

Tender Number: PSBA/RFP/EAUC/2022-23/009 Dated 31/03/2023  
Corrigendum 3 Dated 28.04.2023



# PSB Alliance Private Limited

Promoted by Banks

Request for Proposal for Supply, Installation & Maintenance of End-to-End E-AUCTION Solution

(RFP Ref. No. PSBA/RFP/EAUC/2022-23/009 Dated 31/03/2023)

## Contents

Section 1: Modification in RFP Dates.....	2
Section 2: Modification in RFP Clauses.....	2
Section 3: Technology Stack.....	3
Section 4: Revised Appendix 2- Commercial Bill of Material .....	7
Section 5: Addition to Appendix 1B- Technical Specifications Revised.....	7

### Corrigendum – 3 Request for Proposal for Supply, Installation & Maintenance of End-to-End E-AUCTION Solution

In reference to our RFP for Supply, Installation & Maintenance of End-to-End E-Auction Solution vide Tender No. PSBA/RFP/EAUC/2022-23/009 dated 31.03.2023

Kindly be guided by the clarification and changes to clauses.

#### Section 1: Modification in RFP Dates

#	Clause Reference	Original Dates	Revised Dates
1.	Last date for submission of RFP Response	02.05.2023 till 3:00PM	15.05.2023 till 3:00PM
2.	Date of Opening of Bids	02.05.2023 till 3:30PM	15.05.2023 till 3:30PM

#### Section 2: Modification in RFP Clauses

#	Clause Reference	Original Clause	Revised Clause
1.	Section 4: Scope of Work; Hosting Infrastructure and Operations Management	All the deployments including Development, UAT and Production environment, are proposed to be over MeitY (Govt. of India) empanelled and STQC audit compliant (for Public Cloud service offering) Cloud Infrastructure with provision of data localization in India.	Clause stands deleted
2.	Section 4: Scope of Work; Technology Stack	Entire Section	Please refer Section 3 of this document for revised Scope of technology Stack
3.	Appendix 2- Commercial Bill of Material	Entire Section	Please refer Section 4 of this document for revised Appendix 2- Commercial Bill of Material
4.	Appendix 1B- Technical Specifications	Cloud Security	Please refer Section 5 of this document for the added clause in Appendix 1B- Technical Specifications-Security Tab (point no.63)
5.	Earnest Money Deposit (EMD)	Earnest Money Deposit (EMD) EMD can be deposited by means of a Bank Guarantee issued by a Scheduled Commercial Bank as per Annexure-15 MSME Bidders will be exempted from payment of cost of RFP if Bidders can furnish requisite proof subject to satisfaction of the Company.	Earnest Money Deposit (EMD) EMD can be deposited by means of a Bank Guarantee issued by a Scheduled Commercial Bank as per Annexure-15  MSME Bidders will be exempted from payment of cost of RFP if Bidders can furnish requisite proof subject to satisfaction of the Company.  <b>Alternatively,</b> Bidders can submit EMD through NEFT as well by attaching receipt of NEFT transfer along with the

#	Clause Reference	Original Clause	Revised Clause
			<p>RFP submission. The bidder before the submission will be expected to deposit this amount so that the company can confirm the receipt of the funds before bid opening. The bidder will be expected to inform the Company giving details of the transaction. The NEFT details for the transfer are:</p> <p><b>1. Payee Name: PSB Alliance Pvt. Ltd.</b>  <b>2. Bank Name: State Bank of India</b>  <b>3. Bank A/c No: 41204656705</b>  <b>4. IFSC Code: SBIN0001821</b>  <b>5. Type of A/c: Current A/c</b></p>
6.	Non-refundable Tender Application Fee	<p>Tender Application fee of Rs. 10,000/- (Rupees Ten Thousand only) is to be submitted on or before the bid response submission by way of a Demand Draft favouring PSB Alliance Pvt. Ltd. payable at Mumbai / NEFT as per the detailed below:</p> <ul style="list-style-type: none"> <li>• Payee Name: PSB Alliance Private Limited,</li> <li>• A/c No.: 41203155700</li> <li>• IFSC Code: SBIN0001821</li> <li>• Account Type: Current A/C</li> </ul>	<p>Tender Application fee of Rs. 10,000/- (Rupees Ten Thousand only) is to be submitted on or before the bid response submission by way of a Demand Draft favouring PSB Alliance Pvt. Ltd. payable at Mumbai / NEFT as per the detailed below:</p> <p><b>1. Payee Name: PSB Alliance Pvt. Ltd.</b>  <b>2. Bank Name: State Bank of India</b>  <b>3. Bank A/c No: 41204656705</b>  <b>4. IFSC Code: SBIN0001821</b>  <b>5. Type of A/c: Current A/c</b></p>

