November 28, 2023

AFFILIATED AGENCIES

Orange County Transit District

Local Transportation Authority

Service Authority for Freeway Emergencies

Consolidated Transportation Service Agency

Congestion Management Agency

Service Authority for Abandoned Vehicles

SUBJECT: Request for Information (RFI) 3-3042
"Field Operations Service Management System"

All:

The Orange County Transportation Authority (OCTA) is releasing a Request for Information (RFI) to provide an opportunity for firms to review the attached draft Scope of Work and provide information regarding currently available products or customized solutions in order to meet OCTA's objectives. OCTA would also like to receive estimates on all potential costs associated with the project.

Participation in this process is optional and no contracts will be awarded under this RFI. Please be advised that OCTA reserves the right to accept and reject any comments to the Scope of Work.

If you have any questions regarding this RFI, please contact the undersigned via email at lmartinez1@octa.net no later than 5:00 p.m. on December 5, 2023. All questions regarding this RFI must be in writing. Responses from OCTA will be posted on CAMM NET.

Please submit all RFI responses via email to lmartinez1@octa.net by **2:00 p.m., December 19, 2023**.

Sincerely,

Luis Martinez

Luis Martinez
Senior Contract Administrator
Contracts Administration and Materials Management

REQUEST FOR INFORMATION

FIELD OPERATIONS SERVICE MANAGEMENT SYSTEM

INTRODUCTION

The Orange County Transportation Authority (OCTA) is seeking information for a solution to support our field operations team. The team manages OCTA's on-street transit environment to ensure safe, courteous, and reliable service for all our customers. They correctly identify, evaluate, and communicate conditions and situations affecting bus operations. They also formulate, recommend, and implement solutions, as appropriate.

THIS IS A REQUEST FOR INFORMATION (RFI) ONLY. This RFI is issued solely for information and planning purposes – it does not constitute a Request for Proposal (RFP) or a promise to issue an RFP in the future. This RFI does not commit OCTA to contract for any supply or service whatsoever. Firms are advised that OCTA will not pay for any information or administrative costs incurred in response to this RFI. All costs associated with responding to this RFI will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future RFP, if any is issued.

BACKGROUND

OCTA is a 24 x 7 state-mandated, multi-modal transportation agency in Orange County, California. OCTA regulates, prioritizes, funds, plans, designs, builds, operates, and maintains the transportation network. This includes major highway & freeway projects, high-occupancy managed lanes, street improvements, commuter rail, streetcar, the public transit system, and paratransit services.

OCTA has locations within the County of Orange; headquarters and a conference building located in the City of Orange, and operational transport/maintenance bases in the cities of Anaheim, Garden Grove, Irvine, and Santa Ana.

OCTA currently has thirteen (13) facilities:

- Five (5) bus bases: Santa Ana, Garden Grove, Anaheim, Construction Circle in Irvine, and Sand Canyon in Irvine.
- Seven (7) transit facilities.
    - Four (4) transportation centers: Fullerton, Goldenwest, Laguna Hills, Newport Beach
    - Two (2) park & ride lots: Brea, Fullerton
    - One (1) OCTA employee restroom at the Tustin Metrolink station
- Fifty-five (55) fixed-route bus lines.
- Over 6,500 active Bus Stops (and 2,000 inactive Bus Stops).

OCTA will be adding eight (8) streetcars, and one (1) central communications facility in the upcoming two (2) – four (4) years. There are two (2) physical warehouses that are operated by OCTA, and three (3) warehouses operated by OCTA contractors.

OCTA is currently using an OCTA developed application for the solution requirements listed below.

PURPOSE STATEMENT

The objective of this RFI is to get a broad overview of available solutions in the marketplace for a robust, easy to use system to support field operations. As such, the requirements are merely an expression of the intent, not a restrictive list of must-have requirements.

REQUEST FOR INFORMATION

The proposed solution should include an overview of the functionality, cost of equipment and software licensing, and average time to implement.

