



**ADDENDUM NO. 2
ALAMEDA CTC RFP NO. R22-0009
ELECTRONIC TOLL SYSTEM INTEGRATION
SERVICES FOR EXPRESS LANES OPERATED BY ALAMEDA CTC**

April 15, 2022

Request for Proposals (RFP) No. R22-0009 is modified as set forth in this Addendum No. 2. The original RFP remains in full force and effect, except as modified by this Addendum, which is hereby made part thereof and subject to all applicable requirements hereunder as if originally shown and/or specified. Proposers shall take this Addendum into consideration when preparing and submitting proposals.

The RFP is hereby revised per the following:

- 1. The following shall be added to the end of RFP Appendix E (Sample Agreement):**

Appendix G to Sample Agreement

Special Conditions Relating to Personally Identifiable Information

To the extent that CONTRACTOR will have access to personally identifiable information (“PII”) in connection with the performance of this AGREEMENT, such access shall be governed by this Appendix G. PII is any information that is collected or maintained by CONTRACTOR that identifies or describes a person or can be directly linked to a specific individual. Examples of PII include, but are not limited to, name, address, phone or fax number, signature, FasTrak[®] account number, credit card information, toll tag number, license plate number, and travel pattern data. The following special conditions related to the confidentiality and use of PII apply to this AGREEMENT, but only with respect to PII related in any way to FasTrak[®] or Express Lanes:

- 1. Right to Audit**

CONTRACTOR shall permit ALAMEDA CTC and its authorized representatives to audit and inspect: (i) CONTRACTOR’s facilities where PII is stored or maintained, including third party hosting or service provider systems; (ii) any computerized systems used to share, disseminate or otherwise exchange PII; and (iii) CONTRACTOR’s security practices and procedures, data protection, business continuity and recovery facilities, resources, plans and procedures. The audit and inspection rights hereunder shall be for the purpose of verifying CONTRACTOR’s compliance with this AGREEMENT, and all applicable laws.

For a third-party multi-tenant cloud service (e.g. Microsoft Azure or Amazon Web Services), CONTRACTOR’s obligation to permit an audit for its third-party multi-tenant cloud service shall be satisfied by the provision of the cloud service’s most recent third party audit compliance, certifications and assurance results for the PaaS and SaaS offerings, including ISO 27001, SSAE 16 or 18 SOC 1, SOC 2, SOC 3, PCI-DSS, and FedRAMP as applicable.

2. Protecting PII

All PII made available to or independently obtained by CONTRACTOR in connection with this AGREEMENT shall be protected by CONTRACTOR from unauthorized use and disclosure through the observance of adequate security measures consistent with industry standards and technology best practices. This includes, but is not limited to, the secure transport, transmission and storage of data used or acquired in the performance of this AGREEMENT. All PII shall be encrypted during transport, transmission and in storage.

CONTRACTOR agrees to properly secure at all times any computer systems (hardware and software applications), third party hosting or cloud services, or electronic media that it will use in the performance of this AGREEMENT, and shall ensure that any third-party hosting or service providers with access to PII adhere to the terms of this Appendix A. This includes ensuring all security patches, upgrades, and anti-virus updates are applied as appropriate to secure PII which may be used, transmitted, or stored on such systems in the performance of this AGREEMENT.

Notwithstanding anything to the contrary in this AGREEMENT, CONTRACTOR agrees to retain PII for no longer than the timeframes specified in subsections (c) and (d) of Street and Highways Code Section 31490. At the conclusion of this retention period, CONTRACTOR agrees to use purge methods described in National Institute of Standards and Technology (NIST) Special Publication 800-88, as may be revised or superseded (“NIST Publication”) to remove PII from any files. Discarded PII will be unavailable and unrecoverable following the purge on any storage media including, but not limited to, magnetic disk, optical disk, memory chips, cloud storage, or other computing system (“Storage Media”). CONTRACTOR agrees to destroy hard-copy documents containing PII by means of a cross-cut shredding machine. CONTRACTOR also agrees to use purge or destroy methods, as described in NIST Publication, to sanitize any Storage Media prior to disposal (including selling, discarding, donating, transferring, and abandoning). At the conclusion of the performance period of this AGREEMENT, CONTRACTOR shall submit a certification to the ALAMEDA CTC Project Manager as follows: “All PII whether in electronic or hard-copy format, has been destroyed in accordance with the requirements contained in Section 2. Protecting PII of Appendix G, Special Conditions Relating to Personally Identifiable Information.” These requirements shall survive termination or expiration of this AGREEMENT.

3. Compliance with Statutes and Regulations

CONTRACTOR agrees to comply with all applicable statutes, rules, regulations and orders of the United States, the State of California and BATA relating to the handling and confidentiality of PII, including but not limited to Streets and Highways Code Section 31490.

4. Contractor Guarantees

CONTRACTOR shall guarantee the following:

CONTRACTOR shall not, except as authorized by ALAMEDA CTC or required by its duties by law, reveal or divulge to any person or entity any PII which becomes known to it during the term of this AGREEMENT.

CONTRACTOR shall not use or attempt to use any such information in any manner which may injure or cause loss, either directly or indirectly, to BATA or ALAMEDA CTC.

CONTRACTOR shall not use or process PII for any purpose other than performance of the scope of work set forth in this AGREEMENT.

CONTRACTOR shall ensure that all PII that is stored, processed, or transmitted is encrypted, using at least then-current best industry practices (or encryption methods mandated by law, whichever provides higher levels of protection).

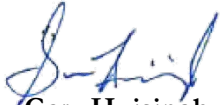
CONTRACTOR shall comply, and shall cause its employees, representatives, agents and contractors to comply, with such directions as ALAMEDA CTC may make to ensure the safeguarding or confidentiality of PII.

CONTRACTOR shall, if requested by BATA or ALAMEDA CTC, sign an information security and confidentiality agreement provided by BATA or ALAMEDA CTC and attest that its employees, representatives, agents, and contractors involved in the performance of this AGREEMENT shall be bound by terms of a confidentiality agreement.

5. Notice of Security Breach

Each party shall immediately notify other party when it discovers that there may have been a potential breach in security which has or could have resulted in unauthorized access to PII. For purposes of this section, immediately is defined as within two hours of discovery. The parties' contacts for such notification are the CONTRACTOR Project Manager and the ALAMEDA CTC Project Manager identified in this AGREEMENT.

Approved for issuance:



Gary Huisingsh
Deputy Executive Director of Projects