



**CONTRACT NO. 500178
(EMERG 806613)**

FARE SYSTEM REPLACEMENT

CONTRACTOR:

Cubic Transportation Systems
9233 Balboa Ave
San Diego, CA 92123
858-268-3100
karim.elsharnouby@cubic.com

AWARD DATE:

August 21, 2024

CONTRACT TERM:

One year from Notice to Proceed (NTP)

NOT TO EXCEED AWARD AMOUNT:

\$3,565,200.00

PROJECT MANAGER:

Jonathan Tanzer
512-369-6053
jonathan.tanzer@capmetro.org

CONTRACT ADMINISTRATOR:

Jeffery Yeomans
512-369-7727
jeffery.yeomans@capmetro.org

PROCUREMENT DEPARTMENT
CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY
2910 E. 5th STREET
AUSTIN, TEXAS 78702




CONTRACT 500178
(EMERG 806613)

FARE SYSTEM REPLACEMENT

TABLE OF CONTENTS

ITEM	DESCRIPTION
	AWARD/CONTRACT FORM
1	EXHIBIT A - PRICING SCHEDULE
2	EXHIBIT B - REPRESENTATIONS AND CERTIFICATIONS
3	EXHIBIT E-Revised-1 - CONTRACTUAL TERMS AND CONDITIONS
4	EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX
5	EXHIBIT G – AUTHORIZATION OF WORK PRODUCT
6	EXHIBIT H -Revised-1- IT PROPRIETARY RIGHTS AND DATA SECURITY ADDENDUM
7	EXHIBIT I-Revised-1 - IT ACCESS AND USE AGREEMENT
8	EXHIBIT L-Revised-1 - WARRANTY AND SERVICES AGREEMENT
9	UMO SERVICES AGREEMENT

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY AUSTIN, TEXAS		
AWARD/CONTRACT FORM		
1. SOLICITATION NO: EMERG 806613	2. CONTRACT NO: 500178	3. EFFECTIVE DATE: Upon Execution
4. CONTRACTS ADMINISTRATOR: Jeffery Yeomans		PHONE: 512-369-7727
5. SHIP TO ADDRESS:	6. DELIVERY TERMS:	
Capital Metro 2910 East 5 th Street Austin, Texas 78702	F.O.B. Destination	
7. DISCOUNTS FOR PROMPT PAYMENT: N/A		
8. CONTRACTOR NAME & ADDRESS:	9. REMITTANCE ADDRESS:	(If different from Item 8)
Cubic Transportation System 9233 Balboa Ave. San Diego, CA 92123		
PHONE: 858-268-3100	EMAIL: karim.elsharnouby@cubic.com	
10. DBE GOAL: Not Applicable		
CONTRACT EXECUTION		
CAUTION: A false statement in any bid or proposal submitted to CMTA may be a criminal offense in violation of Section 37.10 of the Texas Penal Code.		
<input checked="" type="checkbox"/> NEGOTIATED AGREEMENT:	(Contractor is required to sign below and return to the Contracting Officer within three (3) calendar days of receipt.)	
SIGNATURE OF CONTRACTOR:		
Name/Title: Frank Capone, Contracts Manager Signature: <u>Frank Capone</u> Date: August 21, 2024		
<input checked="" type="checkbox"/> AWARD:	Items listed below are changes from the original offer and solicitation as submitted.	
This Award/Contract Form may be executed in multiple originals, and an executed facsimile or email copy shall have the same force and effect as an original document.		
ALTERATIONS IN CONTRACT: Changes are as follows:		
<p>The following documents are hereby incorporated into the contract:</p> <ol style="list-style-type: none"> Exhibit E, Contractual Terms and Conditions is replaced in it's entirety with Exhibit-E-Revised-1, attached hereto and incorporated herein by reference. Exhibit H, IT Proprietary Rights and Data Security Addendum is replaced in it's entirety with Exhibit-H-Revised-1, attached hereto and incorporated herein by reference. Exhibit I, IT Access and Use Agreement is replaced in it's entirety with Exhibit-I -Revised-1, attached hereto and incorporated herein by reference. Exhibit L, Maintenance and Services Agreement is replaced in it's entirety with Exhibit-L-Revised-1, attached hereto and incorporated herein by reference. New: Umo® Services Agreement is attached hereto and incorporated herein by reference. 		
11. ACCEPTED AS TO:		
Exhibit A (Pricing Schedule), Section 5.A. PRICING: BASE PERIOD 1, all Items 1 through 14 for a Total Base Period amount of \$3,565,200.00		
SIGNATURE OF CAPMETRO:		
 E-SIGNED by Muhammad Abdullah on 2024-08-27 15:13:23 CDT		August 27, 2024
Signature _____ Date: _____ Muhammad Abdullah, C.P.M., VP Procurement & Chief Contracting Officer		

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

EXHIBIT A
PRICING SCHEDULE
EMERG 806613

THE OFFEROR IS REQUIRED TO SIGN AND DATE EACH PAGE OF THIS SCHEDULE

1. IDENTIFICATION OF OFFEROR AND SIGNATURE OF AUTHORIZED AGENT

Company Name (Printed)	Cubic Transportation Systems		
Address	233 Balboa Ave		
City, State, Zip	San Diego, CA, 92123		
Phone, Fax, Email	613-799-1119		karim.elsharnouby@cubic.com
The undersigned agrees, if this offer is accepted within the period specified, to furnish any or all supplies and/or services specified in the Schedule at the prices offered therein.			
Authorized Agent Name and Title (Printed)	Frank Capone		
Signature and Date	<i>Frank Capone</i>		15-Jul-24

2. PROMPT PAYMENT DISCOUNT

# of Days		Percentage	%
-----------	--	------------	---

Note, payment terms are specified in Exhibit E, Contractual Terms and Conditions.

3. AUTHORITY'S ACCEPTANCE (TO BE COMPLETED UPON AWARD BY CAPITAL METRO)

The Authority hereby accepts this offer.

Authorized Agent Name and Title (Printed)	
Signature and Date	
Accepted as to:	

The remainder of Exhibit A – Pricing Schedule has been redacted.

For further information regarding Exhibit A, you may:

- Reach out to the Contractor directly via the Contractor contact details provided on the cover page of this contract.

OR

- Submit a public information request directly to PIR@capmetro.org.

For more information regarding the Public Information Act and submitting public information requests, follow this link to our website: <https://www.capmetro.org/legal/>

2. Exhibit B – Representations and Certifications

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

EXHIBIT B

REPRESENTATIONS AND CERTIFICATIONS

(LOCALLY FUNDED SUPPLY/SERVICE/CONSTRUCTION CONTRACTS)

MUST BE RETURNED WITH THE OFFER

1. TYPE OF BUSINESS

(a) The offeror operates as (mark one):

- ☐ An individual
☐ A partnership
☐ A sole proprietor
☒ A corporation
☐ Another entity _____

(b) If incorporated, under the laws of the State of:

California

2. PARENT COMPANY AND IDENTIFYING DATA

(a) The offeror (mark one):

- ☒ is
☐ is not

owned or controlled by a parent company. A parent company is one that owns or controls the activities and basic business policies of the offeror. To own the offering company means that the parent company must own more than fifty percent (50%) of the voting rights in that company.

(b) A company may control an offeror as a parent even though not meeting the requirements for such ownership if the company is able to formulate, determine, or veto basic policy decisions of the offeror through the use of dominant minority voting rights, use of proxy voting, or otherwise.

(c) If not owned or controlled by a parent company, the offeror shall insert its own EIN (Employer's Identification Number) below:

(d) If the offeror is owned or controlled by a parent company, it shall enter the name, main office and EIN number of the parent company, below:

Cubic Corporation
9233 Balboa Ave
San Diego, CA 92123

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

3. CERTIFICATION OF INDEPENDENT PRICE DETERMINATION

(a) The offeror (and all joint venture members, if the offer is submitted by a joint venture) certifies that in connection with this solicitation:

(1) the prices offered have been arrived at independently, without consultation, communication, or agreement for the purpose of restricting competition, with any other offeror or with any other competitor;

(2) unless otherwise required by law, the prices offered have not been knowingly disclosed by the offeror and will not knowingly be disclosed by the offeror prior to opening of bids in the case of an invitation for bids, or prior to contract award in the case of a request for proposals, directly or indirectly to any other offeror or to any competitor; and

(3) no attempt has been made or will be made by the offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.

(b) Each signature on the offer is considered to be a certification by the signatory that the signatory:

(1) is the person in the offeror's organization responsible for determining the prices being offered in this bid or proposal, and that the signatory has not participated and will not participate in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; or

(i) has been authorized, in writing, to act as agent for the following principals in certifying that those principals have not participated, and will not participate in any action contrary to paragraphs (a)(1) through (a)(3) of this provision 95-95-1678055 [insert full name of person(s) in the offeror's organization responsible for determining the prices offered in this bid or proposal, and the title of his or her position in the offeror's organization];

(ii) as an authorized agent, does certify that the principals named in subdivision (b)(1)(i) of this provision have not participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; and

(iii) as an agent, has not personally participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision.

(c) If the offeror deletes or modifies paragraph (a)(2) of this provision, the offeror must furnish with its offer a signed statement setting forth in detail the circumstances of the disclosure.

4. DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION

(a) In accordance with the provisions of 2 C.F.R. (Code of Federal Regulations), part 180, the offeror certifies to the best of the offeror's knowledge and belief, that it and its principals:

(1) are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;

(2) have not within a three (3) year period preceding this offer been convicted of or had a civil judgment rendered against them for the commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes, or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

(3) are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses enumerated in (a)(2) above; and

(4) have not within a three (3) year period preceding this offer had one or more public transactions (Federal, State, or local) terminated for cause or default.

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

(b) Where the offeror is unable to certify to any of the statements above, the offeror shall attach a full explanation to this offer.

(c) For any subcontract at any tier expected to equal or exceed \$25,000:

(1) In accordance with the provisions of 2 C.F.R. part 180, the prospective lower tier subcontractor certifies, by submission of this offer, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

(2) Where the prospective lower tier participant is unable to certify to the statement, above, an explanation shall be attached to the offer.

(3) This certification (specified in paragraphs (c)(1) and (c)(2), above) shall be included in all applicable subcontracts and a copy kept on file by the prime contractor. The prime contractor shall be required to furnish copies of the certifications to the Authority upon request.

5. COMMUNICATIONS

(a) All oral and written communications with the Authority regarding this solicitation shall be exclusively with, or on the subjects and with the persons approved by, the persons identified in this solicitation. Discussions with any other person not specified could result in disclosure of proprietary or other competitive sensitive information or otherwise create the appearance of impropriety or unfair competition and thereby compromise the integrity of the Authority's procurement system. If competition cannot be resolved through normal communication channels, the Authority's protest procedures shall be used for actual or prospective competitors claiming any impropriety in connection with this solicitation.

(b) By submission of this offer, the offeror certifies that it has not, and will not prior to contract award, communicate orally or in writing with any Authority employee or other representative of the Authority (including Board Members, Capital Metro contractors or consultants), except as described below:

Individual's Name	Date/Subject of Communication

(Attach continuation form, if necessary.)

6. CONTINGENT FEE

(a) Except for full-time, bona fide employees working solely for the offeror, the offeror represents as part of its offer that it (mark one):

- ☐ has
☒ has not

employed or retained any company or persons to solicit or obtain this contract, and (mark one):

- ☐ has
☒ has not

paid or agreed to pay any person or company employed or retained to solicit or obtain this contract any commission, percentage, brokerage, or other fee contingent upon or resulting from the award of this contract.

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

(b) The offeror agrees to provide information relating to (a) above, when any item is answered affirmatively.

7. CODE OF ETHICS

(a) Statement of Purpose

The brand and reputation of Capital Metro is determined in large part by the actions or ethics of representatives of the agency. Capital Metro is committed to a strong ethical culture and to ethical behavior by all individuals serving Capital Metro as employees, members of the Board of Directors or volunteers. Individuals serving Capital Metro will conduct business with honesty and integrity. We will make decisions and take actions that are in the best interest of the people we serve and that are consistent with our mission, vision and this policy. The Code of Ethics (the "Code") documents Capital Metro's Standards of Ethical Conduct and policies for Ethical Business Transactions. Compliance with the Code will help protect Capital Metro's reputation for honesty and integrity. The Code attempts to provide clear principles for Capital Metro's expectations for behavior in conducting Capital Metro business. We have a duty to read, understand and comply with the letter and spirit of the Code and Capital Metro policies. You are encouraged to inquire if any aspect of the Code needs clarification.

(b) Applicability

The Code applies to Capital Metro employees, contractors, potential contractors, Board Members and citizen advisory committee members. Violation of the Code of Ethics may result in discipline up to and including termination or removal from the Board of Directors.

(c) Standards of Ethical Conduct

The public must have confidence in our integrity as a public agency and we will act at all times to preserve the trust of the community and protect Capital Metro's reputation. To demonstrate our integrity and commitment to ethical conduct we will:

- (1) Continuously exhibit a desire to serve the public and display a helpful, respectful manner.
- (2) Exhibit and embody a culture of safety in our operations.
- (3) Understand, respect and obey all applicable laws, regulations and Capital Metro policies and procedures both in letter and spirit.
- (4) Exercise sound judgment to determine when to seek advice from legal counsel, the Ethics Officer or others.
- (5) Treat each other with honesty, dignity and respect and will not discriminate in our actions toward others.
- (6) Continuously strive for improvement in our work and be accountable for our actions.
- (7) Transact Capital Metro business effectively and efficiently and act in good faith to protect the Authority's assets from waste, abuse, theft or damage.
- (8) Be good stewards of Capital Metro's reputation and will not make any representation in public or private, orally or in writing, that states, or appears to state, an official position of Capital Metro unless authorized to do so.
- (9) Report all material facts known when reporting on work projects, which if not revealed, could either conceal unlawful or improper practices or prevent informed decisions from being made.
- (10) Be fair, impartial and ethical in our business dealings and will not use our authority to unfairly or illegally influence the decisions of other employees or Board members.

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

(11) Ensure that our personal or business activities, relationships and other interests do not conflict or appear to conflict with the interests of Capital Metro and disclose any potential conflicts.

(12) Encourage ethical behavior and report all known unethical or wrongful conduct to the Capital Metro Ethics Officer or the Board Ethics Officer.

(d) Roles and Responsibilities

It is everyone's responsibility to understand and comply with the Code of Ethics and the law. Lack of knowledge or understanding of the Code will not be considered. If you have a question about the Code of Ethics, ask.

It is the responsibility of Capital Metro management to model appropriate conduct at all times and promote an ethical culture. Seek guidance if you are uncertain what to do.

It is Capital Metro's responsibility to provide a system of reporting and access to guidance when an employee wishes to report a suspected violation and to seek counseling, and the normal chain of command cannot, for whatever reason, be utilized. If you need to report something or seek guidance outside the normal chain of command, Capital Metro provides the following resources:

- (1) Anonymous Fraud Hotline – Internal Audit
- (2) Anonymous Online Ethics Reporting System
- (3) Contact the Capital Metro Ethics Officer, Vice-President of Internal Audit, the EEO Officer or Director of Human Resources
- (4) Safety Hotline

The Capital Metro Ethics Officer is the Chief Counsel. The Ethics Officer is responsible for the interpretation and implementation of the Code and any questions about the interpretation of the Code should be directed to the Ethics Officer.

(e) Ethical Business Transactions

Section 1. Impartiality and Official Position

- (1) A Substantial Interest is defined by Tex. Loc. Govt. Code, § 171.002. An official or a person related to the official in the first degree by consanguinity or affinity has a Substantial Interest in:
 - (i) A business entity if the person owns ten percent (10%) or more of the voting stock or shares of the business entity or owns either 10% or more or \$15,000 or more of the fair market value of the business entity OR funds received by the person from the business entity exceed 10% of the person's gross income for the previous year, or
 - (ii) Real property if the interest is an equitable or legal ownership with a fair market value of \$2,500 or more.

Capital Metro will not enter into a contract with a business in which a Board Member or employee or a Family Member of a Board Member or employee as defined in Section 8 has a Substantial Interest except in case of emergency as defined in the Acquisition Policy PRC-100 or the business is the only available source for essential goods and services or property.

- (2) No Board Member or employee shall:
 - (i) Act as a surety for a business that has work, business or a contract with Capital Metro or act as a surety on any official bond required of an officer of Capital Metro.

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

(ii) Represent for compensation, advise or appear on behalf of any person or firm concerning any contract or transaction or in any proceeding involving Capital Metro's interests.

(iii) Use his or her official position or employment, or Capital Metro's facilities, equipment or supplies to obtain or attempt to obtain private gain or advantage.

(iv) Use his or her official position or employment to unfairly influence other Board members or employees to perform illegal, immoral, or discreditable acts or do anything that would violate Capital Metro policies.

(v) Use Capital Metro's resources, including employees, facilities, equipment, and supplies in political campaign activities.

(vi) Participate in a contract for a contractor or first-tier subcontractor with Capital Metro for a period of one (1) year after leaving employment on any contract with Capital Metro.

(vii) Participate for a period of two (2) years in a contract for a contractor or first-tier subcontractor with Capital Metro if the Board Member or employee participated in the recommendation, bid, proposal or solicitation of the Capital Metro contract or procurement.

Section 2. Employment and Representation

A Board Member or employee must disclose to his or her supervisor, appropriate Capital Metro staff or the Board Chair any discussions of future employment with any business which has, or the Board Member or employee should reasonably foresee is likely to have, any interest in a transaction upon which the Board Member or employee may or must act or make a recommendation subsequent to such discussion. The Board Member or employee shall take no further action on matters regarding the potential future employer.

A Board Member or employee shall not solicit or accept other employment to be performed or compensation to be received while still a Board Member or employee, if the employment or compensation could reasonably be expected to impair independence in judgment or performance of their duties.

A Board Member or employee with authority to appoint or hire employees shall not exercise such authority in favor of an individual who is related within the first degree, within the second degree by affinity or within the third degree by consanguinity as defined by the Capital Metro Nepotism Policy in accordance with Tex. Govt. Code, Ch. 573.

Section 3. Gifts

It is critical to keep an arms-length relationship with the entities and vendors Capital Metro does business with in order to prevent the appearance of impropriety, undue influence or favoritism.

No Board Member or employee shall:

(1) Solicit, accept or agree to accept any benefit or item of monetary value as consideration for the Board Member's or employee's decision, vote, opinion, recommendation or other exercise of discretion as a public servant. [Tex. Penal Code §36.02(c)]

(2) Solicit, accept or agree to accept any benefit or item of monetary value as consideration for a violation of any law or duty. [Tex. Penal Code §36.02(a)(1)]

(3) Solicit, accept or agree to accept any benefit or item of monetary value from a person the Board Member or employee knows is interested in or likely to become interested in any Capital Metro contract or transaction if the benefit or item of monetary value could reasonably be inferred as intended to influence the Board Member or employee. [Tex. Penal Code §36.08(d)]

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

(4) Receive or accept any gift, favor or item of monetary value from a contractor or potential contractor of Capital Metro or from any individual or entity that could reasonably be inferred as intended to influence the Board Member or employee.

