THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY
KENYA DIGITAL ECONOMY ACCELERATION PROJECT
ICTA-PROGRAM IMPLEMENTATION UNIT

Name of Assignment: Procurement of an Electronic Auctions Platform
RFP Reference No.: KE-ICTA-414831-NC-RFB
Loan No./Credit No./Grant No.: IDA 7289-KE and 7290-KE
Country: Kenya
Date: 5th December 2024

Dear Mr./Ms.: **All Interested Bidders**

RE: AMENDMENT OF RFB DOCUMENT THROUGH ADDENDUM NO. 1

In accordance with the Instructions to Bidders ITB 8 *[Amendment of Bidding Document]*, the Client has amended the following sections of Specification of the issued RFB Document:

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
1.	Page # 64 6.4 Payment Terms	Can we propose our own payment terms? Please confirm	The propose Payment terms is according to SCC 6.4. This is subject to negotiations at contracting stage
2.	Page # 15 20.3 Bid Security	Is a bid bond in the form of cash acceptable? Please Confirm	No. Bid Security is in the form of bank guarantee
3	Page # 91 1.3.1.1 Cloud Infrastructure	Cloud Provider Selection: Is there a preferred cloud provider (AWS, Azure, Google Cloud) for this project, or is the choice left to the service provider?	There is no preferred cloud provider. *"The requirement is to utilize cloud providers (AWS, Azure, Google Cloud **or equivalent**) to leverage scalable virtualized hardware resources"*
4	Page # 92 Multi-Tenancy:	Data Residency Requirements: Are there any specific data residency requirements that need to be adhered to, such as data storage within Kenya or specific regions?	Refer to Appendix A- - Description of Services for the legal framework.
5	Page# 92 APIs	Integration with Existing Systems: Are there any existing	None currently

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		systems or platforms that the new auction platform needs to integrate with? If so, what are the specific requirements or APIs available?	
6	Page # 90 Standards Compliance	Security Compliance: Are there any specific security compliance standards (e.g., GDPR, HIPAA) that the platform must adhere to beyond the mentioned requirements?	The mentioned requirements are the minimum. Bidders can meet or exceed the stipulated requirements.
7	Page # 91 1.3.1.3 Performance:	Performance Metrics: Are there any specific performance metrics or SLAs (Service Level Agreements) that need to be met, particularly regarding uptime, response time, and concurrency?	The requirement includes: "*Cloud Monitoring Tools: Implement cloud-native monitoring tools (AWS CloudWatch, Azure Monitor, Google Cloud Operations) for real-time infrastructure health and performance tracking.*"
8	Page # 39 Bullet point: Integration	Could you please provide details of the existing ERP system? Please advise	The ERP is Microsoft Navision/Microsoft Dynamics NAV
9	Page # 91 1.3 Architectural Requirements to be met by the Information System	Will all third-party licenses, such as Oracle as a service, be the responsibility of the Employer (*The Information and Communications Technology Authority*)? Please advise	The offer should come as a fully packaged service meeting the stated requirements
10	Page # 94, 1.6, 1.6.1.2 Cyber Security – RBAC – MFA – Audit Logs Security considerations in computing resources, network, and Application level,	• Which authentication protocols are required (e.g., SAML, OAuth, OpenID Connect)? Should the system integrate with LDAP/Active Directory, and is MFA with session timeout enforcement needed? • Login History: How long should login	• Requirements as stated. • The Public Procurement and Disposal Act in Kenya requires retention of records for a minimum of 7 years.