1. SOLUTION REQUIREMENTS

OCTA is looking for a solution for field supervisors to document every minute of their work while they are managing and supporting OCTA's on-street transit environment. The information they document includes activities related to tracking the timing of buses out on the routes, logging departure and arrival times of buses, inspection of bus stops and detours, and activities in support of the coach operators.

a. A solution that allows users to record their activities throughout the day for their entire workday.

b. A solution that allows users to monitor if buses are running on time by logging the exact time the buses arrive at bus stops. This should include an easy-to-use function to log the exact time of arrival, such as a click of a button.

c. A solution that allows users to monitor and log the times when buses depart the terminals, arrival times and departure times at the bases. This should include an easy-to-use function to log the exact time, such as a click of a button.

d. A solution that allows users to document conditions of detours along a bus route, such as appropriate signage, start date and end date of the detour, hours of the detour, bus stops impacted, and notes.

e. A solution that allows users to document conditions of a bus stop such as date of inspection, notes of inspection, check frequency, validity period of these inspection notes (start date/end date).

f. A solution that allows users to document notes when they provide mentoring to coach operators with details such as name of coach operator, badge number, location, date/time, bus route information and notes about the mentoring provided to the coach operator.

g. A solution that allows users to record if a bus had to sit idle and for how long.

h. A solution that allows users to record vehicle defects as a result of the vehicle inspection before they take out the vehicle each morning.

i. A solution that allows for monthly goals for each type of activity and reports whether each user is on track for the monthly goal for each type of activity.

j. A solution that interfaces with an in-house application for documenting office performance observation and disciplinary actions for coach operators.

k. A solution that can interface with external systems to display bus route schedules, specific bus runs (bus number, line, coach operator, expected arrival and departure at each point).

2. TECHNICAL REQUIREMENTS

A solution where the infrastructure and peripherals are agnostic, not dependent on applications. Refer to Attachment E for OCTA's Information Systems' Technology Standards.

3. PROPOSED PROJECT SCHEDULE

For the purpose of the RFI, provide an estimated project schedule with the phases and the high-level tasks. Tasks could be grouped into the project phases.

Example project schedule:

Project Implementation Effort	**Duration**
Task 1 (Project Planning & Management)	
Task 2 (Requirements Gathering)	
Task 3 (Design)	
Task 4 (Construct / Build)	
Task 5 (Test)	
Task 6 (Train)	
Task 7 (Deploy)	
Task 8 (Post-Deployment Support / Warranty)	

4. COST and PRICE ESTIMATES

Please provide cost and price estimates for the functionality included below in attachments A through D.

EXHIBIT A - ATTACHMENT A

COST AND PRICE SUMMARY SHEET

Enter below the cost and price estimates for the functionality described in this RFI. Prices shall include direct costs, indirect costs, profits, and tax.

SOLUTION COSTS	Cost	Comments
Application Software/Licensing *	$	(This should represent the cost for the core software, SaaS Subscriptions, and/or Licensing.)
Third Party Software (if applicable) *	$	(This should represent the cost for any 3rd-party software that is required to support the system.)
Project Implementation Effort	$	(The total cost for the project implementation effort should be the sum of the costs of all Tasks 1-8.)
Task 1 (Project Planning & Management)	$	
Task 2 (Requirements Gathering)	$	
Task 3 (Design)	$	
Task 4 (Construct / Build)	$	
Task 5 (Test)	$	
Task 6 (Train)	$	
Task 7 (Deploy)	$	
Task 8 (Post-Deployment Support / Warranty)	$	
TOTAL COST of PROJECT IMPLEMENTATION EFFORT	$	
Support, Maintenance, Warranty	$	(OCTA expects this solution to be used as a production system for at least one (1) or two (2) years after completion of the implementation effort.)
Environment (if applicable)	$	(Hosting Services, or On-Premise hardware costs.)
Software and Technical Components	$	(Include details in Attachment D)
Travel and Expenses (if applicable)	$	(Shall be budgeted as a firm-fixed amount based on a calculated number of trips. Please provide the number of trips. OCTA will only pay for trips that are actually travelled.)
Other Costs (if applicable)	$	(If there are other costs, please identify what such costs would be.)
GRAND TOTAL	**$**	(This amount should reflect the Grand Total for the expected implementation, plus one (1) or two (2) years as a production system.)

