardening of assets	Sub AUA/ Sub KUA should ensure all the end-point devices and assets are used only after hardening to reduce/eliminate the attack vector and condense the system attack surface.

9	25	Maintenance of software inventory	Sub AUA/ Sub KUA should ensure that it uses only licensed software for Aadhaar authentication related infrastructure environment. Record of all software licenses should be kept and updated regularly.
10	26	Asset disposal procedure	Sub AUA/ Sub KUA should define a procedure for disposal of the information assets being used for authentication operations. Information systems and documents containing Aadhaar related information should be disposed of securely.
11	27	Asset repair procedure and asset movement logs	Sub AUA/ Sub KUA should, before consigning any asset for repair, sanitize the same to ensure that it does not contain any Aadhaar related data. A register to log the movement of all the assets consigned outside should be maintained.
12	28	Asset repair procedure	Sub AUA/ Sub KUA should, in case of in-house repair of assets, document the details of the original equipment manufacturer (OEM) and maintain the logs of the assets being repaired.
13	29	Background verification and signing of confidentiality agreement	Sub AUA/ Sub KUA should conduct a background check and sign a confidentiality agreement / non-disclosure agreement (NDA) with all personnel/agency handling Aadhaar related information. Access to authentication infrastructure should not be granted before signing NDA and completion of background verification (BGV) for personnel.
14	31	Training and awareness	Sub AUA/ Sub KUA should ensure that MPOC, TPOC and their supporting teams that manage and maintain the authentication application and its underlying infrastructure, are aware of Aadhaar security requirements.
15	32	Operator qualification	Sub AUA/ Sub KUA should ensure that the operator employed for performing authentication functions and maintaining necessary systems, infrastructure and process, possess requisite qualification for undertaking such work.
16	34	Incident management procedure and RCA procedure	Sub AUA/ Sub KUA should ensure that incident management framework, including forensic investigation, is implemented in accordance with the requirements under UIDAI’s Information Security Policy and circulars. Sub AUA/ Sub KUA should perform Root Cause Analysis (RCA) for major incidents identified in its ecosystem as well as that of its sub- contractors, if any.

17	35	Reporting of incidents to UIDAI and CERT-In	Sub AUA/ Sub KUA should— (a) inform UIDAI misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within its network, and report any confidentiality security breach of Aadhaar related information to UIDAI within 24 hours; (b) report cyber incidents as mentioned in Annexure I to the directions dated 28.4.2022 of CERT-In, bearing no. 20(3)/2022- CERT-In, within 6 hours of noticing such incidents or the same being brought to their notice; and (c) on and from the date of coming into force of sub- section (6) of section 8 of the DPDP Act, intimation of personal data breach to the Board and each affected Data Principal, within such time as may be prescribed by rules made under the said Act.
18	38	Access provisioning mechanism	Sub AUA/ Sub KUA should ensure that only authorised individuals are able to access information facilities such as the authentication application, audit logs, authentication servers, application, source code, information security infrastructure, etc., and Aadhaar processing related information.
19	39	Privilege user access management	Sub AUA/ Sub KUA should ensure that systems and procedures are in place for privilege user access management (PAM). Privilege user access should be limited to authorised users only.
20	40	Privilege accounts	Sub AUA/ Sub KUA should ensure through the PAM tool that privileged accounts, such as NT Authority, Administrator, and root accounts, are accessible only to a limited set of users, and that access to privileged account is not allowed to normal users.
21	41	Periodic access review	Sub AUA/ Sub KUA should ensure that access is provided based on least privilege and that access is reviewed periodically (at least half-yearly).
22	42	Access revocation mechanism	Within 24 hours of exit of any personnel, Sub AUA/ Sub KUA should revoke the rights and privileges to access or process Aadhaar related information. Upon such revocation, user IDs should be deleted forthwith if not in use.
23	44	Initial password allocation	Sub AUA/ Sub KUA should ensure that the allocation of initial passwords is done in a secure manner and that such passwords are changed on first log in.
24	46	User account lockout	Sub AUA/ Sub KUA should ensure that three successive log-in failures result in the user account being locked. End users / operators should not be able to log in until their account is unlocked and the password is reset.