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
	User Access and Security Inquiry	history be stored to meet audit and compliance requirements like GDPR or HIPAA? What level of detail (e.g., IP, device details) should logs include? • RBAC Frameworks: Are there specific role-based access control (RBAC) policies or frameworks to follow? Should frequent access rights changes be automated based on predefined rules? • Change Logs: What level of detail should change logs include (e.g., IP address, device details, timestamps)? Should changes notify specific administrators or be archived for periodic audits?	No specific RBAC frameworks and access rights changes to be automated • Details to Include in Change Logs Timestamp: ○ Precise date and time of the change. ○ Ensure timestamps are in GMT or a clearly defined timezone to avoid discrepancies. Actor Details: ○ Identify who made the change (e.g., username, user ID). ○ Include additional identifiers like user roles or privileges. IP Address: ○ Capture the source IP address of the actor's device for traceability. Device Details: ○ Log device-specific identifiers (e.g., MAC address, device name, or operating system version), especially for sensitive systems. Action Performed: ○ A clear description of what was changed, including the before and after states, if possible. Affected Resource: ○ Specify the system, file, or record that was altered. Method of Change:

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
			○ How the change was made (e.g., via API call, GUI, command line). Success/Failure Status: ○ Indicate whether the action was completed successfully or failed, along with any error messages. Reference Information: ○ Include any associated ticket numbers or reasons for the change for audit clarity. • Access control to be controlled both at user and group level dependent on roles
		• Access Controls: How granular should access controls be—at the user, role, or group level? Are there restrictions required based on IP, network zones, or geolocation? Should privileged access management (PAM) be included? • Encryption Standards: What encryption standards are necessary to protect data in transit and at rest (e.g., VPNs, TLS)? Are there specific compliance or organizational	• Encryption Standards: The minimum standard is "**Data Encryption:** Ensure data is encrypted in transit using SSL/TLS. " • **Network Security Measures:** Implement security groups, virtual private clouds (VPCs), and firewalls to protect network traffic. • This will be managed through the continuous monitoring, detection, and responsive action mechanisms.

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		standards to follow? • Network Security Integration: Should the system integrate with firewalls, IDS/IPS, or SIEM tools for real-time monitoring? Are there network segmentation needs for enhanced security? • Compromised Account Handling: How should the system manage compromised accounts? Is continuous monitoring for abnormal user behavior and detection of SSO attacks (e.g., brute force) required? • API Security: What access levels should be defined for users, systems, and resources? How should token management be handled, including lifetimes, renewal, and revocation? Is two-way SSL with automated certificate renewal necessary? • Authentication Methods: What authentication methods are preferred (e.g., password-based, biometric, OAuth)?	• Use role-based access control (RBAC) to assign predefined permissions based on user roles and Incorporate multi-factor authentication (MFA) for high-privilege roles. "The system should have two-factor authentication for bidder accounts." • "Authentication and Authorization: Implement robust identity and access management (IAM) solutions using OAuth, SAML, or cloud-native IAM services. " • Role-based. Authorisation policies centralised • OAuth 2.0 with JWT for modern, scalable, and stateless authentication. Username/Password with MFA for backward compatibility or simple

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		How many users are expected to authenticate simultaneously, and what failover mechanisms are required? • Authorization Policies: Should access control be role-based or attribute- based? Should authorization policies be centralized, and how should changes propagate across the network? API Management Security: How should security policies for APIs be defined, monitored, and enforced? Is logging and auditing access attempts necessary for compliance and incident response? • Access Management: Which authentication methods (e.g., OAuth, JWT, username/password) should be prioritized? What should be the token lifetimes, and how should renewal or revocation be handled?	systems. **Token lifetimes** • **Short Lifetimes:** o Lifespan: **5 to 15 minutes**. • **Longer Lifetimes:** o Lifespan: **7 to 30 days**. • **Revocation Mechanism:** o Revoke immediately upon detection of anomalies or account compromise. • **Web Applications:** o Lifespan: Session duration or **8 hours** for typical workdays. o Expire on user logout or browser closure. • The system should have two-factor authentication for bidder accounts. • "Concurrency: Support for thousands of concurrent users without performance degradation, especially during high-traffic bidding sessions. "

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		• Certificate Management: What certificates will be used for two-way SSL, and how will certificate management be handled? Should automated certificate renewal be implemented to minimize downtime? • For Concurrent User Access, how many users are expected to access the system simultaneously? Should the system accommodate potential spikes in user activity, and what is the expected load?	
11	Users Information Generic: Inquiry about users details and types	• For Concurrent User Access, how many users are expected to access the system simultaneously? Should the system accommodate potential spikes in user activity, and what is the expected load? • Are there any bandwidth or latency considerations to ensure smooth	• It is envisaged that the system should accommodate a minimum of 500 concurrent users with a possibility to spike • Content, latency and bandwidth management with usage monitoring to ensure fair use by all