*Provide the software(s), 3rd party software, and any unique technical components that are necessary to support the solution in the "List of Software and Technical Components" table in Attachment C below.

EXHIBIT A - ATTACHMENT B

PROFESSIONAL SERVICES RATE SCHEDULE

RESOURCE	Fully-Burdened Hourly Rate *	Comments
Program Manager		
Project Manager		
Architect		
Engineer / Developer		
Business Analyst		
Trainer		
QA		
…		

*These rates would be used for approved change requests.

EXHIBIT A - ATTACHMENT C

LIST OF SOFTWARE AND TECHNICAL COMPONENTS

Ref	Software or Technical Component Name	Software or Component's Vendor	High-level Purpose	Integration Complexity & Level of Effort	**Use or Acquisition Costs** (for software, include installation & interface development costs)
A	*Application Software: core software*				$
B	*(example: 3rd party software ABC)*				$
C	*(example: 3rd party software XYZ)*				$
D					$
…					$
	TOTAL for SOFTWARE and TECHNICAL COMPONENTS				**$**

EXHIBIT A - ATTACHMENT D

LIST OF SUGGESTED ENHANCEMENTS

The List of Suggested Enhancements should be reflected in the table below.

CONSULTANT-SUGGESTED ENHANCEMENTS	Cost	Comments*
(example: enhancement #1)	$	
(example: enhancement #2)	$	
	$	
	$	
TOTAL	**$**	

Please include in comments, the future path of R&D (What are the features of the next substantial release / upgrade and when it will be happening?).

EXHIBIT A - ATTACHMENT E

OCTA INFORMATION SYSTEMS' TECHNOLOGY STANDARDS

Purpose

This document provides a high-level description of Orange County Transportation Authority's (OCTA) computing environment and indicates the Information Technology (IT) tools on which OCTA has standardized. This document does not address standard practices and methodologies used by OCTA's Information Systems department.

All IT related initiatives or product procurements are evaluated partially on their compliance with the standards listed herein. Based on criteria such as support expectations and the level of integration required with other systems, some standards may be more strictly enforced than others.

Technology standardization is a key component to controlling costs, ensuring quality, enabling compatibility, and retaining stability. Standardization is also a key to the Information Systems department (IS) in achieving many of the desired improvements in its services produced for the Authority. OCTA has adopted many of the viable, mainstream product lines from viable, mainstream vendors to position OCTA in a non-proprietary, widely supported, and manageable Information Technology environment. These standards provide a framework within which the majority of computing needs can be met with the best possible mix of equipment, software, and support given existing resources.

Scope

This guide is for use by all personnel, including contractors, who are responsible for or involved in the development of OCTA's general support systems and major applications. This guide is intended to assist them in determining and applying the relevant standards to the system and applications.

This guide sets out the standards by which the IT infrastructure is designed and operated and lists the technologies and products that promote transition from the current technical architecture to the envisioned technical architecture. OCTA uses the Minimum Mandatory Compliance Technologies table as the basis for the technology and products guide.

Audience

This information Systems Technology Standards document is intended to serve as specification guidelines for the purchase of new information systems and software tools. The intended audience would be prospective vendors providing such systems of tools.

