January 9, 2025

NOTICE TO OFFERORS

SUBJECT: Request for Proposals (RFP) 4-2622
"Time Clock Management Solution"

This letter shall serve as **Addendum No. 2** to the subject RFP issued by the Orange County Transportation Authority (OCTA). Offerors are reminded that the proposal submittal date is at or before **2:00 p.m., January 22, 2025**.

Offerors are advised of the following:

1. The agreement resulting from this solicitation, if awarded, will have a (3)-year term.

2. The date to conduct interviews has been changed to February 13, 2025. All prospective Offerors will be asked to keep this date available.

3. Responses to written questions submitted by the 2:00 p.m. deadline on December 24, 2024, are as follows:

Question 1:
Can you please tell me how many employees your Time Clock RFP pertains to?

Response 1:
Around 300.

Question 2:
We are requesting a two (2)-week extension for submittal of this RFP due to the holidays.

Response 2:
Per Addendum No. 1, the proposal submittal date has been changed to at or before 2:00 p.m., January 22, 2025.

Question 3:
How many employees/users will be utilizing the proposed Time/Attendance system?

Response 3:
See Response 1.

Question 4:
Can OCTA please provide a list of the specific groups that will be utilizing this solution along with any specific union/collective bargaining agreement (CBA) rules that would need to managed in a new Time/Attendance solution?

Response 4:
Maintenance, facilities, materials management, Human Resources and supported by the Information Systems department. The time clocks are not part of any CBA.

Question 5:
#58 under the system requirements references “maintaining and supporting interfaces to and from other applications.” Can OCTA please provide a list of the other applications aside from Workday and Lawson that the system would need to interface with?

Response 5:
Only Lawson and Workday.

Question 6:
Please list any gaps you are currently experiencing within Workforce Software, which must be rectified/provided within a new Time/Attendance solution.

Response 6:
See the business requirements section in the scope of work (SOW).

Question 7:
Can you please verify the following contract language to be a one (1)-year or three (3)-year term? We are seeing the following verbiage, and want to be sure that we are proposing the correct term length, as term length can affect pricing:

a. It is anticipated that the Agreement resulting from this solicitation, if awarded, will be a firm-fixed price contract specifying firm-fixed prices for individual tasks specified in the SOW, included in this RFP as Exhibit A. The Agreement will have a one (1)-year term.
b. Vendor shall provide all-inclusive license, hosting, maintenance, support, and other services for three (3) years, beginning with OCTA’s acceptance of the project. After one (1) year, OCTA reserves the right to terminate the contract at any time, and will provide Vendor a thirty (30)-day termination notice.
c. Termination for Convenience Customer may terminate this Agreement for any reason at any time with thirty (30) days written notice. Upon such termination, Customer shall have no claim for return of any license fees paid to Licensor.

Response 7:
The contract for the implementation and support is three (3) years minimum production with options.

Question 8:
Would eliminating the termination for convenience clause from the MSA automatically exclude vendors from a partnership opportunity?

Response 8:
See Exhibit F, Proposal Exceptions and/or Deviations form. The form shall be completed for each technical and/or contractual exception or deviation that is submitted by Offeror for review and consideration by OCTA.

Question 9:
Will the Time/Attendance and Workday projects be implemented simultaneously?

Response 9:
Yes, they are.

Question 10:
Will there be any need to update/fix punch data in the proposed Time/Attendance system or would this all be done in Workday?

Response 10:
In Workday.

Question 11:
Is the intent for users to only access the Time/Attendance system to clock in/out and log absences/review accruals?

Response 11:
Yes.

Question 12:
There are several requirements in the RFP surrounding reporting and analytics capabilities that would generally be done in Workday for a project like this. Is the intent to use full functionality in a Time/Attendance system or produce all of this data in Workday?

Response 12:
Reporting analytics should be reported in Workday.

Question 13:
Is the intent to continue with eleven (11) Time Clocks amongst OCTA's five (5) operational facilities? If there are to be more or less, can you please provide that information.

Response 13:
This RFP is to replace the current eleven (11) systems. If new requirements arise in the future, they will be addressed accordingly.

Question 14:
Can you please provide more information regarding the following requirement?

a. Unless otherwise agreed to by the OCTA Project Manager (PM), Consultant's staff shall be available to work onsite at OCTA's Orange, California headquarters building, bases where the time clocks will be installed, or from a pre-authorized remote location. Exceptions require OCTA's PM approval for work performed offsite or offshore. Physical on-site work is limited at OCTA.

Response 14:
This gives the OCTA PM the ability to provide Consultant a work location at OCTA bases or headquarters.

Question 15:
Will there be a need for data validation during collection of punches?

Response 15:
Yes.

Question 16:
Will there be a need for job codes or cost codes correlated to punch data?

Response 16:
No, the codes will come from Workday.