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		performance with multiple concurrent users? Should traffic be segmented or prioritized for certain programs or users? • Are there any bandwidth or latency considerations to ensure smooth performance with multiple concurrent users? Should traffic be segmented or prioritized for certain programs or users? • How should concurrent user sessions be monitored for potential threats or anomalies? Are there requirements for securing user session data, and should session logging be implemented for audit purposes? • For Scalability, do purchaser anticipate the need for future expansion to accommodate more users or Applications? Should the system be designed to scale dynamically to handle increased load without impacting performance • Could the purchaser provide an estimate of the total number	• "Scalability: The Information System must handle varying loads, especially during peak auction times, with seamless scalability to accommodate increased traffic and bidding activity." • "Concurrency: Support for thousands of concurrent users without performance degradation, especially during high-traffic bidding sessions."

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		of in-house users who will need access to the system? • Does the purchaser anticipate a significant number of remote users accessing the system, and if so, could they provide an estimate of their numbers? • Are there distinct user entities within the purchaser's organization that will require different levels of access to the Application? • To ensure security and streamline access, would it be advisable for the purchaser to implement user-based policies to regulate access levels within the Application? • If user-based policies are deemed necessary, could the purchaser specify the different categories of users and their corresponding access requirements? • What is the total number of expected users for the system, including both internal and external users? Are there different categories of users (e.g., employees, contractors, and	

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		partners) that we should account for in our planning? • Will there be users accessing the system from the disaster recovery (DR) site? If so, how many users are anticipated, and what specific functionalities will they require? • How many remote users do purchaser expect, and what level of access will they need to the system? Are there any specific security measures or VPN requirements for these remote users? • Will any third-party users require access to the system? If yes, how many third-party users do purchaser anticipate, and what specific roles or permissions will they need?	
12	Accessibility with Purchaser's Needs User Access Details Planned Data Sharing within the Ecosystem Compliance & Authorities	• Could the purchaser provide details on the user groups requiring access, including internal stakeholders and external Stakeholders? • Clarifying if users require remote access and how	• This is generic the internal users include project staff, Procurement team, Legal and Compliance Team, Finance, IT Support, Executive Management. External Stakeholders include Suppliers/Bidders, Auditors/Regulators and Consultants/Advisors,Collaborative Partners • "Multi-Factor Authentication (MFA): Due to the sensitivity and confidentiality of the bidding exercises, all the user accounts on the system, especially those with

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		authentication will be managed will further guide the purchaser in tailoring a solution to meet their requirements efficiently. • Could the purchaser provide details regarding the types of data and entities that are planned to be interconnected with the main Application and other related solutions for data sharing purposes? • Could the purchaser provide further clarity on how Stakeholders envisions the core technologies working together to deliver business value, and what specific outcomes or benefits are expected? • Additionally, what types of robust cyber security products and services are anticipated from bidders to maximize value for Stakeholders, and are there particular features or capabilities desired? Regarding the common management system/console for	administrative access, must use multi-factor authentication." • "Standards Compliance: Ensure software complies with industry standards for data exchange (e.g., JSON, XML, SOAP). " • The Business Function Requirements to be met by the Information System MUST support the specified functions. • "Security and Compliance Training: Training materials covering security best practices, data encryption, access controls, and compliance requirements relevant to the auctioneering and bidding system shall be required. Virtual workshops on cybersecurity awareness, phishing prevention, and data protection measures can be conducted for technical staff." • "**Scalability and Performance**: **High Availability**: Ensuring the platform is reliable and available during critical auction periods. **Performance Optimization:**