References

Information Systems' Technology Business Plan (ISTBP)

Section 6 – Information Systems' Information Technology Investment Plan (ISTIP)

Network Infrastructure and Architecture

OCTA has established a well-defined data and voice communication infrastructure known as the OCTA Network. Principle equipment for OCTA Network hardware is located at OCTA's main administrative office in Orange. In addition, servers, desktops, LAN/WAN, and telecommunication equipment are located at four satellite sites.

Technology Standards Concepts and Strategies

The Standards of most importance to OCTA are the database platforms, operating system platforms, server, desktop, mobile computer hardware, mobile devices and core network infrastructure hardware. Together, these elements form the foundation for OCTA's computing infrastructure upon which the majority of OCTA's business systems are constructed and deployed. Information Systems focuses training and maintenance investments on these foundational technologies to provide the necessary support that each requires. Most of these technologies are the more costly to skill for out of all the technologies used at OCTA. The strategy to maintain this foundation represents a balanced approach that allows for flexibility and variation in IT solutions while allowing OCTA to maintain a manageable set of core technologies and the skills required to support them.

General minimum mandatory compliance for these most important standards is indicated below in Table 1. Adherence to OCTA's computing standards will be evaluated for any IT related acquisition, hardware and software. Response to non-standard elements will be measured in the overall context of a project or initiative. OCTA understands the application of technology standards cannot always be a "cookie-cutter" exercise. Criteria such as functional-fit of a proposed solution relative to others, level of integration required, or the uniqueness or sole-solution nature of a system must be weighed against the value of maintaining standards.

In Information Systems' opinion, the standards communicated herein provide a very flexible starting point to address the majority of all computing needs while providing the best possible mix of equipment, software, stability, and support, given existing resources. Once solutions' benefits, architectures and relative value are understood, efforts can be directed at understanding what is required to bring any non-compliant portion of solutions into compliance. Then it can be decided if the benefits of doing so justify strict enforcement of stated standards versus investing in or arranging for means of support for non-standard technologies.

Information Security Practices:

In today's fast paced technology dependent environment, businesses must balance their needs to quickly deliver innovative products and services with public safety and security considerations in mind. Not only does the public demand better security for the products and services provided by OCTA, but there are also many federal, state, and industry regulations that requires us to provide a certain level of protection or provides us with guidance and best practices.

The following is a brief list of the major federal, state, and industry information security regulations that can be applicable to some OCTA systems and data:

- **Health Insurance Portability and Accountability Act (HIPAA):** Requires agencies to protect the privacy of individually identifiable health information.
- **California Senate Bill 1286 (SB1386):** Requires agencies that own or license computerized personal information to disclose any breach of security.
- **California Assembly Bill 1950 (AB1950):** Requires agencies that own or license personal information about a California resident to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use , modification, or disclosure.
- **California Assembly Bill 2246 (AB2246):** This bill would require a business to ensure the privacy of a customer's personal information.
- **Payment Card Industry – Data Security Standard 3.0:** The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- **CA Senate Bill 327:** IoT Information Privacy
- **California Consumer Privacy Act (CCPA):** California Personal Information (PI)
- **Business and Professions Code (BPC) Chapter 22:** Internet Privacy Requirements 22575-22579

The Authority security policies are based on guidance from the NIST 800-53 – Security and Privacy Controls

To help meet the demands of our community and address our compliance requirements, the Authority recommends that prospective vendors include an explanation of security characteristics of their products or service offerings. Furthermore, we recommend that vendors specify how their products and service offerings address and help support the Authority's commitment to a secure and compliant environment.

During times of transitions between standards, IS will make a judgment on what to specify, the retiring standard versus the new standard.