25	48	Change logs management	Sub AUA/ Sub KUA should document all changes to Aadhaar authentication applications, infrastructure, processes and information processing facilities, and maintain change log/register.
26	67	Use of ADV on cloud	Sub AUA / Sub KUA having ADV on cloud should get annual SOC2 Type2 examination performed for cloud hosting service. Management review should be performed for non- compliant / qualified controls reported in the SOC2 Type2 reports.
27	70	Use of ADV	Sub AUA / Sub KUA should ensure that strong access controls, authentication measures, monitoring and logging of access and raising of necessary alerts for unusual and/or unauthorised attempts to access ADV are implemented.
28	71	End-point security	Sub AUA / Sub KUA should ensure that USB access on the servers and endpoints is, in the default, restricted for all, and the same is allowed only on approval basis.
29	74	Restriction on display/ publishing of identity information	Sub AUA / Sub KUA, Business Correspondents and other sub-contractors performing Aadhaar authentication should ensure that identity information is not displayed or disclosed to external agencies or unauthorized persons.
30	75	Restriction in display/ publishing of identity information	Sub AUA / Sub KUA should not publish any personal identifiable data including Aadhaar in public domain/websites etc.
31	79	Restriction in local storage of Aadhaar data / PII information	Sub AUA / Sub KUA should ensure that there is no local storage of Aadhaar number or VID or the PID block on the system, volatile memory or the database. In case of a mobile application, Sub AUA / Sub KUA should ensure that there is no local storage of Aadhaar number or the PID block in the shared preference folder.
32	85	Firewall access of network	Sub AUA / Sub KUA should ensure that authentication application servers and infrastructure are hosted behind a firewall and that firewall rules block incoming access requests to the Sub AUA / Sub KUA server from all sources other than whitelisted IP addresses/zones.
33	86	NIPS/IDS implementation	Sub AUA / Sub KUA should ensure that network intrusion and prevention systems (NIPS) and intrusion detection system (IDS) are implemented to safeguard the network from external attacks / DDoS attacks.

34	91	Implementation of Virtual ID	Sub AUA / Sub KUA must provide in their authentication application the option for an Aadhaar number holder to use a Virtual ID (VID) for authentication, in place of their Aadhaar number.
35	94	Back-up / alternative identity authentication mechanism	Sub AUA / Sub KUA should implement exception- handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication delivery of services to Aadhaar number holders.
36	95	Notification to Aadhaar number holders	Sub AUA / Sub KUA should notify the Aadhaar number holder of the success or failure of each authentication request, through email and/or SMS. Such notification should shall include the name of the requesting entity, the date and time of authentication, the authentication response code (in case of online authentication), the last four digits of the Aadhaar number and the purpose of authentication, as the case may be. In case of authentication failure, the AUA/KUA should, in clear and precise language, inform the Aadhaar number holder of the reasons of authentication failure, such as "Aadhaar cancelled", "Aadhaar deactivated", "Aadhaar locked", "Aadhaar omitted", "Aadhaar suspended" and "Biometrics locked".
37	96	Establishment of grievance handling mechanism	Sub AUA / Sub KUA should have an effective grievance handling mechanism and provide the same through multiple channels.
38	99	API whitelisting and API gateway implementation	Sub AUA / Sub KUA should ensure that it has API whitelist implemented to limit the data exchange using only authorised APIs and with whitelisted IP addresses. Sub AUA / Sub KUA should also ensure that API gateway is deployed for centralised security enforcement, monitoring and management. Sub AUA / Sub KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDoS) attacks. Sub AUA / Sub KUA should ensure that Cross-Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side.
39	108	Security incident monitoring	Sub AUA / Sub KUA should ensure that regular monitoring of event/security logs takes place to detect unauthorised use of information systems and that results of the same are recorded. Further, access to audit trails and event logs should be provided to authorized personnel only.
40	110	Fraud analytics module	Sub AUA / Sub KUA should deploy, as part of its systems, a fraud analytics module that is capable of analysing authentication related transactions to identify fraud.

****