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		cyber security, what functionalities are deemed essential for user management, data management, component management, and hardware component management? • How does Stakeholders envision the proposed architecture creating an integrated and simple data environment for managing cyber security threats, and are there any scalability or performance requirements? • what key considerations exist for ensuring a seamless user experience and accessibility within the cyber security system, and are there any specific user interface requirements or preferences for the management system/console? • Could the purchaser specify the roles within their organization that will	Handling large numbers of concurrent users and bids without performance degradation " • "Implement a user interface where administrators can specify lot categories, lot size, Time allocated and other relevant details for the MRRA event. Responsive Design: Ensure the user interface is responsive and accessible on various devices and screen sizes. " Refer to item No. 12 above

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		require access to the solution and the associated permissions and privileges?	
13	Page # 95, 1.6.1.3, 1.6.1.5, 1.6.1.6 Access and Encryption Requirements Access Control, Data Governance, and Security Measures	• Could the purchaser specify the roles within their organization that will require access to the solution and the associated permissions and privileges? • Regarding data encryption, we need to understand the types of data to be encrypted (at rest, in transit, and in backup media) and any specific encryption standards or algorithms to be followed. Additionally, clarification on which columns or fields require encryption at the column level and any access restrictions for administrators, such as DBAs and root-level administrators, is necessary. Ensuring these administrators cannot view encrypted data is crucial. Lastly, understanding any compliance regulations,	• Refer to item No. 12 above • "Data Encryption: Ensure all data is encrypted at rest and in transit using cloud-native encryption services. " • The access will be granted based on the roles assigned for the system

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		monitoring procedures for encrypted data access, and governance requirements for encryption keys and access controls. • could the purchaser provide details on how access will be granted based on the role and responsibility matrix within their organization? • Additionally, we'd like to learn more about the purchaser's plans for establishing a data governance practice to ensure the security of data, including adherence to governing authorities' standards. Regarding security measures, could the purchaser specify which columns or fields require protection at the column and row levels, along with any criteria or rules for determining access?	• The requirement is that "Data Encryption: Ensure all data is encrypted at rest and in transit using cloud-native encryption services. "
14	Page # 95. 1.6.1.3 Page # 137. 1.2.95 Audit Trail Detailed Information on Access Control and Audit Trail Management	• Could the purchaser provide more details on how the defined access matrix will be structured and managed, and what criteria will determine access authorization for sensitive data and transactions?	• The bidder will provide: "Role-Based Access Control: Different access levels for administrators, buyers, and suppliers." • The "**Access Control**: Robust mechanisms to prevent unauthorized access to the

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		• Additionally, we'd like to clarify how default access restrictions will be enforced unless formally authorized by the access matrix, and if there are any exceptions to this rule. Furthermore, could the purchaser elaborate on the granularity level at which access will be defined within the matrix, and what specific types of access authorization will be included? • Regarding audit trail requirements, besides user log-in and log-out date/time, what other information needs to be captured, and how will the accuracy and completeness of audit trail records be ensured? • how does the purchaser plan to ensure that audit trail records are easily retrievable from a report at any time, and are there any specific reporting requirements or stakeholders who need access to these reports?	platform and data. " and as well • "**User Suspension and Deactivatio**n: Administrators should have the ability to suspend or deactivate user accounts. Deactivated accounts should restrict access to the system. Provide reasons and audit trail for user suspension or deactivation." • The requirement is that **"Administrators** should have the ability to suspend or deactivate user accounts. Deactivated accounts should restrict access to the system. Provide reasons and audit trail for user suspension or deactivation" • "Audit Trail: Maintain a comprehensive audit trail for all account management activities. Record changes to user roles, profile updates, and account status changes. Logs should be immutable and tamper-proof."