Minimum Mandatory Compliance Technologies

TABLE 1: Minimum Mandatory Compliance for Key Technologies

Category	Minimum Mandatory Compliance
Relational Database Software	• Microsoft SQL Server 2019 (preferred) or Oracle (Linux and Windows)
Server Operating Systems	• Microsoft Windows Server 2022 or greater (preferred) or RedHat Enterprise Linux (RHEL) 7.9 or greater (preferred)
Server-Class Computers	• VMWare (Datrium) Hyper Converged Infrastructure, Hewlett Packard Enterprise Servers
Desktop / Workstation / Laptop Operating Systems	• Microsoft Windows 10 or greater
Desktop / Workstation Computers Laptop Computers, tablets	• Lenovo, MS Surface 7 or greater and IOS devices 14 or greater
Network Infrastructure Hardware	• Cisco and Aruba (wireless)
Publishing Applications	• Web enabled or Citrix
Software Distribution Systems	• Microsoft SCCM
Telecommunications	• Microsoft Teams
E-Mail	• Microsoft Exchange Online Office 365
Copiers	• Kyocera
Server Virtualization	• VMWare
Storage Area Network	• VMWare (Datrium), Hewlett Packard Enterprise (Nimble) Storage
Printers	• Hewlett Packard
Browsers	• Latest Edge, IE, and Chrome
Collaboration and enterprise content management	• SharePoint 2019
MFA and SSO	• Microsoft Azure AD
Remote Systems/Connections	• No 3rd party systems will be joined to the OCTA domain or initiate remote access. All remote access, data pulls, or data pushes will be initiated from within the OCTA network.

Application Architecture

The Authority has a guiding philosophy to purchase commercial off-the-shelf (COTS) software solutions whenever possible, and to contract third party custom development when a suitable COTS solution is not available. Multi-tier client/server or web based using .NET architecture is our preferred standard for custom application development projects at the Authority.

For developing custom software applications within OCTA infrastructure, the Authority has defined certain tools and preliminary guidelines noted by tier. The guidelines are indicated per tier in Table 2 below. Any deviations from these tools and requirements must be brought to the Authority's attention and approved by the Authority before any work effort is expended.

Table 2: Custom Application Development Guidelines

Tier	Guidelines
1 Client	• Use no proprietary client-side executables. If application access is ever extended beyond the boundaries of OCTA's network, any browser could be used resulting in the same application experience being achieved. • Custom software should be agent-less or client-less therefore browser-based architectures are preferred. • Avoid software dependencies for client-side environment variables if possible (reliance upon native support components residing on the client is not recommended). • Refrain from using older database connectivity techniques if at all possible (e.g. JDBC, ActiveX, etc.) • Any customized or program-specific scripting needs to be fully signed (unsigned scripting is not acceptable). • Java is not a preferred solution. Refrain from using Java Applets or JIT Compiler (machine code) calls that are dependent on legacy Java platforms. Any Java used should be fully compliant with current versions of Java that are available at the time the program is compiled (extra effort should be placed toward only using logic that is not scheduled for obsolescence or will be unsupported in the future versions of Java). • Minimize locating or executing any business logic on the client side. Any such practice shall only be with the agreement of the Authority. • Ensure that development activities are coordinated throughout the Authority and that developed applications can be fully integrated into the production environment without impacting existing applications. • Periodic code reviews may be required.
2 Application Server	• Perform all logic execution on the server-side. • ODBC connectivity to compliant database. • Periodic code reviews may be required.
3 Database	• Refrain from using low-level DBMS (e.g. MS Access) as opposed to SQL Server or Oracle. • Standard SQL for stored procedures, triggers, functions, etc. • Periodic code reviews may be required.

IS Best Practices

The following best practices should be considered to appropriately engineer and plan for technical solutions when working with OCTA. These best practices may not be applicable for all solutions but should be used to provide guidance to minimize incompatibility and rework when designing solutions for OCTA.