Exception: Consistent with state law governing public servants, a gift does not include a benefit or item of monetary value with a value of less than \$50, excluding cash or negotiable instruments, unless it can reasonably be inferred that the item was intended to influence the Board Member or employee. A department may adopt more restrictive provisions if there is a demonstrated and documented business need. [Tex. Penal Code § 36.10(a)(6)]

Exception: A gift or other benefit conferred, independent of the Board Member's or employee's relationship with Capital Metro, that is not given or received with the intent to influence the Board Member or employee in the performance of his or her official duties is not a violation of this policy. The Capital Metro Ethics Officer or Board Ethics Officer must be consulted for a determination as to whether a potential gift falls within this exception.

Exception: Food, lodging, or transportation that is provided as consideration for legitimate services rendered by the Board Member or employee related to his or her official duties is not a violation of this policy.

If you are uncertain about a gift, seek guidance from the Ethics Officer.

Section 4. Business Meals and Functions

Board Members and employees may accept invitations for free, reasonable meals in the course of conducting Capital Metro's business or while attending a seminar or conference in connection with Capital Metro business as long as there is not an active or impending solicitation in which the inviting contractor or party may participate and attendance at the event or meal does not create an appearance that the invitation was intended to influence the Board Member or employee.

When attending such events, it is important to remember that you are representing Capital Metro and if you chose to drink alcohol, you must do so responsibly. Drinking irresponsibly may lead to poor judgment and actions that may violate the Code or other Capital Metro policies and may damage the reputation of Capital Metro in the community and the industry.

Section 5. Confidential Information

It is everyone's responsibility to safeguard Capital Metro's nonpublic and confidential information.

No Board Member or employee shall:

(1) Disclose, use or allow others to use nonpublic or confidential information that Capital Metro has not made public unless it is necessary and part of their job duties and then only pursuant to a nondisclosure agreement approved by legal counsel or with consultation and permission of legal counsel.

(2) Communicate details of any active Capital Metro procurement or solicitation or other contract opportunity to any contractor, potential contractor or individual not authorized to receive information regarding the active procurement or contract opportunity.

Section 6. Financial Accountability and Record Keeping

Capital Metro's financial records and reports should be accurate, timely, and in accordance with applicable laws and accounting rules and principles. Our records must reflect all components of a transaction in an honest and forthright manner. These records reflect the results of Capital Metro's operations and our stewardship of public funds.

A Board Member or employee shall:

(1) Not falsify a document or distort the true nature of a transaction.

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

- (2) Properly disclose risks and potential liabilities to appropriate Capital Metro staff.
- (3) Cooperate with audits of financial records.
- (4) Ensure that all transactions are supported by accurate documentation.
- (5) Ensure that all reports made to government authorities are full, fair, accurate and timely.
- (6) Ensure all accruals and estimates are based on documentation and good faith judgment.

Section 7. Conflict of Interest

Employees and Board Members are expected to deal at arms-length in any transaction on behalf of Capital Metro and avoid and disclose actual conflicts of interest under the law and the Code and any circumstance which could impart the appearance of a conflict of interest. A conflict of interest exists when a Board Member or employee is in a position in which any official act or action taken by them is, may be, or appears to be influenced by considerations of personal gain rather than the general public trust.

Conflict of Interest [Tex. Loc. Govt. Code, Ch. 171 & 176, § 2252.908]

No Board Member or employee shall participate in a matter involving a business, contract or real property transaction in which the Board Member or employee has a Substantial Interest if it is reasonably foreseeable that an action on the matter would confer a special economic benefit on the business, contract or real property that is distinguishable from its effect on the public. [Tex. Loc. Govt. Code, § 171.004]

Disclosure

A Board Member or employee must disclose a Substantial Interest in a business, contract, or real property that would confer a benefit by their vote or decision. The Board Member or employee may not participate in the consideration of the matter subject to the vote or decision. Prior to the vote or decision, a Board Member shall file an affidavit citing the nature and extent of his or her interest with the Board Vice Chair or Ethics Officer. [Tex. Loc. Govt. Code, § 171.004]

A Board Member or employee may choose not to participate in a vote or decision based on an appearance of a conflict of interest and may file an affidavit documenting their recusal.

Section 8. Disclosure of Certain Relationships [Tex. Loc. Govt. Code, Ch. 176]

Definitions

(1) A Local Government Officer is defined by Tex. Loc. Govt. Code § 176.001(4). A Local Government Officer is:

- (i) A member of the Board of Directors;
- (ii) The President/CEO; or

(iii) A third party agent of Capital Metro, including an employee, who exercises discretion in the planning, recommending, selecting or contracting of a vendor.

- (2) A Family Member is a person related within the first degree by consanguinity or the second degree by affinity as defined by Tex. Govt. Code, Ch. 573.
- (3) A Family Relationship is a relationship between a person and another person within the third degree by consanguinity or the second degree by affinity as defined by Tex. Govt. Code, Ch. 573.
- (4) A Local Government Officer must file a Conflicts Disclosure Statement (FORM CIS) if:

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

(i) The person or certain Family Members received at least \$2,500 in taxable income (other than investment income) from a vendor or potential vendor in the last twelve (12) months through an employment or other business relationship;

(ii) The person or certain Family Members received gifts from a vendor or potential vendor with an aggregate value greater than \$100 in the last 12 months; or

(iii) The vendor (or an employee of the vendor) has a Family Relationship with the Local Government Officer.

- (5) A vendor doing business with Capital Metro or seeking to do business with Capital Metro is required to file a completed questionnaire (FORM CIQ) disclosing the vendor's affiliations or business relationship with any Board Member or local government officer or his or her Family Member.

Section 9. Duty to Report and Prohibition on Retaliation

Board Members and employees have a duty to promptly report any violation or possible violation of this Code of Ethics, as well as any actual or potential violation of laws, regulations, or policies and procedures to the hotline, the Capital Metro Ethics Officer or the Board Ethics Officer.

Any employee who reports a violation will be treated with dignity and respect and will not be subjected to any form of retaliation for reporting truthfully and in good faith. Any retaliation is a violation of the Code of Ethics and may also be a violation of the law, and as such, could subject both the individual offender and Capital Metro to legal liability.

Section 10. Penalties for Violation of the Code of Ethics

In addition to turning over evidence of misconduct to the proper law enforcement agency when appropriate, the following penalties may be enforced:

(1) If a Board Member does not comply with the requirements of this policy, the Board member may be subject to censure or removal from the Board in accordance with Section 451.511 of the Texas Transportation Code.

(2) If an employee does not comply with the requirements of this policy, the employee shall be subject to appropriate disciplinary action up to and including termination.

(3) Any individual or business entity contracting or attempting to contract with Capital Metro which offers, confers or agrees to confer any benefit as consideration for a Board Member's or employee's decision, opinion, recommendation, vote or other exercise of discretion as a public servant in exchange for the Board Member's or employee's having exercised his official powers or performed his official duties, or which attempts to communicate with a Board Member or Capital Metro employee regarding details of a procurement or other contract opportunity in violation of Section 5, or which participates in the violation of any provision of this Policy may have its existing Capital Metro contracts terminated and may be excluded from future business with Capital Metro for a period of time as determined appropriate by the President/CEO.

(4) Any individual who makes a false statement in a complaint or during an investigation of a complaint with regard to a matter that is a subject of this policy is in violation of this Code of Ethics and is subject to its penalties. In addition, Capital Metro may pursue any and all available legal and equitable remedies against the person making the false statement or complaint.

Section 11. Miscellaneous Provisions

(1) This Policy shall be construed liberally to effectuate its purposes and policies and to supplement such existing laws as they may relate to the conduct of Board Members and employees.

(2) Within sixty (60) days of the effective date for the adoption of this Code each Board Member and employee of Capital Metro will receive a copy of the Code and sign a statement acknowledging that they have read,

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

understand and will comply with Capital Metro's Code of Ethics. New Board Members and employees will receive a copy of the Code and are required to sign this statement when they begin office or at the time of initial employment.

(3) Board Members and employees shall participate in regular training related to ethical conduct, this Code of Ethics and related laws and policies.

8. RESERVED

9. TEXAS ETHICS COMMISSION CERTIFICATION

In accordance with Section 2252.908, Texas Government Code, upon request of the Authority, the selected contractor may be required to electronically submit a "Certificate of Interested Parties" with the Texas Ethics Commission in the form required by the Texas Ethics Commission, and furnish the Authority with the original signed and notarized document prior to the time the Authority signs the contract. The form can be found at www.ethics.state.tx.us. Questions regarding the form should be directed to the Texas Ethics Commission.

10. TEXAS LABOR CODE CERTIFICATION (CONSTRUCTION ONLY)

Contractor certifies that Contractor will provide workers' compensation insurance coverage on every employee of the Contractor employed on the Project. Contractor shall require that each Subcontractor employed on the Project provide workers' compensation insurance coverage on every employee of the Subcontractor employed on the Project and certify coverage to Contractor as required by Section 406.96 of the Texas Labor Code, and submit the Subcontractor's certificate to the Authority prior to the time the Subcontractor performs any work on the Project.

11. CERTIFICATION REGARDING ISRAEL

As applicable and in accordance with Section 2271.002 of the Texas Government Code, the Contractor certifies that it does not boycott Israel and will not boycott Israel during the term of this Contract.

12. CERTIFICATION REGARDING FOREIGN TERRORIST ORGANIZATIONS

Contractor certifies and warrants that it is not engaged in business with Iran, Sudan, or a foreign terrorist organization, as prohibited by Section 2252.152 of the Texas Government Code.

13. VERIFICATION REGARDING FIREARM ENTITIES AND FIREARM TRADE ASSOCIATIONS

As applicable and in accordance with Section 2274.002 of the Texas Government Code, Contractor verifies that it does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association and will not discriminate during the term of the Contract against a firearm entity or firearm trade association.

14. BOYCOTT OF ENERGY COMPANIES PROHIBITED

Pursuant to Chapter 2274 of Texas Government Code, Contractor verifies that:

(a) it does not, and will not for the duration of the Contract, boycott energy companies, as defined in Section 2274.002 of the Texas Government Code, or

(b) the verification required by Section 2274.002 of the Texas Government Code does not apply to Contractor and this Contract. If circumstances relevant to this provision change during the course of the Contract, Contractor shall promptly notify the Authority.

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

15. CRITICAL INFRASTRUCTURE PROHIBITION

Pursuant to Chapter 2274 of Texas Government Code, Contractor certifies that, if this Contract or any contract between Contractor and Capital Metro relates to critical infrastructure, as defined in Chapter 2274 of the Texas Government Code, Contractor is not owned by or the majority of stock or other ownership interest of its firm is not held or controlled by:

- (a) individuals who are citizens of China, Iran, North Korea, Russia, or a Governor-designated country; or
- (b) a company or other entity, including a governmental entity, that is owned or controlled by citizens of or is directly controlled by the government of China, Iran, North Korea, Russia, or a Governor-designated country; or
- (c) headquartered in China, Iran, North Korea, Russia, or a Governor-designated country.

16. CERTIFICATION OF PRIME CONTRACTOR PARTICIPATION

- (a) The Prime Contractor certifies that it shall perform no less than thirty percent (30%) of the work with his own organization. The on-site production of materials produced by other than the Prime Contractor's forces shall be considered as being subcontracted.
- (b) The organization of the specifications into divisions, sections, articles, and the arrangement and titles of the project drawings shall not control the Prime Contractor in dividing the work among subcontractors or in establishing the extent of the work to be performed by any trade.
- (c) The offeror further certifies that no more than seventy percent (70%) of the work will be done by subcontractors.

17. REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

(a) *Prohibition.* This Contract is subject to the Public Law 115-232, Section 889, and 2 Code of Federal Regulations (CFR) Part 200, including §200.216 and §200.471 related to the prohibition of certain "covered telecommunications equipment and services", which includes:

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities)

(2) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

(3) Telecommunications or video surveillance services provided by such entities or using such equipment.

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(c) *Representation.* The Offeror represents that—

- (1) It

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

- ☐ will
☒ will not

provide covered telecommunications equipment or services to the Authority in the performance of any contract, sub-contract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (d)(1) of this section if the Offeror responds "will" in paragraph (c)(1) of this section; and

- (2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

- ☐ does
☒ does not

use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (d)(2) of this section if the Offeror responds "does" in paragraph (c)(2) of this section.

(d) *Disclosures.*

(1) Disclosure for the representation in paragraph (c)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (c)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (a)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (a)(1) of this provision.

(2) Disclosure for the representation in paragraph (c)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (c)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (a)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (a)(2) of this provision.

18. SIGNATURE BLOCK FOR ALL REPRESENTATIONS AND CERTIFICATIONS

(a) These representations and certifications concern a material representation of fact upon which reliance will be placed in awarding a contract. If it is later determined that the offeror knowingly rendered an erroneous or false certification, in addition to all other remedies the Authority may have, the Authority may terminate the contract for default and/or recommend that the offeror be debarred or suspended from doing business with the Authority in the future.

(b) The offeror shall provide immediate written notice to the Authority if, at any time prior to contract award, the offeror learns that the offeror's certification was, or a subsequent communication makes, the certification erroneous.

(c) Offerors must set forth full, accurate and complete information as required by this solicitation (including this attachment). Failure of an offeror to do so may render the offer nonresponsive.

(d) A false statement in any offer submitted to the Authority may be a criminal offense in violation of Section 37.10 of the Texas Penal Code.

(e) I understand that a false statement on this certification may be grounds for rejection of this submittal or termination of the awarded contract.

Name of Offeror:

Cubic Transportation Systems, Inc.

Type/Print Name of Signatory:

Frank Capone

Signature:

Frank Capone

Date:

July 9, 2024

EXHIBIT E-Revised-1
CONTRACTUAL TERMS AND CONDITIONS
(SERVICES CONTRACT)

1. DEFINITIONS

As used throughout this Contract, the following terms shall have the meaning set forth below:

- (a) “Applicable Anti-Corruption and Bribery Laws” means international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the Contractor’s provision of goods and/or services to Authority, including without limitation “FCPA” or any applicable laws and regulations, including in the jurisdiction in which the Contractor operates and/or manufactures goods for the Authority, relating to anti-corruption and bribery.
- (b) “Authority”, “Capital Metro”, “CapMetro”, “CMTA” means Capital Metropolitan Transportation Authority.
- (c) “Authority Data” or “Customer Data” means the data collected through the Services relating to Users’ use of Customer’s transportation services and analytics, reporting, results, or other information that Cubic provides to Customer in respect of such data as part of the Services including all data, content and information (i) submitted by or on behalf of the Authority or its customers to the Contractor or loaded into the System, (ii) obtained, developed, produced or processed by the Contractor in its provision of the Services in connection with the Contract, or (iii) to which the Contractor has access in connection with the Contract, and all derivative versions of such data, content and information, and any derivative versions thereof, in any form or format .
- (d) “Authority Electronic Property” means (i) any websites controlled by the Authority, (ii) any Authority mobile device apps, (iii) any application programming interfaces (API) to the Authority’s information technology systems, (iv) any other kiosks, devices or properties for consumer interaction that are created, owned, or controlled by the Authority, and (v) versions and successors of the foregoing, any form or format now known or later developed, that may be used by customers obtaining products or services from the Authority.
- (e) “Change Order” means a written order to the Contractor signed by the Contracting Officer, issued after execution of the Contract, authorizing a change in the term or scope of the Contract.
- (f) “Contract” or “Contract Documents” means this written agreement between the parties comprised of all the documents listed in the Table of Contents, Change Orders and/or Contract Modifications that may be entered into by the parties.
- (g) “Contract Award Date” means the date of the Contract award notice, which may take the form of a purchase order, signed Contract or Notice of Award, issued by the Authority.
- (h) “Contract Modification” means any changes in the terms or provisions of the Contract which are reduced to writing and fully executed by both parties.
- (i) “Contract Sum” means the total compensation payable to the Contractor for performing the Services as originally contracted for or as subsequently adjusted by Contract Modification.
- (j) “Contract Term” means period of performance set forth in the paragraph entitled “Term” contained in Exhibit E.
- (k) “Contracting Officer” means a person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings on behalf of the Authority. The term includes certain authorized representatives of the Contracting Officer acting within the limits of their authority as delegated by the Contracting Officer.
- (l) “Contractor” means the entity that has assumed the legal obligation to perform the Services as identified in the Contract.
- (m) “Days” means calendar days. In computing any period of time established under this Contract, the day of the event from which the designated period of time begins to run shall not be included, but the last day shall be included.

unless it is a Saturday, Sunday, or Federal or State of Texas holiday, in which event the period shall run to the end of the next business day.

- (n) "FAR" means the Federal Acquisition Regulations codified in 48 C.F.R. Title 48.
- (o) "FCPA" means the United States Foreign Corrupt Practices Act, 15 U.S.C. §§ 78dd-1, et seq., as amended.
- (p) "Force Majeure Event" means strikes, lockouts, or other industrial disputes; explosions, epidemics, civil disturbances, acts of domestic or foreign terrorism, pandemics wars, riots or insurrections; embargos, natural disasters, including but not limited to landslides, fire, earthquakes, floods, storms or washouts; interruptions by government or court orders; declarations of emergencies by applicable federal, state or local authorities; and present or future orders of any regulatory body having proper jurisdiction.
- (q) "Intellectual Property Rights" means the worldwide legal rights or interests evidenced by or embodied in: (i) any idea, software, design, concept, personality right, method, process, technique, apparatus, invention, discovery, or improvement, including any patents, trade secrets, and know-how; (ii) any work of authorship, including any copyrights, moral rights or neighboring rights, and any derivative works thereto; (iii) any trademark, service mark, trade dress, trade name, or other indicia of source or origin; (iv) domain name registrations; and (v) any other proprietary or similar rights. The Intellectual Property Rights of a party include all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.
- (r) "Manufacturing Materials" mean any completed or partially completed supplies and materials that are deliverables under this Contract and have been, specifically produced or specially acquired by the Contractor for the performance of the Contract.
- (s) "Notice of Award" means formal notice of award of the Contract to the Contractor issued by the Contracting Officer.
- (t) "Notice to Proceed" means written authorization for the Contractor to start the Services.
- (u) "Project Manager" means the designated individual to act on behalf of the Authority, to monitor and certify the technical progress of the Contractor's Services under the terms of this Contract.
- (v) "Proposal" means the offer of the proposer, submitted on the prescribed form, stating prices for performing the work described in the Scope of Services.
- (w) "Services" or "Umo Services" means the services to be performed by the Contractor under this Contract, and includes services performed, workmanship, and supplies furnished or utilized in the performance of the Services.
- (x) "Subcontract" means the Contract between the Contractor and its Subcontractors.
- (y) "Subcontractor" means Subcontractors .
- (z) "USD" means United States Dollars and is the currency for all prices and fees under this Contract.
- (aa) "Works" means any tangible or intangible items or things that have been or will be specifically, generated, prepared, created, or developed by the Contractor (or such third parties as the Contractor may be permitted to engage) at any time following the effective date of the Contract, for the exclusive use of, and ownership by, Authority under the Contract, including but not limited to any (i) works of authorship (such as literary works, musical works, dramatic works, choreographic works, pictorial, graphic and sculptural works, motion pictures and other audiovisual works, sound recordings and architectural works, which includes but is not limited to manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer software, scripts, object code, source code or other programming code, HTML code, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or

improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, and (vi) all documentation and materials related to any of the foregoing.