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		Gathering this information will help tailor the solution to meet the purchaser's access control and audit trail management needs effectively	
15	Page # 95. 1.6.1.4 & 1.6.1.5 Disaster recovery strategy Recovery Time Objective (RTO) Recovery Point Objective (RPO)	• How frequently is data backed up, and are there specific intervals for different types of data? Are industry regulations like GDPR, HIPAA, or SOX dictating purchaser data retention and backup frequency, and how do these affect purchaser practices? • In a disaster, which systems are prioritized for recovery, and what is the maximum acceptable downtime for each critical system? Does the purchaser need a secondary recovery site, or are they considering cloud-based solutions? • What are the main threats and risks the purchaser's organization faces, such as natural disasters, cyber-attacks, or hardware failures? • Would the purchaser prefer on- premises,	• "**Backup and Recovery**: Implement automated backup and disaster recovery plans using cloud-native solutions. " • Cloud-based solutions • Cybersecurity Threats Include Ransomware attacks, Phishing and social engineering, Distributed Denial of Service (DDoS) attacks, Data breaches and insider threats • "Backup and Recovery: Implement automated backup and disaster recovery plans using cloud-native solutions. " • The Bidder is expected to implement a automated backup and disaster recovery plans

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		cloud-based, or hybrid solutions for their disaster recovery strategy? • Is the purchaser seeking assistance with the regular testing and updating of their disaster recovery plan?	
16	Page # 95. 1.6.1.4 & 1.6.1.5 Network Bandwidth Determination for Primary and Disaster Recovery Sites Disaster Recovery Infrastructure and Functionality Inquiry Data backup procedures, tools used and methods of taking backups.	The determination of network bandwidth, whether it pertains to internet connectivity or DPLC bandwidth, for establishing a secure connection between Primary (PR) and Disaster Recovery (DR) sites, will be contingent upon the service provision facilitated by the Internet Service Provider (ISP) or the Link Data Provider (LDP) integrated within the proposed solution framework. • Is the purchaser looking to maintain identical equipment between the primary site and the disaster recovery (DR) site, or are there specific differences the purchaser is considering? • Regarding high availability, are there any specific requirements for redundancy at the equipment level at both the primary and DR sites? • If high availability is necessary, is the purchaser leaning	• The envisaged solution is Software as a Service and hence no equipment will be delivered to the purchaser • "Uptime: High availability with an uptime of 99.9% or higher is mandatory to ensure that the platform is reliable and accessible during bidding exercises." • High availability • The envisaged solution is Software as a Service and hence no

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		towards an Active/Active or Active/Passive setup, or do they have another preference? • Does the purchaser expect the DR site to function at the same level as the primary site in terms of performance and capabilities? • To better understand the purchaser's data backup needs, could the purchaser provide insight into their current procedures? • The frequency of backups, any specific schedules in place for different data types, and the tools utilized for backup. Additionally, could the purchaser elaborate on the methods employed for taking backups, such as whether they utilize full, incremental, or differential backups, and whether backups are stored onsite, offsite, or both?	equipment will be delivered to the purchaser • This will be on a real time basis and dependent on the requirements of the issue • "Backup and Recovery: Implement automated backup and disaster recovery plans using cloud-native solutions. "
17	Page # 139, 1.6.1.4 Monitoring and Logging: Monitoring Tool for Maintenance and Reporting Mechanism	• Does the purchaser's required solution incorporate an OEM-based integrated monitoring tool, guaranteeing comprehensive monitoring,	• "Implement cloud-native monitoring tools (AWS CloudWatch, Azure Monitor, Google Cloud Operations **or equivalent**) for real-time infrastructure health and performance tracking. "

S/No	Reference to SPD	*ICTA Comments/amendments*	*ICTA Comments/amendments*
		surveillance, maintenance alerts, and reporting extraction functionalities? • Does this robust toolset ensure proactive oversight of the infrastructure, facilitating prompt detection and resolution of potential issues? • By seamlessly integrating monitoring capabilities into our solution, do we uphold operational efficiency and bolster reliability, fostering a professional-grade environment conducive to sustained performance and service excellence?	• Yes • Yes
		We kindly request an extension of one (01) week from the date of bid submission to allow adequate time for preparing a comprehensive proposal.	**The deadline for Bid submission has been extended as below:** **Date: 20th December 2024** **Time: 1000Hrs East African Time** **Consultants shall not have the option of submitting their Bids electronically**

This addendum forms part of the issued RFB document.
All other terms and conditions of the issued RFB document remain unchanged.

Stanley Kamanguya, OGW
Chief Executive Officer
ICT Authority