Question 17:
Will there be a need for web capabilities to clock in/clock out?

Response 17:
No, punches are in person. The devices do not need internet access, there is a time server on the network for time synchronization.

Question 18:
Is there a need to provide comments for every item on the requirements list, or can we provide additional information only as needed?

Response 18:
As needed.

Question 19:
Can OCTA please provide a copy of the IS Preferred Standards and Practices document for review?

Response 19:
See Attachment B to Exhibit A, which is attached to this Addendum No. 2.

Question 20:
What is the proposed date of award for this project?

Response 20:
OCTA expects to award the contract in February.

Question 21:
Are there additional features required not listed in RFP, such as reporting or analytics?

Response 21:
Only the functional requirements.

Question 22:
What compliances or regulatory requirements (e.g. labor laws) are to be considered?

Response 22:
This is a time clock, reporting time.

Question 23:
Please provide list of all supported PTO types (e.g., sick, vacation, PPH) and their respective rules, if unique.

Response 23:
These rules are irrelevant to reporting time.

Question 24:
Any accessibility standards (e.g., Web Content Accessibility Guidelines (WCAG)) that the interface is required to comply with?

Response 24:
The systems should not have access to the internet, will be connected by local area network (LAN) to OCTA network.

Question 25:
Is the time clock expected to support multiple languages?

Response 25:
English language only.

Question 26:
How many employees and shifts will the time clocks serve simultaneously?

Response 26:
See Response 1. There are three (3) shifts every day.

Question 27:
Is the time clock expected to support employee notifications (e.g., missing punches)?

Response 27:
No.

Question 28:
Are there specific hardware vendors or models approved for use?

Response 28:
No.

Question 29:
Is the time clock expected to integrate additional peripherals (e.g., biometric readers, printers)?

Response 29:
No.

Question 30:
What version of Workday is being used, and are there specific Application Programming Interface (APIs) or middleware for integration?

Response 30:
Version 2024R2.

Question 31:
How is syncing of punches to Workday expected to be triggered. Will it be scheduled or event based or be handled manually?

Response 31:
It can be scheduled or event based.

Question 32:
For communication between the time clock and Workday, are there encryption or authentication protocols (e.g., SSL/TLS, OAuth) required?

Response 32:
Encryption required in transit and at rest.

Question 33:
Need some information on how are badges issued, deactivated, or replaced. Is badge management expected to be part of the solution?

Response 33:
No.

Question 34:
What is the number of time clocks needed per facility?

Response 34:
OCTA has five (5) bases and require eleven (11) systems.

Question 35:
What actions are expected to be supported for administrators to perform remotely (e.g., firmware updates, troubleshooting)? And how (any specific tools or protocols to be used like, virtual private network (VPN), remote desktop protocol (RDP))?

Response 35:
Administrators should have the ability to remote to the clocks to update, check the health, troubleshoot, reset, and disable/shutdown, using RDP and VPN.

Question 36:
It is assumed that licenses for Workday integration or any third-party integration will be provided. Please confirm.

Response 36:
Yes.

Question 37:
Are there specific certifications required for time clock hardware or software to integrate with Workday's Time Tracking and Absences modules?

Response 37:
See Question and Response 36.

Question 38:
Is OCTA open to a cloud-based time management system, or is on-premise deployment required?

Response 38:
Cloud-based is preferred.

Question 39:
Will OCTA provide any resources or pre-existing network configurations for hardware installation, or should the Consultant plan to handle this entirely?

Response 39:
OCTA will provide.

Question 40:
Are there constraints or preferences regarding the physical placement of time clocks at the facilities?

Response 40:
No.

Question 41:
How many employees and administrators need to be trained, and what are their proficiency levels with similar systems?

Response 41:
Three hundred (300) employees are users and about twelve (12) administrators/clerks. All current employees use Kronos to log their punches.

Question 42:
Are there any accessibility requirements for training materials (e.g., Americans with Disabilities Act (ADA) compliance, multilingual support)?

Response 42:
Has to be ADA compliant.

Question 43:
Will OCTA provide feedback on training content, or should the Consultant propose the entire training program independently?

Response 43:
OCTA will need to work with the Consultant to determine the format, location and timing of training.

Question 44:
Are there specific expectations for response times and resolution times for maintenance issues?

Response 44:
Within an hour of acknowledging the issue and a twenty-four (24)-hour resolution.

Question 45:
Are there any predefined test cases or performance benchmarks for hardware and software validation?

Response 45:
Yes. Consultant will also need to provide cases that comply with their systems.

Question 46:
How will user acceptance testing (UAT) be conducted, and what are the criteria for final approval?

Response 46:
OCTA will work with Consultant to determine the UAT test cases to execute and then proctor the UAT but will need to have a schedule for defect resolution and re-testing.