2. FIXED PRICE/INDEFINITE QUANTITY, INDEFINITE DELIVERY CONTRACT

This is a fixed price definite quantity Contract for the supplies or Services specified in the Pricing Schedule, Exhibit A to the Contract, and stated in the Umo Service Agreement in the Contract.

3. TERM

The term of the Contract shall one (1) year from the Contract notice to proceed. No Services shall be performed under this Contract prior to issuance of a Notice to Proceed.

4. OPTION TO EXTEND CONTRACT TERM

The Authority shall have the unilateral right and option to extend the Contract for up to four option periods of twelve (12) month in duration each at the option prices set forth in Exhibit A - Pricing Schedule upon giving no less than thirty (30) Days written notice to the Contractor.

5. ADDITIONAL OPTION TO EXTEND CONTRACT PERFORMANCE

If the options granted in Paragraph 4 have been exercised in their entirety, by mutual agreement, the parties may agree to the continued performance of any services within the limits and rates specified in the Contract. This option may be exercised more than once, but the extension of performance hereunder shall not exceed a total of 6 months. The Authority may exercise the option by written notice to the Contractor.

6. PERFORMANCE BOND - NOT USED

7. INVOICING AND PAYMENT

The prices and Fees applicable to this Contract for the payment of Services and, where applicable, Payment Milestones are set out in the Authority's Exhibit A (Pricing Schedule EMERG 8-6613) and further detailed in Exhibit C of the Umo Services Agreement.

Invoices may be submitted once per month for work completed and accepted by the Authority, and marked "Original" to:

Accounts Payable
Capital Metropolitan Transportation Authority
P.O. Box 6308
Austin, Texas 78762-6308

Or via e-mail to: ap_invoices@capmetro.org

and shall conform to policies or regulations adopted from time to time by the Authority. Invoices shall be legible and shall contain reasonable supporting information including:

- (1) the Contract and order number (if any);
- (2) where applicable, a complete itemization of all costs including quantities ordered and delivery order numbers (if any);
- (3) in respect of milestone payments only, evidence of the acceptance of the supplies or Services by the Authority; and
- (4) any other information necessary to demonstrate entitlement to payment under the terms of the Contract.

(f) Subject to the withholding regarding retainage as provided herein, all undisputed invoices shall be paid within the time period allowed by law through the Texas Prompt Payment Act, Tex. Gov't Code § 2251.021(b).

(g) The Contractor shall be responsible for all costs/expenses not otherwise specified in this Contract, including by way of example, all costs of equipment provided by the Contractor or Subcontractor(s), all fees, fines, licenses, bonds, or taxes required or imposed against the Contractor and Subcontractor(s), travel related expenses, and all other Contractor's costs of doing business.

(h) In the event an overpayment is made to the Contractor under this Contract or the Authority discovers that the Authority has paid any invoices or charges not authorized under this Contract, the Authority shall first notify the Contractor in writing and may offset the amount of such overpayment or unauthorized charges against any indebtedness owed by the Authority to the Contractor, whether arising under this Contract or otherwise, including withholding payment of an invoice, in whole or in part, or the Authority may deduct such amounts from future invoices. If an overpayment is made to the Contractor under this Contract which cannot be offset under this Contract, the Contractor shall remit the full overpayment amount to the Authority within thirty (30) calendar days of the date of the written notice of such overpayment or such other period as the Authority may agree. The Authority reserves the right to withhold payment of an invoice, in whole or in part, or deduct the overpayment from future invoices to recoup the overpayment.

(i) Release of Payment Claims by Contractor. The final invoice submitted by Contractor shall be accompanied by a complete and legally effective release of the Authority from all known and unknown payment claims relating to the Contract on a form provided by the Authority. Contractor's acceptance of final payment constitutes a waiver of all known or unknown payment claims against the Authority related to the Contract, other than those specifically excepted in the General Release of Claims Form.

8. ACCEPTANCE CRITERIA

A review of the Contractor's Services will be performed by the Authority. upon delivery. If any Services performed under this Contract are deemed materially incomplete or unacceptable, per Acceptance Criteria referenced in Exhibit F-Scope of Services and Compliance Matrix, the Authority will require the Contractor to take corrective measures at no additional cost to the Authority. Refer to Exhibit K, Performance Deficiency Credits (PDCs).

9. INSURANCE

(a) The Contractor shall furnish proof of CapMetro stipulated insurance requirements specified below. All insurance policies shall be primary and non-contributing with the exception of Professional Liability and Workers Compensation with any other valid and collectible insurance or self-insurance available to the Authority and shall contain a contract waiver of subrogation with the exception of Professional Liability in favor of the Authority. The Contractor shall furnish to the Authority certificate(s) of insurance evidencing the required coverage and endorsement(s) and, upon request, a copy of any of those policies. Prior to the expiration of a certificate of insurance, a new certificate of insurance shall be furnished to the Authority showing continued coverage. Each policy shall be endorsed to provide thirty (30) days written notice of cancellation or non-renewal except ten (10) days for non-payment of premium to the Authority and the Authority shall be named as an Additional Insured under each policy except Professional Liability insurance if required by this Contract. All insurance policies shall be written by reputable insurance company or companies acceptable to the Authority with a current Best's Insurance Guide Rating of A- and Class VII or better. All insurance companies shall be authorized to transact business in the State of Texas. The Contractor shall notify the Authority in writing of any material alteration of such policies, including any change in the retroactive date in any "claims-made" policy or substantial reduction of aggregate limits, if such limits apply or cancellation thereof at least thirty (30) days prior thereto. The below requirements only represent the minimum coverage acceptable to the Authority and these requirements are not intended to represent the maximum risk or the maximum liability of the Contractor. The Contractor shall be responsible for setting its own insurance requirements, if any, for the kind and amounts of insurance to be carried by its Subcontractors.

The Contractor shall carry and pay the premiums for insurance of the types and in the amounts stated below.

CAPMETRO MINIMUM COVERAGE REQUIREMENTS

1. **Comprehensive General Liability Insurance** Coverage with limits of not less than One Million and No/100 Dollars (\$1,000,000) Combine Single Limit of Liability for Bodily Injury and Property Damage including Prod-

ucts Liability.

2. **Automobile Liability Insurance** covering all owned, hired and non-owned automobiles used in connection with work with limits not less than One Million and No/100 Dollars (\$1,000,000) Combined Single Limit of Liability for Bodily Injury and Property Damage.

3. **Statutory Workers' Compensation** coverage in the State of Texas. Employers Liability Insurance with minimum limits of liability of One Million Dollars and No/100 Dollars (\$1,000,000).

4. Professional Liability Insurance covering negligent acts, errors and omissions arising from the Contractor's work to pay damages for which the Contractor may become legally obligated. Minimum limits of liability shall be not less than One Million Dollars and No/100 Dollars (\$1,000,000) per claim and on an annual aggregate basis.

5. All policies shall include coverage for TRIA.

(b) The limits of liability as required above may be provided by a single policy of insurance or by a combination of primary, excess or umbrella policies but in no event shall the total limits of liability available for any one occurrence or accident be less than the amount required above.

(c) The Contractor, and all of its insurers shall, in regard to the above stated insurance with the exception of Professional Liability, agree to waive all rights of recovery or subrogation against the Authority, its directors, officers, employees, agents, successors and assigns, and the Authority's insurance companies arising out of any claims for injury(ies) or damages resulting from the Services performed by or on behalf of the Contractor under this Contract and/or use of any Authority premises or equipment under this Contract.

(d) Each insurance policy shall contain the following endorsements: PRIMARY AND NON-CONTRIBUTORY INSURANCE with the exception of Professional Liability and Workers Compensation and WAIVER OF TRANSFER OF RIGHTS OF RECOVERY AGAINST OTHERS with the exception of Professional Liability, which shall be evidenced on the Certificate of Insurance. The General Liability insurance shall include contractual endorsement(s) which acknowledge all indemnification requirements under the Agreement. All required endorsements shall be evidenced on the Certificate of Insurance, which shall be evidenced on the Certificate of Insurance. Proof that insurance coverage exists shall be furnished to the Authority by way of a Certificate of Insurance before any part of the Contract work is started.

(e) If any insurance coverage required to be provided by the Contractor is canceled, terminated, or modified so that the required insurance coverages are no longer in full force and effect, the Authority may terminate this Contract or obtain insurance coverages equal to the required coverage, the full cost of which will be the responsibility of the Contractor and shall be deducted from any payment due the Contractor.

(f) Not used

(g) The Contractor must furnish proof of the required insurance within ten (10) days of the award of the Contract. Certificate of Insurance must indicate the Contract number and description. The insurance certificate should be furnished to the attention of the Contracting Officer.

(h) The Contractor shall and shall procure that its Subcontractors are required to cooperate with the Authority and report all potential material claims estimated to be over \$150,000 (workers' compensation, general liability and automobile liability) pertaining to this Contract to the Authority's Risk Management Department at (512) 389-7538 or emailed to Fay.Milligan@capmetro.org within ten (10) days of Risk Management becoming aware of the incident.

10. PERFORMANCE OF SERVICES BY THE CONTRACTOR

Except as otherwise provided herein, the Contractor shall perform no less than thirty percent (30%) of the Services with its own organization. If, during the progress of Services hereunder, the Contractor requests a reduction in such performance percentage and the Authority determines that it would be to the Authority's advantage, the percentage of the Services required to be performed by the Contractor may be reduced; provided, written approval of such reduction is obtained by the Contractor from the Authority.

11. REMOVAL OF ASSIGNED PERSONNEL

The Authority, acting reasonably and for good cause shown, may request, in writing, that the Contractor remove from the Services any employee or Subcontractor of the Contractor that the Authority deems inappropriate for the assignment.

12. REPRESENTATIONS AND WARRANTIES

The Contractor represents and warrants to the Authority, that the Services shall be performed in conformity with the descriptions and other data set forth in this Contract in all material respect and with sound professional principles and practices in accordance with accepted industry standards, and that work performed by the Contractor's personnel shall reflect sound professional knowledge, skill and judgment. If any breach of the representations and warranties is discovered by the Authority during the process of the work or within one (1) year after acceptance of the work by the Authority, the Contractor shall again cause the nonconforming or inadequate work to be properly performed at the Contractor's sole expense and shall reimburse for costs directly incurred by the Authority as a result of reliance by the Authority on services failing to comply with the representations and warranties.

EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES MADE BY CUBIC IN THIS AGREEMENT AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER CUBIC NOR ITS LICENSORS MAKE ANY REPRESENTATIONS OR WARRANTIES. EXCEPT AS EXPRESSLY SET FORTH HEREIN, THE SERVICES ARE MADE AVAILABLE TO CUSTOMER "AS IS". TO THE MAXIMUM EXTENT PERMITTED BY LAW, CUBIC EXPRESSLY DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, NONINFRINGEMENT, TITLE OR IMPLIED WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. WITHOUT LIMITATION OF THE FOREGOING, CUBIC WILL HAVE NO LIABILITY FOR ANY: (A) ERRORS, MISTAKES, INACCURACIES, OR LOSS OF ANY INFORMATION OR DATA; (B) ANY UNAUTHORIZED ACCESS TO OR USE OF THE SERVICES; (C) ANY INTERRUPTION OF TRANSMISSION TO OR FROM THE SERVICES; (D) ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE, WHICH MAY BE TRANSMITTED ON OR THROUGH THE SERVICES BY ANY THIRD PARTY; OR (E) ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF THE SERVICES OR ANY INFORMATION OR DATA OBTAINED, TRANSMITTED, OR OTHERWISE MADE AVAILABLE ON OR THROUGH THE SERVICES.

13. INDEPENDENT CONTRACTOR

The Contractor's relationship to the Authority in the performance of this Contract is that of an independent contractor. The personnel performing Services under this Contract shall at all times be under the Contractor's exclusive direction and control and shall be employees of the Contractor and not employees of the Authority. The Contractor shall be fully liable for all acts and omissions of its employees, Subcontractors, and their suppliers and shall be specifically responsible for sufficient supervision and inspection to assure compliance in every respect with Contract requirements. There shall be no contractual relationship between any Subcontractor or supplier of the Contractor and the Authority by virtue of this Contract. The Contractor shall pay wages, salaries and other amounts due its employees in connection with this Agreement and shall be responsible for all reports and obligations respecting them, such as Social Security, income tax withholding, unemployment compensation, workers' compensation and similar matters.

14. COMPOSITION OF CONTRACTOR

If the Contractor hereunder is comprised of more than one legal entity, each such entity shall be jointly and severally liable hereunder.

15. SUBCONTRACTORS AND OUTSIDE CONSULTANTS

Subject to the terms of this Contract, the Contractor shall be entitled to use any Subcontractors and outside associates or consultants required by the Contractor in connection with the Services covered by the Contract. Contractor shall be fully liable in respect of any Services undertaken by such Subcontractors and outside associates or consultants and will be limited to such individuals or firms as were specifically identified and agreed to by the Authority in connection with the award of this Contract. Any substitution in such Subcontractors, associates, or consultants will be subject to the prior approval of the Authority.

16. EQUITABLE ADJUSTMENTS

(a) Any requests for equitable adjustments under any provision shall be governed by the following provisions:

(1) Upon written request, the Contractor shall submit a proposal, in accordance with the requirements and limitations set forth in this paragraph, for Services involving contemplated changes covered by the request. The proposal shall be submitted within the time limit indicated in the request for any extension of such time limit as may be subsequently granted. The Contractor's written statement of the monetary extent of a claim for equitable adjustment shall be submitted in the following form:

(i) Proposals totaling \$5,000 or less shall be submitted in the form of a lump sum proposal with supporting information to clearly relate elements of cost with specific items of Services involved to the satisfaction of the Contracting Officer, or his/her authorized representative.

(ii) For proposals in excess of \$5,000, the claim for equitable adjustment shall be submitted in the form of a lump sum proposal supported with an itemized breakdown of all increases and decreases in the Contract.

(b) No proposal by the Contractor for an equitable adjustment shall be allowed if asserted after final payment under this Contract.

17. CONTRACTOR AND SUBCONTRACTOR ANNUAL AUDITED FINANCIAL STATEMENTS AND ABILITY TO PERFORM

The Contractor must provide evidence of financial resources and its ability to perform the services for which Contractor is submitting a response. This includes three (3) prior years audited company financial statements that demonstrates its financial capability, financial solvency, and capability to fulfill the requirements of this contract.

The Contractor is a private equity firm and any public financial information must be provided to the Authority in evaluation of this section. If any non-public financial information is requested, Contractor and the Authority agree to enter into a mutually agreeable confidential agreement for the purpose of releasing such financial information regarding the Contractor's ability to perform under the Contract.

18. PERSONNEL ASSIGNMENTS

(a) The Contractor shall perform the Services in an orderly and workmanlike manner, and shall utilize persons skilled and qualified for the performance of the Services. The Authority will have the right to review the experience of each person assigned to perform the Services and approve personnel assignments, including those to be performed by Subcontractors,

(b) The Contractor represents that the Contractor, has established a criminal history back-ground policy that complies with guidance issued by the U.S. Equal Employment Opportunity Commission and that the Contractor and each Subcontractor conducts criminal history checks on its assigned personnel in accordance with such policy to identify, hire and assign personnel to work on this Contract whose criminal backgrounds are appropriate for the Services being performed, considering the risk and liability to the Contractor and the Authority. Contractor hereby confirms that its typical onboarding procedures includes a) employment verification, b) education verification, c) nationwide criminal searches, d) federal and county court searches, e) sex offender searches, and f) employment verification as part of the hiring process.

19. BADGES AND ACCESS CONTROL DEVICES

(a) The Contractor and each of the Contractor's employees, as well as each Subcontractor of any tier and any workers working on behalf of Subcontractor, shall be required to wear a CapMetro Contractor Photo Identification Badge ("badge") at all times while on the Authority's premises. The badge will be provided by CapMetro. If any badge holder loses or misplaces his or her badge, the Contractor shall immediately notify the Project Manager upon discovery. The Contractor will be charged a \$50.00 replacement fee for each lost or misplaced badge, which fee shall be deducted any amounts due and owing to the Contractor or if the Contract is terminated upon demand by the Authority. The Contractor shall return all badges provided when any badge holder is no longer working on the Contract, and all badges shall be returned upon completion of the Contract. In the event the Contractor fails to do so, the Contractor

will pay a \$50.00 per badge fee deducted from any amounts due and owing to the Contractor or if the Contract is terminated upon demand by the Authority. All badges should be returned to the Project Manager. All requests for new and replacement badges must be submitted in writing to the Project Manager. The misuse of a badge may result in termination of the Contract.

(b) Access Control Devices will be issued to employees of the Contractor and to each Subcontractor of any tier and any worker working on behalf of Subcontractor as necessary to perform the Contract. Access Control Devices are not transferable between the Contractor employees or workers working on behalf of the Subcontractor. The Contractor employees and workers on behalf of the Subcontractor are prohibited from loaning Access Control Devices or providing access to an unauthorized person into restricted areas without prior arrangements with the Project Manager. All requests for new and replacement Access Control Devices must be submitted in writing to the Project Manager. Lost Access Control Devices must be reported to the Project Manager immediately upon discovery. All Access Control Devices should be returned to the Project Manager. The misuse of an Access Control Device(s) may result in termination of the Contract. The Contractor shall return all Access Control Devices once an assigned employee or worker is no longer working on the Contract or upon termination of the Contract. In the event the Contractor fails to do so, then the Contractor shall be responsible for the replacement cost of an Access Control Device which shall be deducted from any amounts due and owing to the Contractor or payable on demand if the Contract has terminated. The replacement cost will be calculated at current market value to include labor and materials.

(c) The provisions of this paragraph survive termination of the Contract.

20. **CHANGES**

(a) The Authority may, at any time, propose changes within the general scope of the Contract in the Services to be performed. All such changes must be mutually agreed to by the Parties prior to implementation and going into effect. If such changes cause an increase or decrease in the Contractor's cost of, or time required for, performance of any Services under this Contract, whether or not changed by any order, an equitable adjustment shall be made and the Contract shall be modified in writing accordingly. Any claim of the Contractor for adjustment under this paragraph must be asserted in writing within thirty (30) days from the date of receipt by the Contractor of the notification of change unless the Contracting Officer grants a further period of time before the date of final payment under the Contract.

(b) No Services for which an additional cost or fee will be charged by the Contractor shall be furnished without the prior written authorization of the Authority.

(c) Any other written order (which, as used in this paragraph (c), includes direction, instruction, interpretation, or determination) from the Contracting Officer that causes a change in the Contractor's obligations shall be treated as a Change Order under this paragraph; provided that the Contractor gives the Contracting Officer written notice stating (1) the date, circumstances, and source of the order and (2) that the Contractor regards the order as a Change Order.

(d) Except as provided in this paragraph, no order, statement, or conduct of the Contracting Officer shall be treated as a change under this paragraph or entitle the Contractor to an equitable adjustment.

