SOLICITATION ADDENDUM

Solicitation Number:	RFP 2020-1504
Solicitation Description:	Service Reliability Analysis Software
Solicitation Due Date and Time:	02 July 2020
Addendum Number:	#1
Addendum Date:	24 June 2020
Purpose of Addendum:	Respond to Submitted Questions
Contract Contact:	Eslyn Tripuraneni, Contracts Specialist etripuraneni@actransit.org | 510.891.5434

The Alameda-Contra Costa Transit District herewith issues this Addendum No. #1 to the above-referenced *Request for Proposals*. **Except as modified below, all other terms and conditions remain in effect. Strikethrough text represents deletions from the original RFP, and* ***bold/italicized/underlined text*** *represent additions to original RFP text.*

INSTRUCTIONS

1. Return one (1) properly executed copy of this Addendum with proposal submission. Failure to sign and return this Addendum may result in the rejection of Offeror's proposal.
2. Carefully read, review and adhere to all notices, instructions and changes to the RFP in this Addendum.
3. Following are the District's revisions to the RFP:

QUESTIONS AND CLARIFICATIONS

Question 1: Per Section C, part 2 ("In order to ensure your full response is evaluated, you must also provide a flash drive and two (2) hard copy versions of the Technical and Price Proposals") should these materials be delivered to the District's General Office (1600 Franklin Street, Oakland, California 94612)? By what date and time must these materials be received in order for the full response to be evaluated (is it the same as the deadline for electronic submission, 02 July at 4pm PDT?) Will the District accept proposal materials dropped off by the Offeror or only by mail?

- Response: Yes, the same deadline applies for all methods of proposal delivery. The materials may be dropped off at the District's General Office location address (to the Security Desk addressed to the SPC). All submissions in response to this RFP, must be received by the submission due date. *No late submissions will be accepted. Incomplete submissions may be deemed nonresponsive.*

Question 2: Section C part I states that any requested contract exceptions must be submitted to the District during the Questions/Requests for Clarification period (by 6/24/20). Given that that deadline is very short for full legal review, would it be possible to extend the deadline for submitting potential exceptions, to provide time for review of Exhibit 1 by our legal counsel?

- Response: No; please reference *Section C, Part 3, No. 5*, any exceptions must be submitted with the Proposal.

Question 3: Tab 4 includes Attachment E, Cloud Questionnaire, as a requirement. Where can we locate the Cloud Questionnaire for inclusion?

- Response: Attached please find *Attachment E, Cloud Questionnaire*.

Question 4: What is the total number of vehicles in the District's fleet, which are included in the AVL data to be included in this contract??

- Response: There are currently 626 vehicles in the District's fleet. Please note this information is based on current information only and may be subject to change.