1. 3rd Party Hosted Environments
    a. 3rd party hosted environments should comply with OCTA "IS Preferred Standards & Practices" section, as applicable.
    b. Containerized applications are preferred for Cloud solutions.
    c. For the purpose of guidance, Service Organization Controls (SOC) 2 attestations are the preferred *minimum* control platform, but OCTA follows the NIST 800-53 framework.
2. OCTA Credential Validation for 3rd Party Hosted Environments
    a. Credential validations should utilize Microsoft Azure AD, rather than OCTA's on-prem Active Directory Domain Controllers.
    b. Microsoft Azure Single Sign-On (MS SSO) is the preferred SSO solution.
3. OCTA to 3rd Party Connections
    a. 3rd party systems or networks will not be joined to the OCTA network.
    b. If there is a requirement to transfer data from OCTA to a 3rd party network, it is preferred that data be transmitted from an OCTA system within our DMZ via VPN tunnel.
4. 3rd Party to OCTA Connections
    a. No 3rd party systems will be joined to the OCTA domain or initiate remote access. All remote access, data pulls, or data pushes will be initiated from withing the OCTA network.
    b. All OCTA internal remote access should use OCTA Citrix servers, whenever possible.
    c. 3rd party vendors utilizing OCTA credentials should employ Multi-Factor Authentication (MFA) and Single Sign On (SSO) via Microsoft Azure AD.
    d. Administrative level privileges will NOT be granted at the system/network level for OCTA managed systems.

IS Preferred Standards & Practices

The following preferred standards and practices should be considered to appropriately engineer and plan for technical solutions when working with OCTA. These are preferred standards and practices that may not apply to all solutions.

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:
    a. Appropriate administrative, technical, and physical safeguards designed to protect against Information Security events; including regular security assessments made available upon request.
    b. Compliance to the standards of applicable Data Protection Laws.
    c. Compliance to procedures for Change Management, patching, disaster recovery, and backups.
    d. Provision of written Information Security policies for the Agency upon request.
    e. If required OCTA staff shall be provided with remote access to vendor-maintained data, during the contract's lifetime. Upon contact completion all OCTA data should be returned.
2. Applications, data, and log backups should NOT be maintained on the same physical media as the originals and properly encrypted and protected.
3. Authorized users should only access the systems using an authenticated, role-based login and be uniquely authenticated using a strong password policy.
    a. All remote access should 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 should provide the capability to log and track user activities.
6. The Contractor should provide the capability to log and track changes to applications, databases, and operating systems.
7. The Contractor should use strong encryption methods such as AES and/or RSA, or an equivalent.
    a. Sensitive data will be protected, both in transit and while at rest.
8. When using File Transmission Protocol (FTP), the Contractor should 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 have retained Agency data will be done before releasing the media outside of the control of the Contractor.

10. The Contractor should immediately notify the Agencies 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 should use physical and environmental security to protect all information systems and media in their environment.

If Applicable

12. The Contractor should NOT use 3rd parties unless approved by the Authority in writing and the authorization maintained by the Contractor.
13. PCI DSS Compliance
    a. No PCI data should be shared with those not authorized to view or access it.
    b. The Contractor should ensure that no cardholder data, such as Credit Card numbers or card verification value data, is stored unless properly protected.
    c. The Contractor and the BOS should be compliant with the PCI DSS for a Level 2 merchant, or the appropriate merchant level as defined by the PCI Security Standards Council.
    d. The Contractor should provide PCI Attestation of compliance by either a qualified ISA or an independent QSA, or as required by PCI DSS.
    e. Quarterly vulnerability scans should be conducted by an approved scanning vendor; including annual internal and external penetration testing results and annual Security Assessment Questionnaires (SAQs).
14. HIPAA Compliance
    a. No HIPAA data should be shared with those not authorized to view or access it.
    b. Systems containing health information should be properly protected per applicable requirements.
15. PII Compliance
    a. The Contractor should remain in accordance with California statutes, the Agencies' privacy policy, and National Institute of Standards and Technology (NIST) best practices for general information security.
    b. No PII should be shared with those not authorized to view or access it.
    c. The Contractor should remain vigilant towards the protection of the confidentiality of PII in accordance with the Agencies' privacy policy and with the California Civil Code Section 1747.08.