(e) If any change under this paragraph or if there is a failure by the Authority to comply with its obligation set out in section (f) below that causes an increase or decrease in the Contractor's cost of, or the time required for, the performance of any part of the Services under this Contract, whether or not changed by any such order, the Contracting Officer may make an equitable adjustment and modify the Contract in writing in accordance with the provisions in paragraph entitled "Equitable Adjustments" contained in Exhibit E.

(f) **Customer Obligations.** Customer shall:

(1) provide Cubic:

(i) all necessary cooperation in relation to this Agreement; and

(ii) all necessary access to such information as may be required by Cubic in order to provide the Services, including but not limited to Customer Data, Transit Data, security access information and configuration services; and

- (iii) and its Subcontractors for trip planning purposes a non-exclusive, royalty-free, sublicensable, worldwide, non-exclusive right and license to access, use, distribute, modify, publicly perform, and display Transit Data, including the right to sublicense such rights to Subcontractors. Such right and license is valid only for the Term of the Agreement and shall terminate upon the expiration of the Agreement.
- (2) comply with all applicable laws and regulations with respect to its activities under this Agreement;
- (3) carry out all other Customer responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in Customer's provision of such assistance as agreed by the Parties, Cubic may adjust any agreed upon timetable or delivery schedule as reasonably necessary and Customer shall be liable for any reasonable and demonstrable costs related to such adjustment;
- (4) obtain and shall maintain all necessary licenses, consents, and permissions applicable to Customer that are required for Cubic, its subcontractors and agents to perform their obligations under this Agreement, including without limitation the Services;
- (5) ensure that its network and systems comply with the relevant specifications provided by Cubic from time to time; and
- (6) be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to Customer's data centers, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to Customer's network connections or telecommunications links or caused by the internet.
- (7) Provide required data, approvals, and other deliverables in a timely fashion as reasonably required by Cubic to perform its obligations under this Agreement.
- (8) Implement and execute PCI-DSS practice as required by the responsibilities assigned to the Customer including but not limited to security policies and operational procedures, inspection of equipment for tampering, and personnel training.
- (9) Permit Cubic and its agents reasonable access to Customer's buses, installation sites and to the premises in which Customer conducts its business and furnish to Cubic other information as Cubic may reasonably request for performance of the Services.
- (10) Unless specifically agreed otherwise in writing, provide and maintain the data services required for the Equipment to communicate with the Umo Services.
- (11) Unless otherwise specified in this agreement manage and be responsible for any Customer Managed Third-Parties.

21. LIQUIDATED DAMAGES

If the Contractor misses the go-live date of March 1, 2025—Phase 1: SaaS platform, Account-Based Ticketing with Product Based Farecapping, customer mobile app, customer and partner websites, inspection/validation/citation app, Customer Service and Admin Portals, reporting tools, API available for exporting data to a data warehouse, cash digitization network integration, Flowbird TVM integration, training, testing and project management, as well as installs of new validators across the fixed route fleet, the Contractor must, in place of actual damages, pay to the Authority the sum of \$5,000.00 for each calendar day of delay as liquidated damages and not as a penalty, provided, however, the maximum aggregate amount that Contractor shall be liable under this provision shall not exceed two hundred fifty thousand, and 00/100 dollars (\$250,000.00).

The parties agree that the damages in this section are liquidated damages and not penalties and that they are reasonable in light of the harm that would be caused by breach, the difficulties of proof of loss, and the inconvenience and infeasibility of otherwise obtaining an adequate remedy.

Liquidated damages do not limit the Authority's right to terminate this Contract for default or it limit the Authority's ability to pursue other remedies available to the Authority elsewhere in this Contract. Liquidated damages may be deducted from any amounts due and owing Contractor under this Contract.

22. TERMINATION FOR DEFAULT

(a) The Authority may, subject to the provisions of subparagraph (c) below, by written notice of default to the Contractor, terminate the whole or any part of this Contract in either one of the following circumstances:

(1) if the Contractor fails to perform the Services within the time specified herein or any extension thereof;
or

(2) if the Contractor materially breaches the provisions of this Contract and does not cure such failure within a period of thirty (30) days (or such longer period as the Authority may authorize in writing) after receipt of notice from the Authority specifying such failure.

(b) Corrective Action Plans. If the Authority reasonably believes that Contractor is in material breach of this Contract and such breach is capable of being cured, then prior to issuing written notice of such a breach, the Authority shall notify Contractor that a plan is required to remedy such material breach (a "Corrective Action Plan"). If Contractor fails to provide a Corrective Action Plan within thirty (30) Days of such notification or fails to comply with the Corrective Action Plan, then the Authority shall be entitled to issue a Default Notice.

(c) In the event the Authority terminates this Contract in whole or in part as provided in subparagraph (a) of this paragraph, the Authority may procure, upon such terms and in such manner as the Authority may deem appropriate, supplies or services similar to those so terminated, and, subject to the limits of liability set out in this Contract and the Authority being obliged to mitigate such costs, the Contractor shall be liable to the Authority for any excess costs for such similar supplies or services; provided, that the Contractor shall continue the performance of this Contract to the extent, if any, it has not been terminated under the provisions of this subparagraph.

(d) Except with respect to the defaults of Subcontractors, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises out of causes beyond the control and without the fault or negligence of the Contractor. Such causes may include, but are not restricted to Force Majeure Events; provided, however, in every case the failure to must be beyond the control and without the fault or negligence of the Contractor. If the failure to perform is caused by the default of a Subcontractor and if such default arises out of causes beyond the control of both the Contractor and Subcontractor and without the fault or negligence of either of them, the Contractor shall not be liable for any excess costs for failure to perform, unless the supplies or Services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required delivery schedule.

(e) If this Contract is terminated as provided in subparagraph (a), the Authority, in addition to any other rights provided in this subparagraph, may require the Contractor to transfer title and deliver to the Authority in the manner and to the extent directed by the Authority any Manufacturing Materials as the Contractor has specifically produced or specifically acquired for the performance of such part of this Contract as has been terminated; and the Contractor shall, upon direction of the Authority, protect and preserve property in possession of the Contractor in which the Authority has an interest. Payment for completed Manufacturing Materials delivered to and accepted by the Authority shall be at the Contract price. The Authority may withhold from amounts otherwise due the Contractor for such completed Manufacturing Materials such sum as the Authority determines to be necessary to protect the Authority against loss because of outstanding liens or claims of former lien holders.

(f) If, after notice of termination of this Contract under the provisions of this paragraph, it is determined by the Authority that the Contractor was not in default or that the default was excusable under the provisions of this paragraph, the rights and obligations of the parties shall be those provided in the paragraph entitled "Termination for Convenience" contained in this Exhibit E.

(g) The rights and remedies of the Authority provided in this paragraph shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

23. TERMINATION FOR CONVENIENCE

(a) The Authority may, whenever the interests of the Authority so require, terminate this Contract, in whole or in part, for the convenience of the Authority. The Authority shall give one hundred eighty (180) Days written notice of the termination to the Contractor specifying the part of the Contract terminated and when termination becomes effective.

(b) The Contractor shall incur no further obligations in connection with the terminated orders, and, on the date set forth in the notice of termination, the Contractor will stop providing Services to the extent specified. The Contractor also shall terminate outstanding orders and subcontracts as they relate to the terminated order. The Contractor shall settle the liabilities and claims arising out of the termination of subcontracts and orders connected with the terminated orders. The Authority may direct the Contractor to assign the Contractor's right, title, and interest under terminated orders or Subcontracts to the Authority. The Contractor must still complete any orders not terminated by the notice of termination and may incur such obligations as are necessary to do so.

(c) To the extent the Authority has paid in full for such material, the Authority may require the Contractor to transfer title and deliver to the Authority in the manner and to the extent directed by the Authority: any completed supplies; as the Contractor has specifically produced or specially acquired as a deliverable for the performance of the terminated part of this Contract. The Contractor shall, upon direction of the Authority, protect and preserve property in the possession of the Contractor in which the Authority has an interest. If the Authority does not exercise this right, the Contractor shall use its best efforts to sell such supplies and Manufacturing Materials.

(d) The Authority shall pay the Contractor the following amounts:

(1) Contract prices for supplies required to be delivered under section 22(c) or accepted under the Contract

(2) costs incurred in preparing to perform and performing the terminated portion of the Services plus a fair and reasonable profit on such portion of the Services (such profit shall not include anticipatory profit or consequential damages), less amounts paid or to be paid for accepted supplies; provided, however, that if it appears that the Contractor would have sustained a loss if the entire Contract would have been completed, no profit shall be allowed or included, and the amount of compensation shall be reduced to reflect the anticipated rate of loss;

(3) costs of settling and paying claims arising out of the termination of subcontracts (these costs must not include costs paid in accordance with subparagraph (2) of this paragraph); and

(4) the reasonable settlement costs of the Contractor and other expenses reasonably necessary for the preparation of settlement claims and supporting data with respect to the terminated portion of the Contract and for the termination and settlement of subcontracts thereunder, together with reasonable storage, transportation, and other costs incurred in connection with the protection or disposition of property allocable to the terminated portion of this Contract.

(5) The total sum to be paid the Contractor under this paragraph shall not exceed the total Contract Sum plus the reasonable settlement costs of the Contractor reduced by the amount of payments otherwise made, the proceeds of any sales of supplies and Manufacturing Materials under this paragraph, and the contract price of orders not terminated.

24. CONTRACTOR CERTIFICATION

The Contractor certifies that the fees in this Contract have been arrived at independently without consultation, communication, or agreement for the purpose of restricting competition, as to any matter relating to such fees with any other firm or with any competitor.

25. INTELLECTUAL PROPERTY: DATA PRIVACY PROVISIONS

The Umo Services Agreement included as part of this Contract shall govern Intellectual Property and Data Privacy.

26. STANDARDS OF PERFORMANCE

The Contractor shall perform the Services hereunder in compliance with all applicable federal, state, and local laws and regulations. The Contractor shall use only licensed personnel to perform Services required by law to be performed by such personnel.

27. INSPECTIONS AND APPROVALS

(a) All Services performed by the Contractor, or its Subcontractors or consultants shall be subject to the inspection and approval of the Authority at all times in accordance with the provisions set out in this Contract, but such approval shall not relieve the Contractor of responsibility for the proper performance of the Services. The Contractor shall provide sufficient, safe, and proper facilities at all times for such inspection of the Services and shall furnish all information concerning the Services and give the Authority or its representatives free access at all reasonable times to the facilities where the Services are performed.

(b) To the extent required in this Contract, complete records of all inspection work performed by the Contractor shall be maintained and made available to the Authority during Contract performance and for as long afterwards and the Contract requires.

(c) On reasonable notice, the Authority has the right to inspect and test all Services called for by this Contract, and is practicable, at all reasonable times and places during the term of the Contract. The Authority shall perform inspections and tests in a manner that will not unduly delay the Services.

(d) If any of the Services do not conform with Contract requirements in material respect, the Authority may require the Contractor to perform the Services again in conformity with the Contract requirements, at no increase in the Contract Sum. When the defects in services cannot be corrected by performance, the Authority may require the Contractor to take necessary action to ensure that future performance conforms to Contract requirements.

(e) If the Contractor fails promptly to perform the Services again or to take the necessary action to ensure future performance in conformity with Contract requirements, the Authority may (1) by contract or otherwise, perform the Services and charge to the Contractor any cost incurred by the Authority that is directly related to the performance of such service or (2) terminate the Contract for default.

28. SUSPENSION OF SERVICES

(a) The Authority may order the Contractor in writing to suspend all or any part of the Services for such period of time as the Authority determines to be appropriate for the convenience of the Authority.

(b) If the performance of all or any part of the Services is suspended or delayed by an act of the Authority in the administration of this Contract, or by the Authority's failure to act within the time specified in this Contract (or, if no time is specified, within a reasonable time), an adjustment shall be made for any increase in cost of performance of this Contract (excluding profit) necessarily caused by such suspension or delay, and the Contract modified in writing accordingly. However, no adjustment shall be made under this paragraph for any suspension or delay to the extent (1) that performance would have been suspended or delayed by any other cause, including the fault or negligence of the Contractor, or (2) for which an equitable adjustment is provided for or excluded under any other provision of this Contract.

(c) No claim under this paragraph shall be allowed (1) for any costs incurred more than twenty (20) days before the Contractor shall have notified the Authority in writing of the act or failure to act involved (but this requirement shall not apply to a claim resulting from a suspension order), and (2) unless the claim, in an amount stated, is asserted in writing as soon as practicable after the termination of such suspension or delay, but not later than the date of final payment. No part of any claim based on the provisions of this subparagraph shall be allowed if not supported by adequate evidence showing that the cost would not have been incurred but for a delay within the provisions of this paragraph.

29. PAYMENT TO SUBCONTRACTORS

- (a) Payments by contractors to subcontractors associated with Authority contracts are subject to the time periods established in the Texas Prompt Payment Act, Tex. Gov't Code § 2251.
- (b) A false certification to the Authority under the provisions of the paragraph entitled "Invoicing and Payment" hereof may be a criminal offense in violation of Tex. Penal Code § 10.

30. FEDERAL, STATE AND LOCAL TAXES

The Contract Sum includes all applicable federal, state, and local taxes and duties. The Authority is exempt from taxes imposed by the State of Texas and local sales and use taxes under Texas Tax Code § 151.309, and any such taxes included on any invoice received by the Authority shall be deducted from the amount of the invoice for purposes of payment. The Contractor may claim exemption from payment of applicable State taxes by complying with such procedures as may be prescribed by the State Comptroller of Public Accounts. The Contractor bears sole and total responsibility for obtaining information pertaining to such exemption.

31. EQUAL OPPORTUNITY

During the performance of this Contract, the Contractor agrees that it will, in good faith, afford equal opportunity required by applicable federal, state, or local law to all employees and applicants for employment without regard to race, color, religion, sex, national origin, disability or any other characteristic protected by federal, state or local law.

32. CONFLICT OF INTEREST

- (a) Reference is made to Exhibit B, Representations and Certifications, Code of Ethics, which is incorporated herein and made a part of this Contract. Capitalized terms used in this paragraph and not otherwise defined shall have the meanings as described to them in the Code of Ethics.
- (b) The Contractor represents that no Employee has a Substantial Interest in the Contractor or this Contract, which Substantial Interest would create or give rise to a Conflict of Interest. The Contractor further represents that no person who has a Substantial Interest in the Contractor and is or has been employed by the Authority for a period of two (2) years prior to the date of this Contract has or will (1) participate, for the Contractor, in a recommendation, bid, proposal or solicitation on any Authority contract, procurement or personnel administration matter, or (2) receive any pecuniary benefit from the award of this Contract through an ownership of a Substantial Interest (as that term is defined in Paragraph II, subparagraphs (1) and (3) of the Code of Ethics) in a business entity or real property.
- (c) The Contractor agrees to ensure that the Code of Ethics is not violated as a result of the Contractor's activities in connection with this Contract. The Contractor agrees to immediately inform the Authority if it becomes aware of the existence of any such Substantial Interest or Conflict of Interest, or the existence of any violation of the Code of Ethics arising out of or in connection with this Contract.
- (d) The Authority may, in its sole discretion, require the Contractor to cause an immediate divestiture of such Substantial Interest or elimination of such Conflict of Interest, and failure of the Contractor to so comply shall render this Contract voidable by the Authority. Any willful violation of these provisions, creation of a Substantial Interest or existence of a Conflict of Interest with the express or implied knowledge of the Contractor shall render this Contract voidable by the Authority.
- (e) In accordance with paragraph 176.006, Texas Local Government Code, "vendor" is required to file a conflict-of-interest questionnaire within seven business days of becoming aware of a conflict of interest under Texas law. The conflict of interest questionnaire can be obtained from the Texas Ethics Commission at www.ethics.state.tx.us. The questionnaire shall be sent to the Authority's Contract Administrator.

33. GRATUITIES

The Authority may cancel this Contract, without liability to the Contractor, if it is found that gratuities in the form of entertainment, gifts, or otherwise were offered or given by the Contractor or any agent or representative to any Au-

thority official or employee with a view toward securing favorable treatment with respect to the performance of this Contract. In the event this Contract is canceled by the Authority pursuant to this provision, the Authority shall be entitled, in addition to any other rights and remedies, to recover from the Contractor a sum equal in amount to the cost incurred by the Contractor in providing such gratuities.

34. PUBLICATIONS

All published material and written reports submitted under this Contract must be originally developed material unless otherwise specifically provided in the Contract document. When material, not originally developed, is included in a report, it shall have the source identified. This provision is applicable when the material is in a verbatim or extensive paraphrased format.

35. REQUEST FOR INFORMATION

(a) The Contractor shall not provide information generated or otherwise obtained in the performance of its responsibilities under this Contract to any party other than the Authority and its authorized agents except as otherwise provided by this Contract or after obtaining the prior written permission of the Authority.

(b) This Contract, all data and other information developed pursuant to this Contract shall be subject to the Texas Public Information Act. The Authority shall comply with all aspects of the Texas Public Information Act.

(c) The Contractor is instructed that any requests for information regarding this Contract and any deliverables shall be referred to the Authority.

(d) The requirements of Subchapter J, Chapter 552, Government Code, may apply to this bid/contract and the contractor or vendor agrees that the contract can be terminated if the contractor or vendor knowingly or intentionally fails to comply with a requirement of that subchapter.

(1) The requirement of Subchapter J, Chapter 552, Government Code as amended currently applies to expenditures of at least \$1 million in public funds for the purchase of goods or services.

36. RIGHTS TO PROPOSAL AND CONTRACTUAL MATERIAL

(a) All non-proprietary documentation related to or prepared in connection with any proposal, including the contents of any proposal contracts, responses, inquiries, correspondence, and all other material submitted in connection with the proposal shall become the property of the Authority upon receipt.

(b) All documents, reports, Customer Data, graphics required to be delivered to Customer under this Contract shall become the sole possession of the Authority upon receipt and payment, subject to Cubic's proprietary rights in any material within those documents. Customer may make copies of any such material for its business purposes.

37. LIMITATION OF LIABILITY

37.1 No Consequential Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY WILL HAVE ANY LIABILITY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING, AS A RESULT OF ANY DELAY IN RENDERING SERVICE, LOSS OF DATA, LOSS OF USE, OR THE LOSS OF PROFIT OR REVENUE) ARISING OUT OF OR IN CONNECTION WITH THESE TERMS, HOWEVER CAUSED, AND UNDER WHATEVER CAUSE OF ACTION OR THEORY OF LIABILITY BROUGHT (INCLUDING UNDER ANY CONTRACT, NEGLIGENCE OR OTHER TORT THEORY OF LIABILITY) EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

37.2 Liability Cap. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL CUBIC'S LIABILITY FOR ANY CLAIM ARISING OUT OF OR IN CONNECTION WITH THESE TERMS (WHEN AGGREGATED WITH ITS LIABILITY FOR ALL OTHER CLAIMS ARISING OUT OF OR IN CONNECTION WITH THESE TERMS) EXCEED THE AMOUNTS PAID BY CUSTOMER TO CUBIC DURING THE 12-MONTH PERIOD IMMEDIATELY PRECEDING THE INCIDENT GIVING RISE TO SUCH LIABILITY.