### Section 3: Technology Stack

Bidder to ensure that the Application is:

1. Application to be designed as a Micro-service
2. To be containerized adhering to Open container Initiative (OCI) based standards (both for run time and image) using cloud native containerization service and orchestrated using Kubernetes based container orchestration tools in a multi node/ cluster formation leveraging both OS and VM level virtualization.
3. Data Processing, Event processing, Log Aggregation, Metric collection, website activity tracking, stream processing etc. to be handled using Kafka based messaging frameworks coupled with ELK stack.

4. The Bidder/ CSP should adhere to serverless computing services model to achieve better performance and cost optimization running on cloud. All components and services to be on IaaS model of deployment.
5. The content should be delivered through cloud native Content Delivery Network (CDN) services from the CSP for achieving better response and security.
6. The proposed design Pattern should implement distributed caching environment where the data can span multiple cache servers and be stored in a central location for the benefit of all the consumers of that data. The dedicated caching layer should enable systems and applications to run independently from the cache with their own lifecycles without the risk of affecting the cache enabling application nodes to scale in and out dynamically. The cache should serve as a central layer that can be accessed from disparate systems with its own lifecycle and architectural topology.
7. Bidder needs to note that the application needs to be deployed on AWS (Virtual Private cloud - VPC) and needs to be managed by bidder under back-to-back Business/Enterprise level support from public cloud CSP- AWS \*. All the cost of the hosting all the environment as mentioned in the RFP needs to be factored in by the bidder in the Commercial bill of material with proper details and break up. During selecting of the Cloud service provider, the bidder needs to ensure the following:
  1. The bidder has to develop the application based on IaaS model for the web application and to be based on micro-service and containers-based architecture to support the flexibility and portability.
  2. The infrastructure elements including server, storage, backup storage and network of the Cloud should provide strong tenant isolation, granular identity and access management capability and encryption and be logically separate from the public and other cloud offerings of the cloud service provider. There should be logical separation (of servers, storage, network infrastructure and networks) to protect data, applications and servers and provide robust virtual isolation for the Cloud to PSB Alliance. The cloud service offering should support Network and security with firewall and load balancer integration for auto-scale functions.
8. The Bidder is required to set up different environments like Development, UAT, Production, DR and PreProd on AWS cloud.
9. The Bidder/ CSP should provide & support relational and non-relational database service compatible to store both Structured data and Unstructured data (like but not limited to MySQL/ PostgreSQL/ MongoDB/ Cassandra/ Hadoop based or equivalent as applicable) provided as a cloud service enabled to handle routine database tasks such as provisioning, patching, backup, recovery, failure detection, and repair etc. The cloud native database has to be compatible to support Big data requirements also. Bidder should consider open-source database deployed on IaaS model on AWS EC2 instances and shall own all the Database management related tasks during operations.
10. The Bidder/ CSP should adhere to serverless computing services that are able to run code in response to events and automatically manage the compute resources. The CSP should offer highly scalable and high-performance container management service (e.g. Kubernetes or equivalent) in a multi node/ cluster formation leveraging both OS and VM level virtualization.
11. Bidder needs to host all the environment (Development, UAT, Production, DR and PreProd) on AWS (Virtual Private cloud) with Private Subnets and Built-in Firewalls to control how accessible the VMs are by configuring built-in firewall rules and Gateway, and other services to implement the serverless architecture.