EXHIBIT E – CLOUD QUESTIONNAIRE

AC TRANSIT
CLOUD SECURITY QUESTIONNAIRE

	NETWORK/SECURE ISOLATION
1	Provide a proposed architecture document which includes a full network diagram of the proposed AC Transit, illustrating the relationship between the AC Transit and any other relevant networks (include ports/protocols). Must support 3-tier architecture - Public layer, App layer and DB layer.
2	Provide a data flowchart that details where AC Transit data resides (including backup processes), what data will be collected (data inventory), data fields required, and the applications that manipulate the data.
3	Does your company require virtual Firewalls to be installed at the VM level so that network traffic moving in and out of VM's can be controlled?
4	Does your company implement Memory Virtualization not to exceed physical memory capacity?
5	Explain how customer data is either physically or logically separated from your other customers.
6	Is the cloud solution a single-tenant and/or shared (multi-tenant) cloud service?
7	Do you share networks, VPNs, firewalls and load balancers between your dedicated and public cloud environments?
8	Does your company require the use of two (2) factor authentication for the administrative control of servers, routers, switches and firewalls?
9	Does your company support Secure Sockets Layer (or other industry-standard transport security) with 128-bit or stronger encryption and two-factor authentication for connecting to the application?
10	Does your company provide redundancy and load balancing for firewalls, intrusion prevention and other critical security elements?
11	Does your company perform, or have a third-party perform, external penetration tests at least quarterly, and internal network security audits at least annually?
12	Does your company contract for, or provide protection against, denial-of-service attacks against its Internet presence?
	PLATFORM
13	Does your company have a documented policy for "hardening" the operating system under the Web and other servers?
14	Does your company have validated procedures for configuration management, patch installation, and malware prevention for all servers involved in SaaS delivery?
15	Does your company document set of controls to ensure the separation of data and security information between customer applications?
16	Does your company monitor web servers for OWASP Top 10 Vulnerabilities?
17	Does your company provide reporting of web servers on ninety (90) day trend graphs, depicting critical and high severity vulnerabilities discovered over the past six (6) months?
	DATA PROTECTION
18	Describe how you review the security of applications such as ActiveX controls and Java applets.
19	Describe how you ensure content monitoring and filtering.
20	Describe what data leak prevention processes and controls are in place to detect inappropriate data flows.
21	Provide documented procedures for configuration management, including installing security patches, for all applications.
22	Define how you implement TPM to securely store and compare platform measurements including hypervisors, O/S, BIOS and ensure security validation and protect from malware and rootkits.
23	Does your company use Hardware Security Module (HSM) to store and manage encryption keys?
24	Does your company create a SHA/MAC hash of the Operating System and store it in the HSM for future comparison?
25	Does your company subscribe to an attestation service to ensure that only protected environment is invoked using TPM?
26	Does your company protect cloud platform resource pool via trusted resource pools and use of TPM's, Code signing, geotagging, security status?
	SECURITY
27	What actions do you take after identifying a security issue? Define "security issue" as it relates to your cloud solution.
28	Do you have an incident response plan? Will you provide a copy? Provide incident response history or examples.
29	Explain how you notify a customer in the event of a breach or security issue?
30	Do you have a formal Risk Analysis plan and review it annually? Provide a copy for review.
31	Do you have a Disaster Recovery plan, and what tests do you perform on your disaster recovery plan? Describe the maximum downtime limits: RPO and RTO objectives.
32	What are the contract stipulations regarding potential customer losses and/or for transfer of data and support to another organization should the business fail?
33	Does your company implement an Authentication Gateway Service as a reverse proxy front end between consumer and the cloud?
34	Does your company implement an Authentication Gateway Service and an IAM system to authenticate and authorize users?
35	Does your company implement a Secure Token Service type authorization to the IAM users (also SSO) and integrate with logging and monitoring service?
36	Does your company implement a Certificate Validation Service to check for certificate revocation?

	SERVICE LEVEL AGREEMENTS
37	Monthly Uptime for Cloud Services - 99.9% or higher (excluding scheduled down time)
38	Monthly Uptime for Virtual Machines - 99.9% or higher (excluding scheduled down time). Ensure that total memory capacity of all the virtual machines put together does not exceed the memory capacity of the physical host.
39	Network Availability - 99.9% or higher
40	Storage and Data Availability - 99.9% or higher
41	Data Retention - Full secure backup and snapshot of the database, file system, log files, and source codes on a daily basis. Copy should be retained for at least sixty (60) days onsite and seven (7) years in an offsite location.
42	IT Support Availability - Vendor should provide IT Support, 24x7 and 365 days of the year.
43	Response Time to Error - If customer reports a problem, vendor must respond within thirty (30) mins and kick off the investigation of the problem immediately.
44	Recovery Time Objective -All components must be able to recover within thirty (30) minutes of a disaster to the data center.
45	Cryptography Keys - At a minimum, AES 256-bit symmetric key and RSA 2048 bit for asymmetric key must be used where cryptographic protection is used for resources.
46	Encryption - Data will be encrypted at rest and in transit at all times. The keys identified in the SLA shall be secured in the Hardware Security Module (HSM) and should have a minimum of 99.9% availability. Certification Validation Service and other crypto services shall all have at least 99.9% availability.
47	Resiliency - Hypervisor clustering to be used for all hypervisors.
48	Attestation Service - A daily report on the security status of the virtual machines and other components shall be made available.
49	Authentication and Authorization - Support for LDAP authentication service and other authorization service should be available. Industry standard protocols like OAuth or SAML shall be used for authentication and authorization purposes. AC Transit may require an ability to control and configure the authorization roles, profiles, and rules directly for its clients and administrators. All transactions shall be captured in logs and made available for AC Transit administrator viewing, if requested within twenty-four (24) hours.
	Insurance
50	Do you carry Cybersecurity Insurance? If yes, please provide a copy of the declarations from the insurance policy.

Acknowledgment of Addenda

The undersigned acknowledges receipt of the following addenda to the bidding document: Addendum #1. The completed acknowledgement of addenda form should be returned with bid response package; not sent to the District separately. *** NOTE: Failure to acknowledge receipt of all addenda may cause the bid to be considered non-responsive to the solicitation. Acknowledged receipt of each addendum must be clearly established and included with the bid.*

____

Name of Proposer

____

Street Address

____

City, State, Zip

____

Signature of Authorized Official

____

Date