37.3 Exceptions. THE EXCLUSIONS AND LIMITATIONS OF LIABILITY IN THIS SECTION 37 SHALL NOT APPLY TO (A) INTENTIONAL TORT OR FRAUD, (B) A BREACH BY A PARTY OF ITS CONFIDENTIALITY

OBLIGATIONS UNDER THIS CONTRACT; (B) A PARTY'S INDEMNIFICATION OBLIGATIONS UNDER THIS CONTRACT (OR ANY AMOUNTS PAID OR PAYABLE IN CONNECTION WITH SUCH OBLIGATIONS); (C) A PARTY'S LIABILITY FOR PERSONAL INJURY OR PHYSICAL HARM; OR (D) CUSTOMER'S BREACH OF ANY LICENSE GRANTED IN RESPECT OF CONTRACTOR'S OR ITS LICENSORS PROPRIETARY MATERIAL.

The Contractor shall include similar liability provisions in all its Subcontracts.

38. LAWS, STATUTES AND OTHER GOVERNMENTAL REQUIREMENTS

The Contractor agrees that it shall be in compliance with all laws, statutes, and other governmental requirements, regulations or standards prevailing during the term of this Contract.

39. CLAIMS

In the event that any claim, demand, suit, or other action is made or brought by any person, firm, corporation, or other entity against the Contractor arising out of this Contract, the Contractor shall give written notice thereof, to the Authority within three (3) working days after being notified of such claim, demand, suit, or action. Such notice shall state the date and hour of notification of any such claim, demand, suit, or other action; the name and address of the person, firm, corporation, or other entity making such claim or instituting or threatening to institute any type of action or proceeding; the basis of such claim, action, or proceeding; and the name of any person against whom such claim is being made or threatened. Such written notice shall be delivered either personally or by mail and shall be directly sent to the attention of the President/CEO, Capital Metropolitan Transportation Authority, 2910 E. 5th Street, Austin, Texas 78702.

40. LICENSES AND PERMITS

The Contractor shall, without additional expense to the Authority, be responsible for obtaining any necessary licenses, permits, and approvals for complying with any federal, state, county, municipal, and other laws, codes, and regulations applicable to the Services to be provided under this Contract including, but not limited to, any laws or regulations requiring the use of licensed Subcontractors to perform parts of the work.

41. NOTICE OF LABOR DISPUTES

(a) If the Contractor has knowledge that any actual or potential labor dispute is delaying or threatens to delay the timely performance of this Contract, the Contractor immediately shall give notice, including all relevant information, to the Authority.

(b) The Contractor agrees to insert the substance of this paragraph, including this subparagraph (b), in any Subcontract under which a labor dispute may delay the timely performance of this Contract; except that each Subcontract shall provide that in the event its timely performance is delayed or threatened by delay by any actual or potential labor dispute, the Subcontractor shall immediately notify the next higher tier Subcontractor or the Contractor, as the case may be, of all relevant information concerning the dispute.

42. PUBLICITY RELEASES

All publicity releases or releases of reports, papers, articles, maps, or other documents in any way concerning this Contract or the Services hereunder which the Contractor or any of its Subcontractors desires to make for the purposes of publication in whole or in part, shall be subject to approval by the Authority prior to release.

43. INTEREST OF PUBLIC OFFICIALS

The Contractor represents and warrants that no employee, official, or member of the Board of the Authority is or will be pecuniarily interested or benefited directly or indirectly in this Contract. The Contractor further represents and warrants that it has not offered or given gratuities (in the form of entertainment, gifts or otherwise) to any employee, official, or member of the Board of the Authority with a view toward securing favorable treatment in the awarding, amending, or evaluating the performance of this Contract. For breach of any representation or warranty in this paragraph, the Authority shall have the right to terminate this Contract without liability and/or have recourse to any other remedy it may have at law or in equity.

44. INDEMNIFICATION

(a) THE CONTRACTOR WILL INDEMNIFY, DEFEND AND HOLD THE AUTHORITY AND ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS AND REPRESENTATIVES (THE AUTHORITY AND EACH SUCH PERSON OR ENTITY IS AN "INDEMNIFIED PARTY") HARMLESS FROM AND AGAINST AND PAY ANY AND ALL DAMAGES (AS DEFINED HEREIN) DIRECTLY OR INDIRECTLY RESULTING FROM, RELATING TO, ARISING OUT OF OR ATTRIBUTABLE TO ANY OF THE FOLLOWING:

(1) ANY BREACH OF ANY REPRESENTATION OR WARRANTY THAT THE CONTRACTOR HAS MADE IN THIS CONTRACT;

(2) ANY BREACH, VIOLATION OR DEFAULT BY OR THROUGH THE CONTRACTOR OR ANY OF ITS SUBCONTRACTORS OF ANY OBLIGATION OF THE CONTRACTOR IN THIS CONTRACT;

(3) THE USE, CONDITION, OPERATION OR MAINTENANCE OF ANY PROPERTY, VEHICLE, FACILITY OR OTHER ASSET OF THE AUTHORITY TO WHICH THE CONTRACTOR HAS ACCESS OR AS TO WHICH THE CONTRACTOR PROVIDES SERVICES; OR

(4) ANY ACT OR OMISSION OF THE CONTRACTOR OR ANY OF ITS SUBCONTRACTORS OR ANY OF THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, CUSTOMERS, INVITEES, REPRESENTATIVES OR VENDORS.

(b) "ACTION" MEANS ANY ACTION, APPEAL, PETITION, PLEA, CHARGE, COMPLAINT, CLAIM, SUIT, DEMAND, LITIGATION, MEDIATION, HEARING, INQUIRY, INVESTIGATION OR SIMILAR EVENT, OCCURRENCE OR PROCEEDING.

(c) "DAMAGES" MEANS ALL DIRECT OR INDIRECT DAMAGES, LOSSES, LIABILITIES, DEFICIENCIES, SETTLEMENTS, CLAIMS, AWARDS, INTEREST, PENALTIES, JUDGMENTS, FINES, OR OTHER COSTS OR EXPENSES OF ANY KIND OR NATURE WHATSOEVER INCURRED BY A THIRD PARTY, WHETHER KNOWN OR UNKNOWN, CONTINGENT OR VESTED, MATURED OR UNMATURED, INCURRED BY SUCH THIRD PARTY OR THE AUTHORITY (INCLUDING COSTS (INCLUDING, WITHOUT LIMITATION, REASONABLE FEES AND EXPENSES OF ATTORNEYS, OTHER PROFESSIONAL ADVISORS AND EXPERT WITNESSES) RELATED TO ANY INVESTIGATION, ACTION, SUIT, ARBITRATION, APPEAL, CLAIM, DEMAND, INQUIRY, COMPLAINT, MEDIATION, INVESTIGATION OR SIMILAR EVENT, OCCURRENCE OR PROCEEDING CONCERNING SUCH DAMAGES.

(d) "THREATENED" MEANS A DEMAND OR STATEMENT HAS BEEN MADE (ORALLY OR IN WRITING) OR A NOTICE HAS BEEN GIVEN (ORALLY OR IN WRITING), OR ANY OTHER EVENT HAS OCCURRED OR ANY OTHER CIRCUMSTANCES EXIST THAT WOULD LEAD A PRUDENT PERSON OR ENTITY TO CONCLUDE THAT AN ACTION OR OTHER MATTER IS LIKELY TO BE ASSERTED, COMMENCED, TAKEN OR OTHERWISE PURSUED IN THE FUTURE.

(e) IF ANY ACTION IS COMMENCED OR THREATENED THAT MAY GIVE RISE TO A CLAIM FOR INDEMNIFICATION (A "CLAIM") BY ANY INDEMNIFIED PARTY AGAINST THE CONTRACTOR, THEN SUCH INDEMNIFIED PARTY WILL PROMPTLY GIVE NOTICE TO THE CONTRACTOR AFTER SUCH INDEMNIFIED PARTY BECOMES AWARE OF SUCH CLAIM. FAILURE TO NOTIFY THE CONTRACTOR WILL NOT RELIEVE THE CONTRACTOR OF ANY LIABILITY THAT IT MAY HAVE TO THE INDEMNIFIED PARTY, EXCEPT TO THE EXTENT THAT THE DEFENSE OF SUCH ACTION IS MATERIALLY AND IRREVOCABLY PREJUDICED BY THE INDEMNIFIED PARTY'S FAILURE TO GIVE SUCH NOTICE. THE CONTRACTOR WILL ASSUME AND THEREAFTER DILIGENTLY AND CONTINUOUSLY CONDUCT THE DEFENSE OF A CLAIM WITH COUNSEL THAT IS SATISFACTORY TO THE INDEMNIFIED PARTY. THE INDEMNIFIED PARTY WILL HAVE THE RIGHT, AT ITS OWN EXPENSE, TO PARTICIPATE IN THE DEFENSE OF A CLAIM WITHOUT RELIEVING THE CONTRACTOR OF ANY OBLIGATION DESCRIBED ABOVE. IN NO EVENT WILL THE CONTRACTOR APPROVE THE ENTRY OF ANY JUDGMENT OR ENTER INTO ANY SETTLEMENT WITH RESPECT TO ANY CLAIM WITHOUT THE INDEMNIFIED PARTY'S PRIOR WRITTEN APPROVAL, WHICH WILL NOT BE UNREASONABLY WITHHELD. UNTIL THE CONTRACTOR ASSUMES THE DILIGENT DEFENSE OF A CLAIM, THE INDEMNIFIED PARTY MAY DEFEND AGAINST A CLAIM IN ANY MANNER THE INDEMNIFIED PARTY REASONABLY DEEMS APPROPRI-

ATE. THE CONTRACTOR WILL REIMBURSE THE INDEMNIFIED PARTY PROMPTLY AND PERIODICALLY FOR THE DAMAGES RELATING TO DEFENDING AGAINST A CLAIM AND WILL PAY PROMPTLY THE INDEMNIFIED PARTY FOR ANY DAMAGES THE INDEMNIFIED PARTY MAY SUFFER RELATING TO A CLAIM.

(f) THE INDEMNIFICATION OBLIGATIONS AND RIGHTS PROVIDED FOR IN THIS CONTRACT DO NOT REQUIRE (AND SHALL NOT BE CONSTRUED AS REQUIRING) THE CONTRACTOR TO INDEMNIFY, HOLD HARMLESS, OR DEFEND ANY INDEMNIFIED PARTY (OR ANY THIRD PARTY) AGAINST ANY ACTION OR CLAIM (OR THREATENED ACTION OR CLAIM) TO THE EXTENT SUCH ACTION OR CLAIM IS ALLEGED TO HAVE BEEN CAUSED BY THE NEGLIGENCE OR FAULT, THE BREACH OR VIOLATION OF A STATUTE, ORDINANCE, GOVERNMENTAL REGULATION, STANDARD, OR RULE, OR THE BREACH OF CONTRACT OF ANY INDEMNIFIED PARTY, ITS AGENTS OR EMPLOYEES, OR ANY THIRD PARTY UNDER THE CONTROL OR SUPERVISION OF ANY INDEMNIFIED PARTY, OTHER THAN THE CONTRACTOR OR ITS AGENTS, EMPLOYEES, OR SUBCONTRACTORS OF ANY TIER.

(g) THIS PARAGRAPH WILL SURVIVE ANY TERMINATION OR EXPIRATION OF THIS CONTRACT.

45. RECORD RETENTION: ACCESS TO RECORDS AND REPORTS

(a) The Contractor will retain and will require its Subcontractors of all tiers to retain, complete and readily accessible records related in whole or in part to the Contract, including, but not limited to, data, documents, reports, statistics, sub-agreements, leases, subcontracts, arrangements, other third party agreements of any type, and supporting materials related to those records.

(b) If the Contractor submitted certified cost or pricing data in connection with the pricing of this Contract or if the Contractor's cost of performance is relevant to any change or modification to this Contract, the Authority and its representatives shall have the right to examine all books, records, documents, and other data of the Contractor related to the negotiation, pricing, or performance of such Contract, change, or modification for the purpose of evaluating the costs incurred and the accuracy, completeness, and currency of the cost or pricing data submitted. The right of examination shall extend to all documents necessary to permit adequate evaluation of the costs incurred and the cost or pricing data submitted, along with the computations and projections used therein.

(c) The Contractor shall maintain all books, records, accounts and reports required under this paragraph for a period of at not less than three (3) years after the date of termination or expiration of this Contract, except in the event of litigation or settlement of claims arising from the performance of this Contract, in which case records shall be maintained until the disposition of all such litigation, appeals, claims or exceptions related thereto.

(d) Subject to being given reasonable written notice as to the date, nature, and scope of an audit, the Contractor agrees to provide sufficient access to the Authority and its contractors during its normal business hours to inspect and audit, at its own cost and expense, records and information related to performance of this Contract as reasonably may be required. .

(e) The Contractor agrees to permit the Authority and its contractors' access to the sites of performance during its normal business hours under this Contract as reasonably may be required.

(f) If an audit pursuant to this paragraph reveals that the Authority has paid any invoices or charges not authorized under this Contract, the Authority may offset or recoup such amounts against any indebtedness owed by it to the Contractor, whether arising under this Contract or otherwise, over a period of time equivalent to the time period over which such invoices or charges accrued.

(g) This paragraph will survive any termination or expiration of this Contract.

46. EXCUSABLE DELAYS

(a) Except for payment obligations, neither party shall have any liability to the other party under this Contract if a party is prevented from or delayed in performing its obligations as a result of an Excusable Delay. Except for defaults of Subcontractors at any tier, the Contractor shall not be in default because of any failure to perform this Contract under its terms if the failure arises from Force Majeure Events or any failure by the Authority to perform under this Contract (an "Excusable Delay"). In each instance, the failure to perform must be beyond the control and without the fault or negligence of the Contractor. "Default" includes failure to make progress in the performance of the Services.

(b) If the failure to perform is caused by the failure of a supplier or Subcontractor at any tier to perform or make progress, and if the cause of the failure was beyond the control of both the Contractor and the supplier or Subcontractor and without the fault or negligence of either, the Contractor shall not be deemed to be in default, unless:

- (1) the subcontracted supplies or services were immediately obtainable from other sources at an equivalent costs;
- (2) the Authority ordered the Contractor in writing to obtain these services from the other source; and
- (3) the Contractor failed to comply reasonably with this order.

(c) In the event of an Excusable Delay, the party experiencing such delay shall promptly notify the other party of the nature of the delay and its initial assessment of any impact it has had or will have on the Services. Contractor shall, to the extent caused by the Excusable Event, be entitled to (i) schedule and performance relief and (ii) other than where the Excusable Delay is caused by a Force Majeure Event, additional costs. The impact of the Excusable Delay shall be memorialized through a Change Order. Upon the request of the Contractor, the Authority shall ascertain the facts and extent of the failure. If the Authority determines that any failure to perform results from one or more of the causes above, the delivery schedule or period of performance shall be revised, subject to the rights of the Authority under this Contract.

47. LOSS OR DAMAGE TO PROPERTY

The Contractor shall be responsible for any loss or damage to property including money securities, merchandise, fixtures and equipment belonging to the Authority or to any other individual or organization, if any such loss or damage was caused by the Contractor or any Subcontractor at any tier, or any employee thereof, while such person is on the premises of the Authority as an employee of the Contractor or Subcontractor.

48. CONTRACTOR CONTACT/AUTHORITY DESIGNEE

The Contractor shall provide the Authority with a telephone number to ensure immediate communication with a person (not a recording) anytime during Contract performance. Similarly, the Authority shall designate an Authority representative who shall be similarly available to the Contractor.

49. QUALITY ASSURANCE

A periodic review of the Contractor's scheduled work may be performed by the Authority. If work is deemed incomplete or unacceptable in any way, the Authority will determine the cause and require the Contractor to take corrective measures in accordance with the terms of the Contract.

50. INTERPRETATION OF CONTRACT – DISPUTES

All questions concerning interpretation or clarification of this Contract, or the acceptable fulfillment of this Contract by the Contractor shall be immediately submitted in writing to the Authority's Contracting Officer for determination. All determinations, instructions, and clarifications of the Contracting Officer shall be final and conclusive unless the Contractor files with the CapMetro President/CEO within two (2) weeks after the Authority notifies the Contractor of any such determination, instruction or clarification, a written protest, stating in detail the basis of the protest. The President/CEO shall consider the protest and notify the Contractor within two (2) weeks of the protest filing of his or her final decision. The President/CEO's decisions shall be conclusive subject to judicial review. Notwithstanding any disagreement the Contractor may have with the decisions of the President/CEO, the Contractor shall proceed with the Services in accordance with the determinations, instructions, and clarifications of the President/CEO. The Contractor shall be solely responsible for requesting instructions or interpretations and liable for any cost or expenses arising from its failure to do so. The Contractor's failure to protest the Contracting Officer's determinations, instructions, or clarifications within the two-week period shall constitute a waiver by the Contractor of all of its rights to further protest.

51. TOBACCO FREE WORKPLACE

(a) Tobacco products include cigarettes, cigars, pipes, snuff, snus, chewing tobacco, smokeless tobacco, dipping

tobacco and any other non-FDA approved nicotine delivery device.

(b) The tobacco free workplace policy refers to all CapMetro owned or leased property. Note that this includes all buildings, facilities, work areas, maintenance facilities, parking areas and all Authority owned vehicles.

(c) Tobacco use is not permitted at any time on CapMetro owned or leased property, including personal vehicles parked in CapMetro parking lots.

(d) Littering of tobacco-related products on the grounds or parking lots is also prohibited.

52. ORDER OF PRECEDENCE

In the event of inconsistency between the provisions of this Contract, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order, as revised:

1. Exhibit A - Pricing Schedule
2. Exhibit B - Representations and Certifications
3. Exhibit E - Contractual Terms and Conditions
4. Exhibit G – Authorization of Work Product
5. Exhibit F – Scope of Services and Compliance Matrix
6. Exhibit H – Proprietary Rights and Data Security Addendum
7. Exhibit I – Access and Use Agreement
8. Exhibit L...Maintenance and Services Agreement
9. The Umo Services Agreement
10. Exhibits to the Umo Services Agreement
11. Other mutually agreeable modification, as applicable, to the Contract.

53. ANTI-CORRUPTION AND BRIBERY LAWS

The Contractor shall comply with all Applicable Anti-Corruption and Bribery Laws. The Contractor represents and warrants that it has not and shall not violate or cause the Authority to violate any such Anti-Corruption and Bribery Laws. The Contractor further represents and warrants that, in connection with supplies or Services provided to the Authority or with any other business transaction involving the Authority, it shall not pay, offer, promise, or authorize the payment or transfer of anything of value, directly or indirectly to: (a) any government official or employee (including employees of government owned or controlled companies or public international organizations) or to any political party, party official, or candidate for public office or (b) any other person or entity if such payments or transfers would violate applicable laws, including Applicable Anti-Corruption and Bribery Laws. Notwithstanding anything to the contrary herein contained, the Authority may withhold payments under this Contract, and terminate this Contract immediately by way of written notice to the Contractor, if it believes, in good faith, that the Contractor has violated or caused the Authority to violate the Applicable Anti-Corruption and Bribery Laws. The Authority shall not be liable to the Contractor for any claim, losses, or damages related to its decision to exercise its rights under this provision.

54. ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

(a) This Contract may task the Contractor to prepare or assist in preparing work statements that directly, predictably and without delay are used in future competitive acquisitions. The parties recognize that by the Contractor providing this support a potential conflict of interest arises as defined by FAR 9.5.

(b) For the purposes of this paragraph, the term “Contractor” means the Contractor, its subsidiaries and affiliates, joint ventures involving the Contractor, any entity with which the Contractor may hereafter merge or affiliate and any other successor or assignee of the Contractor.

(c) The Contractor acknowledges the full force and effect of this paragraph. It agrees to be bound by its terms and conditions and understands that violation of this paragraph may, in the judgment of the Contracting Officer, be cause for Termination for Default. The Contractor also acknowledges that this does not represent the sole and exclusive remedy available to the Authority in the event the Contractor breaches this or any other Organizational Conflict of Interest paragraph.

55. MISCELLANEOUS

(a) This Contract does not intend to, and nothing contained in this Contract shall create any partnership, joint venture or other equity type agreement between the Authority and the Contractor.

(b) All notices, statements, demands, requests, consents or approvals required under this Contract or by law by either party to the other shall be in writing and may be given or served by depositing same in the United States mail, postage paid, registered or certified and addressed to the party to be notified, with return receipt requested; by personally delivering same to such party; an agent of such party; or by overnight courier service, postage paid and addressed to the party to be notified; or by e-mail with delivery confirmation. Notice deposited in the U.S. mail in the manner hereinabove described shall be effective upon such deposit. Notice given in any other manner shall be effective only if and when received by the party to be notified.

If to the Contractor: As set forth in Exhibit B to this Contract

If to the Authority: Capital Metropolitan Transportation Authority
Attn: Chief Contracting Officer
2910 E. 5th Street
Austin, Texas 78702

Address for notice can be changed by written notice to the other party.

(c) In the event the Authority finds it necessary to employ legal counsel to enforce its rights under this Contract, or to bring an action at law, or other proceeding against the Contractor to enforce any of the terms, covenants or conditions herein, the Contractor shall pay to the Authority its reasonable attorneys' fees and expenses, regardless of whether suit is filed.

(d) If any term or provision of this Contract or any portion of a term or provision hereof or the application thereof to any person or circumstance shall, to any extent, be void, invalid or unenforceable, the remainder of this Contract will remain in full force and effect unless removal of such invalid terms or provisions destroys the legitimate purpose of the Contract in which event the Contract will be terminated.

(e) This Contract represents the entire agreement between the parties concerning the subject matter of this Contract and supersedes any and all prior or contemporaneous oral or written statements, agreements, correspondence, quotations and negotiations. In executing this Contract, the parties do not rely upon any statement, promise, or representation not expressed herein. This Contract may not be changed except by the mutual written agreement of the parties.

(f) A facsimile signature shall be deemed an original signature for all purposes. For purposes of this paragraph, the phrase "facsimile signature" includes without limitation, an image of an original signature.

(g) Whenever used herein, the term "including" shall be deemed to be followed by the words "without limitation". Words used in the singular number shall include the plural, and vice-versa, and any gender shall be deemed to include each other gender. All Exhibits attached to this Contract are incorporated herein by reference.

(h) All rights and remedies provided in this Contract are cumulative and not exclusive of any other rights or remedies that may be available to the Authority, whether provided by law, equity, statute, or otherwise. The election of any one or more remedies the Authority will not constitute a waiver of the right to pursue other available remedies.

(i) The Contractor shall not assign the whole or any part of this Contract or any monies due hereunder without the prior written consent of the Contracting Officer. Notwithstanding, the Contractor may assign this Contract in connection with the sale of all or substantially all its assets, equity interests or business or to any affiliated entity without the prior written consent of the Authority. With respect to any assignment, Contractor is required to provide the Authority with written notice of such assignment in order to reflect the proper contracting parties to this Contract. No assignment shall relieve the Contractor from any of its obligations hereunder. Any attempted assignment, transfer or other conveyance in violation of the foregoing shall be null and void.

(j) The failure of the Authority to insist upon strict adherence to any term of this Contract on any occasion shall

not be considered a waiver or deprive the Authority thereafter to insist upon strict adherence to that term or other terms of this Contract. Furthermore, the Authority is a governmental entity, and nothing contained in this Contract shall be deemed a waiver of any rights, remedies or privileges available by law.

(k) This Contract shall be governed by and construed in accordance with the laws of the State of Texas. Any dispute arising with respect to this Contract shall be resolved in the state or federal courts of the State of Texas, sitting in Travis County, Texas and the Contractor expressly consents to the personal jurisdiction of these courts.

(l) This Contract is subject to the Texas Public Information Act, Tex. Gov't Code, Chapter 552.

(m) The Contractor represents, warrants and covenants that: (a) it has the requisite power and authority to execute, deliver and perform its obligations under this Contract; and (b) it is in compliance with all applicable laws related to such performance.

(n) The person signing on behalf of the Contractor represents for himself or herself and the Contractor that he or she is duly authorized to execute this Contract.

(o) No term or provision of this Contract is intended to be, or shall be, for the benefit of any person, firm, organization, or corporation for a party hereto, and no such other person, firm, organization or corporation shall have any right or cause of action hereunder.

(p) CapMetro is a governmental entity and nothing in this Contract shall be deemed a waiver of any rights or privileges under the law.

(q) Funding for this Contract after the current fiscal year is subject to revenue availability and appropriation of funds in the annual budget approved by the Authority's Board of Directors.

(r) Time is of the essence for all delivery, performance, submittal, and completion dates in this Contract.

56. FUNDING AVAILABILITY

Funding after the current fiscal year of any contract resulting from this solicitation is subject to revenue availability and appropriation of funds in the annual budget approved by the Authority's Board of Directors.

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

<div>Instructions:</div> <div><div>•For each Compliance Term, select "C-Comply", "N-Cannot Comply" or "A-Will Comply with Alternative."</div><div>•The comments section shall be used for "A-WILL COMPLY WITH AN ALTERNATIVE" for explaining the alternative, or where requested in the Compliance Term column.</div><div>•Do not add comments for "C" or "N" unless instructed otherwise.</div><div>• The selected Contractor ("Contractor") must deliver a system encompassing all requirements including delivery of third-party products to make the solution fully functional.</div><div>• The requirements in the Scope of Services and Compliance Matrix are functional in nature and do not encompass all requirements. The Contractor shall determine, through the Plan and Design phases, the impacts of the Fare System Solution and specific technical modifications needed to carry out the intent herein. The Contractor shall document and discuss said needs with CapMetro and implement the agreed-upon solution accordingly.</div><div>•Contractor must deliver all Compliance Terms unless it is within a section marked "Optional" that is not exercised by CapMetro or CapMetro agrees to an alternative.</div><div>•The final column entitled "Test #" shall be used during the Develop Phase when the Contractor will update the Compliance Matrix with the test number that responds with each line.</div><div>•The Project and Project Schedule shall use the Enterprise Project and Portfolio Phase Tasks and Deliverables shown on Appendix A.</div><div>•Answer all questions on Appendix B Technical Questions</div></div>			
1.0	Overview		
1.1	<div>Introduction. Capital Metropolitan Transportation Authority (“CapMetro”) is requesting proposals for product and services to provide, install and integrate a Customer Payment System replacement, to include on-board validators and a SaaS platform for Account Based Ticketing and Open Loop Payments. The approach must maximize the out-of-the-box functionality of a SaaS Solution to minimize development of customizations and complexity for future supportability and upgradability. The selected Contractor shall supply all hardware, software, licenses and services to fully configure, integrate, and rollout to CapMetro, the Customer Payment Systems Solution.</div> <div>CapMetro connects people, jobs and communities by providing Central Texans with safe, high-quality and sustainable transportation alternatives. The agency provides 30 million rides annually on its buses, trains, paratransit and vanpool vehicles and serves a population of more than 1.2 million in its 543-square-mile service area. The region’s transportation leader, CapMetro has invested in transit services like its High-Frequency Network, which move more people, more reliably, as well as its innovative on-demand service Pickup. CapMetro is committed to increasing regional mobility and, through Project Connect, will transform how people travel throughout Central Texas. Visit capmetro.org for more information.</div>		
	Compliance Term	Vendor Notes	CapMetro Notes
1.2	<div>Fare Strategy Vision. CapMetro seeks to upgrade its existing mobile ticketing fare equipment/systems and implement an account-based, multimodal fare collection system using open architecture that is flexible and scalable to support growth and business changes, and capable of accepting a variety of payments, bringing CapMetro and the region into the next generation of fare payment technology and offerings. The system shall be simple to use, convenient for the customer, and cost-effective to maintain. The upgrade will meet CapMetro's Fare Strategy by providing the following prime objectives:</div> <div><div>•Fast and Easy payment options</div><div>•Equity in payment options</div><div>•Retail network with reloadable smart cards and virtual account</div><div>•Account-based system integrated to all fare systems to increase fare options and programs</div><div>•Faster boarding</div><div>•Simplify fares to increase adoption and build ridership</div><div>•Accept payment in as many forms as possible</div><div>•Simple and straightforward operation so that CapMetro can troubleshoot customer problems</div><div>•Open APIs for integration with other systems (e.g. Transit App, third-party bike sharing, ride sharing, mobility as a service, and parking)</div></div>		
1.3	<div>Scope and Schedule.</div> <div>These are targeted dates. Please confirm your ability to meet or provide alternative timelines.</div> <div>Projected go-live and project completion dates:</div> <div><div>•Estimated Notice of Award (NOA) / Notice to Proceed (NTP): July 22, 2024 / July 26, 2024</div><div>•Phase 1: SaaS platform, Account Based Ticketing with Product Based Farecapping, customer mobile app, customer and partner websites, inspection/validation/citation app, Customer Service and Admin Portals, reporting tools, API available for exporting data to a data warehouse, cash digitization network integration, Flowbird TVM integration, training, testing and project management, as well as installs of new validators across the fixed route fleet: 3/1/2025</div><div>•Phase 2 (Pickup Expansion): Extension of offering to our microtransit fleet (CapMetro Pickup), including new validators: 6/1/2025</div><div>•Phase 3 (Installation of Expansion Vehicles): As vehicles become available 9/1/2025</div></div> <div>Project Completion: September 15, 2025</div>		
1.4	<div>Project Management & Milestones. Project Management must comply with CapMetro's Enterprise Portfolio Project Management (EPPM) outline in Appendix A - EPPM Phases.</div>		

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
2.0	Customer Payment System - Mobile App:				
2.1	Vendor will provide a fully function mobile application. The application will allow for purchasing tickets, managing accounts and displaying a graphical ticket that can be used for fare payment at a fare validator via an optical interface. The graphical ticket should be a dynamic 2D barcode that prevents copying.				
2.2	The customer mobile app will also allow for trip planning and have next departure information available for nearby stops.				
2.3	The customer mobile app will be customizable by CapMetro to allow links to internal websites, which will display within the app.				
2.4	The mobile app will allow for Near Field Communication for the validation of tickets on the fare validators.				
2.5	The customer mobile app will be tested and support the two most recent major versions of operating systems on the Android and iOS platforms on the day that the OS is released to the general public.				
2.6	The customer mobile app will be available in the app stores, offered and maintained by the vendor.				
3.0	Customer Payment System - Web Portal:				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
3.1	The customer web portal, partner portal and merchant shall be branded with CapMetro colors and logo at a minimum.				
3.2	The web portal shall have the ability to be displayed in frame on the CapMetro website.				
3.3	The customer web portal shall allow all customers to access and control their customer accounts over the web. Customers include individuals and businesses. Customers will access varying functionality through the website based on their customer account type.				
3.4	The customer web portal and mobile app shall utilize the same user login.				
4.0	Customer Payment System - Customer Accounts				
4.1	Customers shall be able to create an account using just a username, though the preferred minimum information shall include a phone number registered to the account.				
4.2	Accounts shall allow for the management of purchased tickets and wallet value.				
4.3	Customers shall have the ability to load value into their wallets using stored credit and debit cards from all major providers.				
4.4	Customers shall have the ability to purchase tickets using stored credit and debit cards from all major providers.				
4.5	Customers shall have the ability to purchase tickets or load value into their account using Apple Pay and Google Pay.				
4.6	Customers shall have the ability to link accounts to allow for the purchase of tickets for other family members or dependents.				
4.7	Ability to set role-based security access; audit system changes recording user performing the change				
4.8	Provides robust centralized configuration and software deployment/versioning/management				
5.0	Customer Payment System - Fare Validators				
5.1	Vendor shall provide physical fare validators, such as the HID Val 100, in the quantities specified and provide installation of hardware, including any mounting kits or cabling required.				
5.2	Validators shall have the ability to process contactless payments, read barcodes, use Near Field Communication or RFID to validate tickets or process fares.				
5.3	The validator shall be EMV Level 2 certified.				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
5.4	The validator will be PCI and SRED compliant for contactless payments using major payment processors (VISA, MasterCard, AMEX).				
5.5	The validator shall by ITxPT approved.				
5.6	Validators shall fully integrate with the vendor's backend for health monitoring and troubleshooting.				
6.0	Customer Payment System - Design & Architecture				
6.1	Software upgrades will be centrally managed and fully tested prior to installation. The System shall be able to roll-back to previous software versions without adversely impacting operations.				
6.2	Security patches and updates will be deployed quarterly at a minimum, to the back end system as well as the mobile app platforms.				
6.3	CapMetro will own all data entered into the system.				
6.4	<p>Vendor shall design the System to be compliant with applicable standards, laws, and regulations to ensure that the System:</p> <ul style="list-style-type: none">• Presents no safety hazards for customers and CapMetro employees.• Will withstand the rigors of the environments in which the equipment will be installed, and the public use to which it will be subjected.• Provides for the secure storage and transmittal of data.• Is designed using state-of-the-art methods to maximize quality.• Satisfies federal, state, and other requirements for ergonomics and usability. <p>Applicable codes, laws, ordinances, statutes, standards, rules, and regulations include, but are not be limited to the list below (in 6.5.1). The latest revisions in effect at the time of Final System Acceptance will apply.</p>				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
6.4.1	<div><ul style="list-style-type: none">Americans with Disabilities Act (ADA)Americans with Disabilities Act Accessibility Guidelines (ADAAG)Advanced Encryption StandardANSI X9.24, Financial Services Retail Key ManagementEuropean Norm EN55022, Emissions standards for CE markingEuropean Norm EN55024, Immunity standards for CE markingFCC Part 15 Class B – Radio Frequency DevicesFIPS 140-2IEEE 802.11 a/b/g/n standard for wireless data communicationsIEEE 802.11 i standard for wireless data network securityIEEE 802.11-2016International Electrotechnical Commission Standard 529 (IEC529)ISO/IEC 7810, Identification Cards – Physical CharacteristicsISO 9001ISO/IEC-8583 – Financial transaction card originated messagesISO/IEC 14443 Parts 1 through 4 – Contactless Smart Card StandardISO/IEC 18092 / ECMA-340, Near Field Communication Interface and Protocol-1ISO/IEC 21481 / ECMA-352, Near Field Communication Interface and Protocol-2</div> <div>National Electrical Code (NFPA 70)</div> <div><ul style="list-style-type: none">National Electrical Manufacturers Association Publication 250-2003National Electrical Safety Code (ANSI C2)National Fire Protection Association (NFPA) 130NCITS 322-2002, American National Standard for Information Technology – Card Durability Test MethodsOccupational Safety and Health Administration (OSHA)Payment Card Industry Data Security Standards (PCI-DSS)Payment Card Industry Payment Application Data Security Standards (PA-DSS)Society of Automotive Engineers SAE J1113-13 Electrostatic DischargeSociety of Automotive Engineers SAE J1455 Vibration and ShockUL Standard 60950, “Information Technology Equipment – Safety”World Wide Web Consortium, Mobile Web Application Best PracticesWeb Content Accessibility Guidelines WCAG 2.0</div>				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
6.5	In the case of conflict between the provisions of codes, laws, ordinances, statutes, standards, rules, and regulations, the more stringent requirement will apply.				
6.6	System shall be maintained in a cloud environment allowing for "always up" availability.				
6.7	Vendor shall certify that a plan for the processes that will be used to resume operations in the event of a data loss due to a natural disaster or other emergency situation that puts operations at risk exists. The plan must describe how mission-critical functions will be resumed and how longer-term challenges created by an unexpected loss will be addressed. The Disaster Recovery (DR) plan will conform to the required service level agreement.				
6.8	The System will support fraud prevention policies, including the ability to automatically identify suspect usage patterns based on sales and ridership data, and block the use of fare media, accounts, and fare products based on configurable fraud rules.				
6.9	Customer sensitive data such as passwords and credit card numbers shall be encrypted at rest and in transit.				
6.10	Meet or exceed CapMetro’s required system uptime of 99.99% 24x7x365; A separate Warranty & Maintenance (WMA) Agreement must be submitted with the proposal, based on the WMA template provided by CapMetro.				
6.11	Application security testing – Vendor shall provide an overview of their application testing including annual pen testing, testing by 3rd party, testing by security professional services, and testing that covers the common vulnerabilities as described by OWASP Top 10. Describe the process for vulnerabilities identified and remediations.				
6.12	The System will support the addition of new agencies, including fare rules that are part of the existing design.				
6.13	The System will integrate with CapMetro's GTFS-RT feed.				
6.14	Integrations with third-party products including, but not limited to: Ticket Vending Machine, Onboard Validator, Data Warehouse, Enterprise Resource Planner (ERP), etc.				
6.15	APIs shall be made available for account creation, account management, export of data, integration to Ticket Vending Machines and integration with Transit App.				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
6.16	Vendor will provide a mobile app to support fare inspection and sale of passes.				
7.0	Customer Payment System - Retail Network Integration				
7.1	Vendor shall integrate with the Incomm retail network for cash digitization.				
8.0	Customer Payment System - Fare Policy				
8.1	The System will support the current fare structure as a foundation. Fare structure includes the supported fare policies, fare media, and fare products through which customers purchase fare media and products. The fare structure will be configurable by CapMetro, and designed to be upgraded to a simple, unified system that enables interoperability across current and future transit modes without additional development.				
8.2	The tariff will be configurable in such a way that CapMetro may implement different fare policies for different payment methods, e.g. no capping benefits if paying with open payments.				
8.3	The tariff fare capping program shall offer the ability to specify the customers with eligible access to capping by offering settings limit within a product group or for all customers.				
8.4	Fare policy business rules will be used to determine the fare charged to the rider on the basis of applicable passenger types, fare structures (including mode), and fare products.				
8.5	The System will support a variety of fare policies and products, including stored value wallet, transfers, reduced fares for eligible customers, daily and monthly pass products, multi-ride products, programs that require riders to pre-qualify (e.g., active-duty military, low-income program), programs by customer account type, and other CapMetro-specific programs.				
8.6	The System will support stored value, which will serve as an electronic cash-equivalent, and will be accepted for payment across all modes and services. When stored value is used for payment, the System will deduct the correct fare at each boarding or entry in real-time from the account, based on the fare pricing configuration.				
8.8	Fare policy business rules will be used to determine the fare charged to the rider on the basis of applicable passenger types, fare structures (including mode), and fare products.				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
8.9	The system will support fare capping. If fare capping is enabled, riders will pay per boarding up until a capping threshold; at this point, riders will no longer be charged for their boardings for the remainder of the specified time period				
8.10	The system will support the setting of multiple fare cap time periods, each with their own capped price threshold. Fare cap time periods will be configurable for anywhere from 1 to 366 days. The capping time periods will be calendar-based, not rolling.				
8.11	The system will support separate fare cap price thresholds for different services and different rider categories. This could include a single multiple that is applied to all base fares to establish the relevant caps.				
8.12	The system will support calendar products that are valid for unlimited rides during a predefined calendar period for rides on services costing at or below the face value of the pass. The system will also support rolling products that are valid for unlimited rides on services costing at or below the face value of the product for a predefined period starting at product activation, which may occur upon sale or first use. Calendar and rolling products do not need to be simultaneously supported.				
8.12	The System will support date-based and promotional pricing that offers discounted fares on a temporary and permanent basis, up to and including the offering of free fares. Discounted fare pricing will be able to be configured for specific fare media types, passenger types, modes, service types, and routes, and put into effect indefinitely or for a defined period.				
8.13	The System will support fare products and pricing for business accounts, school pass programs, group fares, and other bulk fare sales.				
8.14	Accounts will be able to contain multiple fare products simultaneously (e.g., stored value and a pass product).				
8.15	The configurable service day may be longer than 24 hours, and service day hours may overlap. Pass products will be configurable to extend the validity to the end of the last service day.				
8.16	Day passes and short-term products (e.g., convention passes) will activate upon first tap, and the validity period will be configurable to accommodate specified transit days.				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
8.13	A passenger type must be defined for each account. The default passenger type that will be associated with a account will be the Adult full fare passenger type. Passenger types include but are not limited to: <ul style="list-style-type: none">• Adult full fare• Youth K-12• Emergency and Active-duty military• MetroAccess• Reduced fare Additional passenger types will be able to be defined by CapMetro.				
8.14	An account may only have one passenger type associated with it.				
8.15	Passenger types will be able to be modified and configured manually, or automatically based on customer date of birth or the granting of a temporary classification with a configurable end date.				
9.0	Customer Payment System - Fare Media				
9.1	System will be able to support virtual and physical fare media.				
9.2	CapMetro-issued EU fare cards will be printed with a unique non-sequential 16-digit serial number that is distinct from the card's Unique Identification Number (UID). Each card will also be printed with a randomized three-digit security code. CapMetro will provide an electronic file that lists each card with its UID, serial number and security code.				
9.3	EU fare cards will be worthless until activated at time of sale.				
9.4	EU fare cards will have the ability to be managed within the mobile app and customer web app.				
10.0	Customer Payment System - TVM Integration:				
10.1	Vendor shall integrate with the Flowbird Ticket Vending Machine via API.				
10.2	Vendor will have the ability to validate barcodes printed at a Flowbird TVM.				
10.3	Customers shall have the ability to load value to their digital wallet at a Flowbird TVM, using cash.				
10.0	Warranty & Support: Contractor provides training, spares, and RMA of parts for CapMetro personnel who will provide field services to meet the SLAs and provisions of the WMA.				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
10.1	Contractor will provide the requirements of CapMetro providing field technician(s) and first-line software support (perform diagnostics and troubleshooting) to include recommendation of number of full-time equivalent employees (FTE) to support. Describe fully in the Comments column.				
10.2	CapMetro will provide field technician(s) to perform preventative maintenance and Return Merchandise Authorization (RMA) repairs (replacing components)				
10.3	CapMetro will investigate presenting software issues and submit tickets to Contractor that Contractor shall resolve				
11.0	Delivery of systems and services				
11.1	Provide an order form that lists individual products, services, components, and pricing for placing orders.				
12.0	System Design & Architecture - Accessibility and ADA Compliance				
12.1	<p>Vendor shall design the System to be compliant with current accessibility standards, laws, and regulations to ensure that the System meets or exceeds the Americans with Disabilities Act (ADA) and accessibility requirements of federal, Texas State and Austin regional governments unless otherwise agreed to in writing by CapMetro and the vendor.</p> <p>The vendor shall ensure compliance with all ICT equipment and system interfaces and create/execute an Accessibility Compliance Plan to document compliance. This plan will be used throughout design and implementation to ascertain that all accessibility requirements will be met and used to track compliance.</p>				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
12.2	<p>COMPLIES WITH WCAG 2.1 AA ACCESSIBILITY STANDARDS AND MEETS ALL FOUR SUCCESS CRITERIA.:</p> <p>CapMetro uses WCAG 2.1 AA as the technical accessibility standard but is obligated under the ADA to general nondiscrimination and effective communication. The vendor must, at a minimum, comply with the WCAG 2.1 AA technical standard, understanding that CapMetro may require additional modifications to meet ADA requirements unless the vendor and CapMetro agree in writing to a modified scope.</p> <ul style="list-style-type: none">- All screens are compatible with assistive technologies including screen readers and screen magnification- Screens make proper use of forms mode, include alt tags on all data collection boxes and image fields, and metadata read back is strictly limited.- Properly labelled images and proper use of alt tags is required.- The ability to navigate pages, utilize functionality and traverse layouts without a mouse is required.- Users of assistive technology shall have ways to skip redundant navigation.- Correct headings and labelling structures for pages, forms and data tables.- Readable content with sufficient contrast ratios and font sizing. <p>- Contractor shall provide information about user testing with people with disabilities and the results of such testing.</p> <p>- Software solution shall be compatible with all applicable standards and/regulations regarding accessible information technology resources and (IRIT). In cases where there is conflict between standards the most stringent standard shall be applicable.</p>				
12.3	<p>Vendor has key accessibility development, verification, and delivery policies and procedures that include integrating Information and Communications Technology (ICT) activities into product and service development. Examples include but are not limited to incorporating accessibility into development procedures, accessibility verification steps throughout the project, and subsystem or component procurement for ICT that will become part of the deliverable, etc.</p> <p>The vendor is required to document the extent to which they do not comply with this requirement in the Proposer Question section.</p>				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX

	Compliance Term	Vendor Response	Vendor Notes	CapMetro Notes	Test #
12.4	The vendor attests that the skills and training resources to develop and produce accessible Information and Communications Technology (ICT) products and services exist prior to engagement.				

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix A: Enterprise Project and Portfolio Management (EPPM) Phase Tasks Deliverables

EPPM Phase Tasks and Deliverables. The Contractor shall perform the following phase tasks and provide the associated deliverables required to deploy all hardware, software, updates and configurations resulting in a fully functional and tested system. Contractor shall obtain CapMetro review of all deliverables and make changes and updates to deliverables per CapMetro review as needed. CapMetro acceptance of all deliverables for each phase as evidenced by a signed phase acceptance certificate is required prior to invoicing. Each phase is closed by Contractor's Phase Completion Notification with Proof of Deliverables, CapMetro's Acceptance Certificate Signoff, and Contractor's Invoice upon Receipt of CapMetro Authorization to Invoice.	
1.0	<p>Plan. Meet with CapMetro project manager and business area stakeholders for project planning, including review of proposed schedule, roles and responsibilities, as well as conduct a complete review of functionality to be delivered, and other project activities. Plan Deliverables:</p> <div><div><div>1. Project organization chart</div><div>2. Project schedule (draft)</div><div>3. Action Items and Issues log (AIL)</div><div>4. Review and comment on CapMetro Project Management Plan</div><div>5. Infrastructure and Integration Audit</div></div><div><div>6. Initiate Risk Register</div><div>7. System Implementation Plan (draft)</div><div>8. Compliance Matrix Review and Update</div><div>9. Kick-off meeting and base product demo with stakeholders to review and clarify requirements including confirmation of any required updates to CapMetro’s environment</div></div></div>
2.0	<p>Design. Contractor's technical requirements gathering and detailed design, beginning with on-site assessment and discussion with affected CapMetro departments. This phase will determine how the system will be installed, product wireframe presentation to the customer, and how it will be managed in the back end. The Contractor will work with CapMetro to develop materials that will provide a basis to help instruct CapMetro stakeholders in the easiest and most efficient way to use the system to their utmost advantage.</p> <p>Design Deliverables:</p> <div><div><div>1. On-Site Assessment; Documentation of Findings</div><div>2. Configuration Management Document (“CMD” - Draft)</div><div>3. Wireframe diagrams (Draft)</div><div>4. System Implementation Plan (Final)</div><div>5. Disaster Recovery Plan (Draft)</div><div>6. Quality Assurance Plan (Draft) CapMetro only confirms QA/QC; Plan shall clearly delineate that the Contractor performs QA/QC process</div><div>7. Risk Management Plan participation (Final)</div><div>8. Data dictionary and Entity Relationship Diagram (ERD)</div></div><div><div>9. Project Schedule (Baseline) with Resource Loading</div><div>10. Network architecture diagram (Draft)</div><div>11. Electrical and communication connection designs (Draft)</div><div>12. Installation Plan (Draft): equipment installation design, procedures, schedule, CapMetro support required; detailed so CapMetro can perform installation & deinstallation if desired post-implementation</div><div>13. Deinstallation Plan (Draft)</div><div>14. Review of Design and System Implementation Plan with Stakeholders</div><div>15. Update of Design based on review</div><div>16. Review and Acceptance of CapMetro Project Management Plan</div><div>17. Compliance Matrix Review and Update</div></div></div>
3.0	<p>Develop. Development, configuration and installation of the solution and integration as well as installation within a development and a test environment so configuration and testing of the required functionality can be started. This task will include setting the initial configuration values by the Contractor so they can be tested and changed if needed. During this phase, the rollout of the system must be worked on to include training all IT and Operational staff who will use or have on-going support roles. Develop Deliverables:</p> <div><div><div>1. Quality Assurance Plan Including QA/QC Checklist (Final)</div><div>2. Test Environment Installation that provides CapMetro full access throughout the project and the life of the system</div><div>3. Supporting Infrastructure Implemented</div><div>4. Application and Functionality Development</div><div>5. Test Procedure/Plan including test Scripts, use cases, acceptance test criteria demonstrating each Compliance Matrix term is developed and meets requirement (Draft)</div><div>6. Update Compliance Matrix with Test Number(s)</div><div>7. CMD Values Test and Update</div><div>8. High-level Training of CapMetro Staff to Prepare for Test Phase</div><div>9. Warranty and Maintenance Plan Review</div><div>10. Review and Feedback of CapMetro Support Responsibility Matrix</div></div><div><div>11. Role-based, On-site Training Plan for all User Types (Draft):<ul style="list-style-type: none">•Training schedule and course outlines for review a minimum of three weeks prior to the scheduled classes•Separate training sessions for revenue, customer service maintenance and system administrator roles•Provide all materials necessary to train participants (CapMetro will provide space and laptops)•Schedule the training staff to be on site timely to ensure equipment, materials, student accounts and classroom are fully ready for when class begins•Arrange for an instructor(s) with thorough knowledge of the material covered in the course(s) and the ability to effectively lead the knowledge transfer•Provide customized training manuals specific to CapMetro's environment in Microsoft Word and PDF. Contractor shall provide the agreed-to number of hard copies</div></div></div>
4.0	<p>Test. Integration and testing by Contractor and CapMetro to determine that all functionality required of the installed solution, software, and integrations into the existing environment is in place and working. The testing phase shall not be deemed complete until all functional requirements of the newly implemented system have been fully tested and approved by the project team. The Contractor shall provide a Test Procedure document with test scripts, use cases and acceptance test criteria for review and acceptance by CapMetro for all phases. Only CapMetro data is to be used for testing. Before CapMetro performs any testing, the Contractor shall provide the written test results of the full test procedure/plan demonstrating no Class 1 or Class 2 failures. Test Deliverables:</p> <div><div><div>1. Document Procedures and Migrate Environment from development to test, stage and production</div><div>2. Contractor’s Successfully Test Procedure/Plan Results</div><div>3. Documentation including User, System Admin, Maintenance, Installation and Training Manuals, (Draft)</div><div>4. Test Procedure/Plan including Test Scripts, Use Cases and Acceptance Test Criteria (Final)</div><div>5. System Acceptance Test (SAT) Plan Developed (Subset to Use to Determine Go, No-Go before Go Live)</div><div>6. Security Penetration Test</div><div>7. Disaster Recovery Test – End-to-End</div><div>8. Installation Plan (Final)</div><div>9. System Acceptance Test (SAT)</div><div>10. Introduction to Contractor’s Support Manager and Team</div><div>11. Detailed Processes and Contact Information for Post Go Live Support</div></div><div><div>12. Test Failure Log & Remediation Plan. Contractor shall lead testing of the solution including integrations and resolve all Significant (Class 1) and Severe (Class 2) Test Failure Results (TFRs). Contractor shall endeavor to resolve Minor (Class 3) TFRs during this phase; however, the requirement for Class 3 resolution is during the Closeout phase. Definition for each class are as follows:<ul style="list-style-type: none">•Severe - A Class 1 test failure is a severe defect that prevents, inhibits, or significantly impairs further testing or operation of the system.•Significant - A Class 2 test failure is a significant defect that does not prevent further testing or has a minimal effect on normal operations of the system.•Minor – A Class 3 test failure is a minor or isolated defect that does not impact or invalidate the testing or normal operations of the system.</div><div>13. Regression Testing of the Entire Test Plan for Any Class 1 and Class 2 Failures</div><div>14. Compliance Matrix Review and Update</div></div></div>

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix A: Enterprise Project and Portfolio Management (EPPM) Phase Tasks Deliverables

EPPM Phase Tasks and Deliverables. The Contractor shall perform the following phase tasks and provide the associated deliverables required to deploy all hardware, software, updates and configurations resulting in a fully functional and tested system. Contractor shall obtain CapMetro review of all deliverables and make changes and updates to deliverables per CapMetro review as needed. CapMetro acceptance of all deliverables for each phase as evidenced by a signed phase acceptance certificate is required prior to invoicing. Each phase is closed by Contractor's Phase Completion Notification with Proof of Deliverables, CapMetro's Acceptance Certificate Signoff, and Contractor's Invoice upon Receipt of CapMetro Authorization to Invoice.

5.0	<p>Deploy/Go Live: Deploy: once all the test failures have been corrected, the Contractor shall install and configure the software and incorporate it into the live environment. Go Live: the system shall go live and be monitored for the first 30 days of operation. If Severe (Class 1) or Significant (Class 2) issues arise, the Go-Live period may be cancelled, extended or restarted. The Contractor shall be required to participate in the monitoring of the system and respond to issues so they are quickly resolved. Deploy/Go Live Deliverables:</p> <div><div><div>1. Conduct Training for all User Types</div><div>2. Document Procedures and Migrate Environment from Test to Production</div><div>3. QA/QC checklist Sign off</div><div>4. Delivery and Inventory of Spares (e.g. optional hand-held devices)</div><div>5. Update to Disaster Recovery Plan</div><div>6. Delivery of all Documentation including User, System Admin, Maintenance, Installation and Training Manuals, (Revise Draft)</div><div>7. Deinstall existing hardware for the immediate removal and safe disposal, in a manner that does not interrupt ticket sales and validation</div><div>8. Deployment, Implementation, Configuration and Integration of the dms solution with all environments</div></div><div><div>9. During contract period, Contractor shall provide a storage container for equipment storage and CapMetro will provide space for container</div><div>10. System Acceptance Test (SAT)</div><div>11. Resolution of SAT TFRs</div><div>12. Go Live Schedule and Transition Plan</div><div>13. System Go Live</div><div>14. Technical Lead On-site During First Week of Go Live, or Longer if System Issues are Experienced</div><div>15. Review and coordinate with CapMetro to update CapMetro Business Process Flowcharts for dms Solution Effectiveness</div><div>16. Revised (final) Copies of all Required Documentation including User and Training Manuals</div><div>17. Compliance Matrix Review and Update</div></div></div>
6.0	<p>Close. Obtain acceptance by CapMetro to formally close the project. Apply appropriate updates to project documents. Close out all procurement activities ensuring termination of all relevant agreements. Close Deliverables:</p> <div><div><div>1. Follow-up training on areas identified during Go Live and Training Documentation (Final)</div><div>2. Data dictionary and Entity Relationship Diagram (Final)</div><div>3. Network architecture diagram (Final)</div><div>4. Electrical and communication connection designs (Final)</div><div>5. All AIL items closed</div><div>6. Resolution of all Minor (Class 3) TFRs</div></div><div><div>8. Final Documentation for Environment Refresh (Develop-Test-Stage-Production)</div><div>9. Disaster Recovery Plan (Final)</div><div>10. Configuration Management Documents (CMD – Final)</div><div>11. APIs and all documentation related to all integrations (Final)</div><div>12. Warranty and Maintenance Procedure Review and Forms</div><div>13. As-builts: updates to any documentation including design document changes</div><div>14. Participation in Lessons Learned</div></div></div>
<p>Project Management. The Contractor shall manage the project continuously beginning with the Notice to Proceed through Close, and shall lead the project and is expected to drive and manage all aspects of the project including the management of any subcontractors. CapMetro shall manage and coordinate all its resources. A full-time Project manager or technical lead is required to be onsite at least two weeks per month during each phase of the project. A PMP is preferred and shall be approved by CapMetro. Project Management Deliverables:</p>	
7.0	<div><div><div>1. Active Partnership with CapMetro in assuring Project Success</div><div>2. Onsite At Least Twice a Month During Each Project Phase (May Be Performed by Technical Lead Depending Upon Scheduled Activities By Agreement with CapMetro)</div><div>3. Single Point of Contact for All Communication Regarding Work Under This Contract</div><div>4. Task Coordination with The Designated CapMetro project manager</div><div>5. Regular Communication with The Project Manager and any other staff designated to discuss progress, critical risk factors, schedule, or unique issues that may surface.</div><div>6. Specification of CapMetro’s staff resources needed for project success with at least two weeks notice in advance within the project schedule.</div><div>7. Support Responsibility Matrix Review and Updates as Needed</div></div><div><div>8. Semi-monthly Status Meetings with Updated Schedule and AIL</div><div>9. Review and Feedback of Change Requests as Needed</div><div>10. Monthly Risk Registry Updates</div><div>11. Monthly Management Review Meetings</div><div>12. Monthly Project Status Report</div><div>13. Quarterly attendance and Status Presentation at Steering Committee Meetings</div><div>14. Responsible for ensuring all project documentation, including meeting minutes, AIL updates, project schedule and plans are kept updated in the CapMetro SharePoint site</div></div></div>

Change Control & Configuration Management	Outsourced Development	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?
	Management Quality Testing	CCC-03.3	Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?
	Unauthorized Software Installations	CCC-03.4 CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?
Data Security & Information Lifecycle Management	Classifications, eCommerce Transactions, Data Inventory / Flows	DSI-01.3	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you have a capability to use system geographic location as an authentication factor?
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?
		DSI-02.1	Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?
		DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?
	Nonproduction Data	DSI-05.1	Production data shall not be replicated or used in non-production environments.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?
	Secure Disposal	DSI-07.1	Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix B2:
TECHNICAL QUESTIONS

Datacenter Security	Asset Management	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership y defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?
	Controlled Access Points	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?
	User Access	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel? Does all remote access require 2 Factor authentication? What is the encryption methodology and ciphers used to protect the data?
Encryption & Key Management	Key Generation	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?
	Encryption	EKM-02.3 EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you maintain key management procedures? Do you encrypt tenant data at rest (on disk/storage) within your environment?
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?