**\* AWS is an existing CSP for PSB alliance**

12. Data Centre and Disaster Site (DR) (Data Centre and Disaster Site (DR) shall be in India and in different seismic zones) selected by bidder shall be in India. Bidder and CSP has to ensure for all type of data should reside within India. Bidder shall provide DC and DR on AWS. Primary Site shall be deployed in Mumbai region with multi-Availability Zone deployment and shall support active-active deployment with synchronous replication and a Far DR site shall be created in AWS Hyderabad region.
13. Conduct periodical DR Drills (a minimum of one in every Calendar quarter).
14. Bidder has to ensure that Far DR setup is ready on the date of Go Live of solution
15. Bidder should carry out the deployment of the application in Development, UAT, Production, DR and PreProd as applicable.
16. Providing network, security and other components at DR site shall be in scope of the bidder and it shall be responsibility of Bidder to ensure similar configuration at DR to that of DC site
17. Bidder should setup the DR site (Data Centre and Disaster Site (DR) shall be in India and in different seismic zones) with data replication on affordable storage, minimal compute resources to maintain ongoing replication and point-in-time recovery. DR solution should support non-disruptive tests. During normal operation, maintain readiness by monitoring replication and periodically performing non-disruptive recovery and failback drills. To achieve complete replication of data and maintaining one copy of data on DR site, the data shall be replicated 100% and shall be sized accordingly to maintain the data at DR site at all the time. Disaster Recovery resources other than data are to be configured scalable (on demand) to 100% of Production Data Centre capacity.
18. Bidder needs to provide RTO of 30 mins and RPO of 15 mins
19. Bidder should consider high-availability (active-active for Primary site and Active-Passive for Far DR) between DC and DR setup for Portal and Mobile app. Bidder shall deploy and consider multi availability Zone deployment of all workloads on AWS. Bidder needs to implement and configure synchronous replication within primary site for all the Application, Database, Stateless and IT infrastructure components are replicated to DR site and are operational at all the time.
20. Recovery time operations (RTO of 30 mins and RPO of 15 mins) to be maintained using Global Server Load Balancing (GSLB) / Availability Zone DNS-based load balancing and failover between DC and DR and within the site using Application Load balancer, Network Load balancers and Gateway load Balancers as applicable.
21. DC and DR set up must comply with all current & future Indian regulatory guidelines defined for providing cloud- based services in India.
22. The Internet connectivity should be available to the applications as per the SLA requirements Additional charges for Data Ingress or Egress will be paid by PSB Alliance as applicable.
23. Cloud must be hosted in India including DC and DR in India, no network, and data sharing/ replication to any data center outside the boundaries of the country is permitted. The bidder will be bound by Indian law and Indian IT Act (Cyber Law). No data in any circumstances should be shared/ copied/ transmitted without Company's consent/ written permission of PSB Alliance and it should be as per the Indian IT act (Cyber Law).
24. The bidder will be required to migrate the application and data to an alternate MeitY (Govt. of India) empaneled hyperscaler public Cloud service provider in case the existing public cloud service provider is de-empaneled by MeitY for whatsoever reasons during the tenure of the contract, at no extra cost to PSB Alliance beyond the existing terms and conditions of the RFP.