Question 47:
Are there any restrictions or guidelines for using offshore resources, such as security or time zone requirements?

Response 47:
Offshore resource requirements are defined in the SOW.

Question 48:
Are there specific legal or regulatory requirements that the system must adhere to, such as California labor laws or accessibility standards?

Response 48:
The system would need to continue to adhere to the current legal requirements.

Question 49:
Are there requirements for system audits, data retention, or compliance reporting?

Response 49:
Yes, the requirements will be determined during the contract period.

Question 50:
Can you elaborate on the expectations for pushing punches to Workday on demand? Should this be user-initiated or automated?

Response 50:
It should be user-initiated.

Question 51:
Are there any specific integrations or dependencies outside Workday and HRIS that the time clock solution must support?

Response 51:
None.

Question 52:
Are there any lessons learned or pain points from the current Ultimate Kronos Group (UKG) system that should be considered for the new solution?

Response 52:
See the business requirements section in the SOW.

Offerors are reminded to acknowledge receipt of this Addendum No. 1 in their transmittal letters and Exhibit B, "Price Summary Sheet." All changes addressed in this Addendum No. 2 shall be incorporated into the final Agreement.

Questions regarding this Addendum No. 2 should be directed to the undersigned at raninzo@octa.net.

Sincerely,

Rhea Aninzo

Associate Contract Administrator
Contracts Administration and Materials Management

OCTA Information Systems Preferred Standards & Practices

3rd Party Non-OCTA Managed Environments

1. The Contractor shall maintain network security and confidentiality, while providing the required software and monitoring tools to ensure the network remains compliant with security standards including:
   1.1. Appropriate administrative, technical, and physical safeguards designed to protect against Information Security events; including regular security assessments made available upon request
   1.2. Compliance to the standards of applicable Data Protection Laws
   1.3. Compliance to procedures for Change Management, patching, disaster recovery, and backups
   1.4. Provision of written Information Security policies for OCTA upon request
   1.5. If required, OCTA staff shall be provided remote access to vendor-maintained data, during the contract lifetime. Upon contract completion all OCTA data shall be returned
2. Applications, data, and log backups shall NOT be maintained on the same physical media as the originals
3. Authorized users shall only access the systems using an authenticated, role-based login and be uniquely authenticated using a strong password policy
   3.1. All remote access shall be limited, documented, and protected to the greatest extent possible
4. Only privileged accounts may access and use tools with administrative capabilities, to conform to the concept of least privilege
5. The Contractor shall provide the capability to log and track user activities
6. The Contractor shall provide the capability to log and track changes to applications, databases, and operating systems
7. The Contractor shall use strong encryption methods such as Advanced Encryption Standard (AES) and/or Rivest Shamir Adelman (RSA), or an equivalent.
   7.1. Sensitive data shall be protected, both in transit and while at rest
8. When using File Transmission Protocol (FTP), the Contractor shall utilize Secure File Transmission Protocols (SFTP) for the transfer of sensitive data and/or files via interfaces and portals
9. Physical destruction or degaussing of all media storage devices that retained OCTA data shall be done before releasing the media outside of the control of the Contractor.
10. The Contractor shall immediately notify the OCTA Cyber Security team in the event (potential or real) of any incident/event resulting the loss (potential or real) of revenue, data, or security breach has occurred
11. The Contractor shall use physical and environmental security to protect all information systems and media

If Applicable

1. The Contractor shall NOT use 3rd parties unless approved by OCTA in writing and the authorization maintained by the Contractor
2. Payment Card Industry Data Security Standard (PCI DSS) Compliance
   2.1. No PCI data shall be shared with those not authorized to view or access it
   2.2. The Contractor shall ensure that no cardholder data, such as Credit Card numbers or card verification value data, is stored unless properly protected
   2.3. The Contractor shall be compliant with the PCI DSS for a Level 2 merchant or the appropriate merchant level as defined by the PCI Security Standards Council

2.4. The Contractor shall provide PCI Attestation of compliance by either a qualified Internal Security Assessors (ISA) or independent Qualified Security Assessors (QSA), or as required by PCI DSS
2.5. Quarterly vulnerability scans shall be conducted by an approved scanning vendor; including annual internal and external penetration testing results and annual Security Assessment Questionnaires (SAQs)

3. Health Insurance Portability and Accountability Act (HIPAA) Compliance

3.1 No HIPAA data shall be shared with those not authorized to view or access it

4. Personally Identifiable Information (PII) Compliance
5. 4.1The Contractor shall remain in accordance with California statutes, OCTA's privacy policy, and National Institute of Standards and Technology (NIST) best practices for general information security
6. 4.2No PII shall be shared with those not authorized to view or access it
7. 4.3The Contractor shall remain vigilant towards the protection of the confidentiality of PII in accordance with OCTA's privacy policy and California Civil Code Section 1747.08