25. The data files along with archives and individual file storage should be hosted in India for primary and secondary copies
26. The bidder must provide the Application Deployment Architecture with diagrams, identifying components and specifications for each component with description. Description must detail the number of servers, specifications for each resource (Web server, Application, DB, File server, Resource Monitoring servers etc.), Operating System and configuration as well as function of each server, Network Bandwidth Requirements and Storage Requirements.
27. The bidder is responsible for actual sizing of the infrastructure as per the scope of work, activities and Service Levels and projections as defined in this RFP
28. The proposed infra should be IPv4 and IPv6 compatible
29. CSP Shall have to provision for the below security components at the minimum to secure the environment (1) DDoS protection (2) Firewall (3) Anti-virus (4) Data Encryption at rest and in transit (5) SSL off-load/ Data protection/ Zero Day Vulnerability protection (6) Web Application Firewall (WAF) (7) Basic SIEM and Security Reporting (8) Network Zoning and segmentation (9) Others (If required) or Cloud marketplace subscription or 3rd party products that shall be deployed on hyperscale cloud.
30. The system must provide the ability to perform backups and recoveries of the system including, but not limited to, virtual machines, storage, the database, core and customized software, software and database configuration options, and user preferences and rights
  1. The Bidder should ensure to perform backups and restores in a full, incremental and differential manner (daily incremental and weekly full backup) to support the recovery time objectives mentioned in the RFP.
  2. The system must support the ability to perform online backups without interruption to system functions or features.
  3. The backup should be tested on a half yearly basis. However, PSB reserves the right to define/ update the backup strategy for different applications and Bidder shall configure the backup policies as per PSB's requirements.
  4. The Bidder shall submit a well-defined plan for backup and recovery including processes and procedures etc. related to recovery or continuation of services.
31. Load balancing: Bidder needs to provision, size and configure fully supported PaaS based load balancing capabilities which should operate at both layer 4 (Global Service Load Balancing/ External HTTP(S) Load Balancing) and layer 7 (application Load balancing/ Internal HTTP(S) Load Balancing).
32. Caching (CDN): The CSP should offer content delivery network service to speed up distribution of static and dynamic web content. CSPs should have content delivery network edge locations in India. The bidder needs to provision at least eight (8) CDN pops for the application. The dynamic and static contents of the web portal to be cached using cloud native CDN service for the quick transfer of assets needed for loading Internet content including HTML pages, JavaScript files, stylesheets, images, and videos. The vendor has to do appropriate sizing of cloud infrastructure to ensure smooth functioning of the website even in case of failure/ absence of CDN. The CDN service should be able to improve website load times, reduce bandwidth consumption costs for website hosting on origin server, increasing content availability and redundancy, improving website security by providing DDoS mitigation, improvements to security certificates, and other optimizations. The vendor should be able to monitor and control the content being delivered through Content Delivery Network (CDN).
33. In memory Caching Engine: The proposed architecture should implement enterprise level in memory caching engines or equivalent cloud native solutions throughout various layers of

technology including Operating Systems, Networking layers including Content Delivery Networks (CDN) and DNS, web applications, and Database. Caching Engine should be based on opensource technology and deployed on AWS with enterprise-grade security and reliability.

34. Bidder should provide CSP native or marketplace based IVR service at DC and DR sites on AWS
35. Bidder should provide CSP native or marketplace based chatbot service at DC and DR sites on AWS
36. Bidder should provide CSP native or marketplace-based Application Performance Management (APM) solution at DC and DR sites on AWS

## Section 4: Revised Appendix 2- Commercial Bill of Material

Revised Appendix 2: Commercial Bill of Material is attached as a separate file

## Section 5: Addition to Appendix 1B- Technical Specifications Revised

Added clause in Appendix 1B- Technical Specifications-Security Tab (point no.63)

a) The solution should have CSPM licensed for minimum 1 AWS / Azure / GCP Account supporting unlimited resources for 5 Years from Day 1 and must provide in-built compliance rules for PCI-DSS, AICPA SOC2 TSC, CIS AWS Foundations Benchmark, CSA CCM, GDPR 1996/679, HIPAA 1996, ISO 27002, NIST 800-53r4, NIST CSF. The CSPM must perform Auto-Remediation of AWS misconfigurations by using AWS Lambda functions and mitigate violations automatically.

b) Solution should have IaaS (AWS / Azure / GCP ) storage scanning for minimum 5TB of data for 5 Years (True Up as per Actual Consumption) and must be able to inspect data in Storage Buckets for Malwares, Threats and protect Data exfiltration. It must have 2500+ Data Identifiers, 1500+ File Types Support and enforce DLP Policies based on content, keywords, patterns, regex, exact data matches, size, etc and use AI/ML Learning to understand sensitive documents in the form of images stored and protect via OCR within Image Files. The IaaS Security solution must provide advance threat protection and Sandboxing for 30+ file types for Zero-Day attack protection from Day 1.

c) All the above capabilities must have a single management & reporting console and must retain all Alerts and Logs for 90 Days with Inbuilt Incident Management Page for Advance Threats and Advance Data Protection and proposed solution must have SOC2, ISO 27018, CSA Star and CIS certifications.

**Note: All other clauses, criteria and terms and conditions in the RFP remains unchanged.**

**-xxx- END OF DOCUMENT -xxx-**