Governance and Risk Management	Baseline Requirements	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?
		GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: <ul style="list-style-type: none"> • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance 	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?
	Policy	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?
	Policy Enforcement	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix B2:
TECHNICAL QUESTIONS

Human Resources	Policy Reviews	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?
	Asset Returns	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?
	Background Screening	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?
	Employment Agreements	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?
		HRS-03.3		Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?
	Employment Termination	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?
	Training / Awareness	HRS-09.5	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Are personnel trained and provided with awareness programs at least once a year?
Identity & Access Management	Audit Tools Access	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?

	User Access Policy	IAM-02.1	<p>User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:</p> <ul style="list-style-type: none"> • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) <ul style="list-style-type: none"> • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expirable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements 	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?
	Diagnostic / Configuration Ports Access	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?
	Policies and Procedures	IAM-04.1	<p>Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.</p>	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix B2:
TECHNICAL QUESTIONS

Source Code Access Restriction	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?
	IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?
	Third Party Access		
	IAM-07.7	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you share your business continuity and redundancy plans with your tenants?
	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?
User Access Reviews	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?
User Access Revocation	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix B2:
TECHNICAL QUESTIONS

Infrastructure & Virtualization Security	User ID Credentials	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: <ul style="list-style-type: none"> • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets) 	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?
		IAM-12.3		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?
		IAM-12.8		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?
	Audit Logging / Intrusion Detection	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?
	Clock Synchronization	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?
	OS Hardening and Base Controls	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?
	Production / Non-Production Environments	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?
		IVS-08.3		Do you logically and physically segregate production and non-production environments?

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix B2:
TECHNICAL QUESTIONS

	Segmentation	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: <ul style="list-style-type: none"> Established policies and procedures Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance Compliance with legal, statutory and regulatory compliance obligations 	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?
	VMM Security - Hypervisor Hardening	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?
	Wireless Security	IVS-12.1 IVS-12.2 IVS-12.3		Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic? Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)? Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network? Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?
Interoperability & Portability	APIs	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	
	Standardized Network Protocols	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?
Mobile Security	Approved Applications	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?
	Awareness and Training	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix B2:
TECHNICAL QUESTIONS

Security Incident Management, E-Discovery, & Cloud Forensics	Incident Management	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?
	Incident Reporting	SEF-02.4	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Do you have a dedicated security team?
		SEF-03.1		Have you tested your security incident response plans in the last year?
				Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?
	Incident Response Legal Preparation	SEF-03.2		What is your SLA for security incident notification?
				Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?
				Does your logging and monitoring framework allow isolation of an incident to specific tenants?
		SEF-04.2	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?
Supply Chain Management, Transparency, and Accountability	Data Quality and Integrity	SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?
				Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?
				Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within your supply chain?
	Incident Reporting	STA-01.2	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	
		STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?
Network / Infrastructure Services	Network / Infrastructure Services	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?

Third Party Agreements STA-05.4

Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:

- Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations)
- Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships

Do third-party agreements include provision for the security and protection of information and assets?

Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts

- Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)
- Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed
- Expiration of the business relationship and treatment of customer (tenant) data impacted
- Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence

STA-05.5

Do you have the capability to recover data for a specific customer in the case of a failure or data loss?

Supply Chain Metrics STA-07.4

Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream).

Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?

Reviews shall performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix B2:
TECHNICAL QUESTIONS

Threat and Vulnerability Management	Third Party Audits	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?
	Antivirus / Malicious Software	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?
	Vulnerability / Patch Management	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? How often do you perform vulnerability scans?
		TVM-02.2		What is your security patch process and how often do you push updates?
		TVM-02.3		Will the customers be impacted during updates and maintenance windows?
		TVM-02.5		Do you have a process for notifying customers of updates and maintenance?

Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?

Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?

Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?

4. Exhibit G - Authorization of Work Product

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

EXHIBIT G – AUTHORIZATION OF WORK PRODUCT

DESCRIPTION: Fare System Replacement
CONTRACT NO.: To be determined following contract award

Authority's Contracting Officer (CO)

- A. The CO for administration of this Contract is Jeffery Yeomans
B. Phone: 512-369-7727
C. Email: jeffery.yeomans@capmetro.org

The Contracting Officer is responsible for the general administration of the Contract, negotiation of any changes, and issuance of written modifications, task order revisions, or Change Orders (as it pertains to Construction Contracts Only and results in a Contract modification – see below) to the Contract. If the parties desire to modify the Contract, or revise the Task Order of the Contract, in any way, only the Contracting Officer is authorized to issue a written modification for authorized signatures.

Authority's Project Manager (PM)

- A. The PM for this Contract is Jonathan Tanzer
B. Phone: 512-369-6053
C. Email: jonathan.tanzer@capmetro.org

The Authority's PM for this Contract is responsible for the overall management and coordination of this Contract and will act as the central point of contact for the Authority. The PM has full authority to act for the Authority in the performance of any project connected to the Contract. However, the PM cannot authorize, in writing or orally, to commence any work. The PM shall meet with Contractor's PM to discuss problems as they occur. Any changes, including changes pursuant to the Changes clause in the Contract, will be handled solely by the CO. As needed, the Authority's PM may assist with development of Change Orders and Contract modifications with the Authority's CO.

Field Change Orders (Construction Contracts Only) – The Authority's PM is permitted to authorize work when an event occurs in the field during construction which requires immediate action. Immediately, but no later than three (3) business days following such action, the Authority's PM must provide a signed Change Order to the CO along with any other required procurement documentation in order to memorialize the Change Order in a task order revision or Contract modification.

The Contractor understands that should Contractor perform any work prior to written authorization by the Authority's CO, Contractor is not allowed to invoice for any additional cost or fee for services or goods under the Contract, nor is the Authority liable for any payment for any unauthorized work.

SIGNED and DATED

Frank Capone
Contractor – must sign and return with Offer

July 9, 2024
Date

to be signed by the Authority following contract award
Authority's Project Manager (PM)

Date

to be signed by the Authority following contract award
Authority's Contracting Officer (CO)

Date

IT PROPRIETARY RIGHTS AND DATA SECURITY ADDENDUM

Capital Metro Transportation Authority (“the Authority”) has invested extensive time, money and specialized resources into developing, collecting and establishing its tangible and intangible proprietary assets. This Proprietary Rights and Data Security Addendum (this “Addendum”) identifies and acknowledges the Authority’s proprietary rights, establishes baseline commitments regarding data security and represents a set of standard terms applicable to service providers and business partners when they enter into contracts with the Authority. Capitalized terms used in this Addendum have the meanings set forth in the Agreement, unless differently defined in this Addendum. The Contractor is responsible for ensuring compliance with the terms of this Addendum by the Contractor’s employees, agents and contractors and all of the restrictions and obligations in this Addendum that apply to the Contractor also apply to the Contractor’s employees, agents and contractors. The term “including” or “includes” means including without limiting the generality of any description to which such term relates.

1. DEFINITIONS

The following terms will have the meanings described below in this Addendum.

- (a) “Authority Data” means Customer Data as defined in the Umo Services Agreement.
- (b) “Authority Electronic Property” means:
 - (i) Not used,
 - (ii) Not used
 - (iii) the Authority’s CAD/AVL feeds (which are publicly available,
 - (iv) Not used, and
 - (v) versions and successors of the foregoing, any form or format now known or later developed, that may be used by customers obtaining products or services from the Authority.
- (c) “Contract” means that certain contract for products and services entered into between the Contractor and Authority to which this Addendum is attached or incorporated by reference.
- (d) “Data Law” means, as in effect from time to time, any law, rule, regulation, declaration, decree, directive, statute or other enactment, order, mandate or resolution, which is applicable to either the Contractor or the Authority, issued or enacted by any national, state, county, municipal, local, or other government or bureau, court, commission, board, authority, or agency, relating to data security, data protection and/or privacy. Data Laws also include ISO 27001 and ISO 27002, the most current Payment Card Industry Data Security Standard (the “PCI DSS”, and other industry standard practices) and any

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

financial standards or business requirements applicable to the Authority's business or the Authority Data and/or the Authority Electronic Property.

(e) "Personal Identifying Information" means any data that identifies or could be used to identify a natural person, including name, mailing address, phone number, fax number, email address, Social Security number, credit card or other payment data, date of birth, driver's license number, account number or user ID, PIN, or password.

(f) "Process" or "Processing" means, with respect to Authority Data, to collect, access, use, process, modify, copy, analyze, disclose, transmit, transfer, sell, rent, store, or retain or destroy such data in any form. For the avoidance of doubt, "Process" includes the compilation or correlation of Authority Data with information from other sources and the application of algorithmic analysis to create new or derivative data sets from Authority Data.

(g) "Remediation Efforts" means, with respect to any Security Incident, activities designed to remedy a Security Incident which may be required by a Data Law or by the Authority's or the Contractor's policies or procedures, or which may otherwise be necessary, reasonable or appropriate under the circumstances, commensurate with the nature of such Security Incident. Remediation Efforts may include:

- (i) development and delivery of legal notices to affected individuals or other third parties;
- (ii) establishment and operation of toll-free telephone numbers for affected individuals to receive specific information and assistance;
- (iii) procurement of credit monitoring, credit or identity repair services and identity theft insurance from third parties that provide such services for affected individuals;
- (iv) provision of identity theft insurance for affected individuals;
- (v) cooperation with and response to regulatory, government and/or law enforcement inquiries and other similar actions;
- (vi) undertaking of investigations (internal or in cooperation with a governmental body) of such Security Incident, including forensics;
- (vii) public relations and other crisis management services; and
- (viii) cooperation with and response to litigation with respect to such Security Incident (including, but not limited to, class action suits or similar proceedings); and in each case of examples (i) through (viii), payment of legal costs, disbursements, fines, settlements and damages.

(h) "Security Incident" means in respect of incidents related to Authority Data and/or Authority Electronic Property:

- (i) the loss or misuse of Authority Data and/or the Authority Electronic Property;
- (ii) the inadvertent, unauthorized, or unlawful processing, alteration, corruption, sale, rental, or destruction of the Authority Data and/or the Authority Electronic Property;
- (iii) unauthorized access to internal resources;
- (iv) programmatic manipulation of a system or network to attack a third party;
- (v) elevation of system privileges without authorization;
- (vi) unauthorized use of system resources;
- (vii) denial of service to a system or network; or
- (viii) any potential or confirmed exposure (which may stem from an act or omission to act) that would result in any of the events described in (i) through (viii).

(i) "Security Policies" means statements of direction for Security Requirements and mandating

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

compliance with applicable Data Laws. Typically, Security Policies are high level instructions to management on how an organization is to be run with respect to Security Requirements.

(j) “Security Procedures” means statements of the step-by-step actions taken to achieve and maintain compliance with Security Requirements.

(k) “Security Requirements” means the security requirements set forth below in Section 7 of this Addendum and any security requirements requested by the Authority from time to time.

(l) “Security Technical Controls” means any specific hardware, software or administrative mechanisms necessary to implement, maintain, comply with and enforce the Security Requirements. Security Technical Controls specify technologies, methodologies, implementation procedures, and other detailed factors or other processes to be used to implement and maintain Security Policies and Procedures relevant to specific groups, individuals, or technologies.

2. FISMA COMPLIANCE

Both parties will comply with all federal and state regulations, statutes, and laws that govern this Agreement which includes, without limitation, the Federal Information Security Management Act, 2006 (FISMA) to the extent applicable to the Authority’s business or the products and services provided by the Contractor. The Contractor accepts ultimate responsibility and liability for the protection and preservation of all Authority Data and the Authority Electronic Property through a security operational plan (the “Security Plan”). The Contractor will make available a current copy of the Security Plan for review upon the Authority’s request. FISMA requires organizations to meet minimum security requirements by selecting the appropriate security controls as described by NIST Special Publication (SP) 800-53 revision 4, “*Security and Privacy Controls for Federal Information Systems and Organizations*.” Note that organizations must always reference the most current version of NIST SP 800-53 for the security control selection process. The Contractor should meet the minimum-security requirements detailed in FIPS Publication 200.

3. AUTHORITY DATA

As between the Contractor and the Authority (*i.e.*, without addressing rights of third parties), the Authority is the sole owner of all rights, title and interest in and to Authority Data and the Authority Electronic Property. Except as expressly authorized in the Agreement, the Contractor may not use, edit, modify, create derivatives, combinations, or compilations of, combine, associate, synthesize, re-identify, reverse engineer, reproduce, display, distribute, disclose, sell or Process any Authority Data or Authority Electronic Property. The Contractor will not use Authority Data or Authority Electronic Property in a manner that is harmful to the Authority.

4. PERSONAL IDENTIFYING INFORMATION

The Contractor will comply with any Data Laws relating to the use, safeguarding, or Processing of any Personal Identifying Information, including any requirement to give notice to or obtain consent of the individual. In Processing any Personal Identifying Information, the Contractor will at all times comply with any posted privacy policy or other representations made to the person to whom the information is identifiable, and to communicate any limitations required thereby to any authorized receiving party (including any modifications thereto) in compliance with all Data Laws. The Contractor will ensure that any such receiving party abides by any such limitations, in addition to the requirements of the Agreement. Notwithstanding the foregoing, the Contractor represents and warrants that Personal Identifying Information will not be Processed, transmitted, or stored outside of the United States. The Contractor shall take reasonable steps to maintain the confidentiality of and will not reveal or divulge to any person or entity any Personal Identifying Information that becomes known to it during the term of this Contract. The Contractor must maintain policies and programs that prohibit unauthorized disclosure of Personal Identifying Information by its employees and subcontractors and promote training and awareness of information security policies and practices. The Contractor must comply, and must cause its employees,

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

representatives, agents, and subcontractors to comply, with such commercially and operationally reasonable directions as the Authority may make to promote the safeguarding or confidentiality of Personal Identifying Information. The Contractor must conduct background checks for employees or sub-Contractors that have access to Personal Identifying Information or systems Processing Personal Identifying Information. The Contractor must limit access to computers and networks that host Personal Identifying Information, including without limitation through user credentials and strong passwords, data encryption both during transmission and at rest, firewall rules, and network-based intrusion detection systems. In addition to the foregoing, to the extent that any Personal Identifying Information qualifies as Protected Health Information that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA," found at Public Law 104-191), and certain privacy and security regulations promulgated by the U.S. Department of Health and Human Services to implement certain provisions of HIPAA and the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), and its implementing regulations found in the Omnibus Final Rule (collectively the "HIPAA Regulations") found at 45 C.F.R. Parts 160, 162 and 164, the Contractor will execute and abide by the rights and obligations set forth in the Business Associate Agreement of the Authority.

5. NO IMPLIED RIGHTS

No right, license, permission, or ownership or other interest of any kind in or to any Authority Data or other intellectual property rights owned or licensed by the Authority is or is intended to be given or transferred to or acquired by the Contractor except as expressly stated in writing in the Contract including the permitted use of the Authority Data that falls under the definition of Customer Data in the Umo Services Agreement).

6. PROHIBITED INTERNET PRACTICES

The Contractor will not, and will not authorize or encourage any third party to, directly or indirectly:

- (a) use any automated, deceptive or fraudulent means to generate impressions, click-throughs, or any other actions in relation to advertisements or Internet promotions on Authority Electronic Property or in relation to advertisements or Internet promotions of the Authority (or its products or services) on third party websites; or
- (b) collect or Process data from an Authority Electronic Property other than as has been expressly authorized by the Authority in the Agreement or another written agreement with the Authority. Except as expressly allowed in the Agreement, the Contractor will not "screen-scrape" Authority Electronic Property or conduct any automated extraction of data from Authority Electronic Property or tracking of activity on Authority Electronic Property.

7. SECURITY REQUIREMENTS

The Contractor will apply reasonable physical, technical and administrative safeguards for Authority Data that is in the Contractor's possession or control in order to protect the same from unauthorized Processing, destruction, modification, or use that would violate the Agreement or any Data Law. The Contractor represents and warrants that the Security Policies, Security Procedures and Security Technical Controls as they pertain to the services being rendered to the Authority by the Contractor or its subcontractors and any Processing of Authority Data by the Contractor or its subcontractors will at all times be in material compliance with all Data Laws. In addition, the Contractor will require any of its employees, agents or contractors with access to Authority Data to adhere to any applicable Data Laws, and the Contractor represents and warrants that such employees, agents and contractors have not been involved in any violation of applicable Data Laws in the twenty-four months before the Effective Date. The Contractor will take into account the sensitivity of any Authority Data in the Contractor's possession in determining reasonable controls used to safeguard such Authority Data.

8. DATA SEGREGATION AND ACCESS

The Contractor will physically or logically segregate stored Authority Data from other data and will ensure that access to Authority Data is restricted to only authorized personnel through security measures. The

Contractor will establish and maintain appropriate internal policies, procedures and systems that are reasonably designed to prevent the inappropriate use or disclosure of Authority Data. For the avoidance of doubt, Authority acknowledges that the Contractor provides the services on a shared services platform hosting multiple customers and that data is segregated by the Contractor by tagging data in shared storage according to ownership and segregating access by means of access controls to the data.

9. PCI COMPLIANCE

If the Contractor Processes payment card data, cardholder data, or sensitive authentication data on behalf of the Authority or if the Contractor otherwise can impact the security of said data belonging to the Authority, the Contractor is responsible for the security of said data. The Contractor represents and warrants that it has performed an assessment to confirm that the material aspects of the Contractor's Security Policies, Security Procedures and Security Technical Controls (as they pertain to the services being rendered to the Authority by the Contractor or its subcontractors and any Processing of Authority Data by the Contractor or its subcontractors) comply with the PCI DSS and the Contractor will repeat this assessment each year during the Term. The Contractor will provide certification of compliance with this requirement upon request from the Authority.

10. SECURITY REVIEWS AND AUDITS

The Contractor will, upon request, provide the Authority with reports of any audits performed on the Contractor's Security Policies, Security Procedures or Security Technical Controls. If applicable, , such reports will include any certifications of the Contractor's agents and contractors. Additionally, the Contractor will respond within a reasonable time period to any inquiries from the Authority relating to the Contractor's and, if applicable, its agents' and contractors' Security Policies, Security Procedures and Security Technical Controls. The Contractor will, upon the Authority's request, provide the Authority or its representatives access to the Contractor's and its agents' and contractors' systems, records, processes and practices that involve Processing of Authority Data so that an audit may be conducted provided that such audit rights shall not include entitlement to any physical or independent access to Cubic systems or any rights to audit (i) the financial books or accounts of Cubic, (ii) Cubic's compliance with its internal security policies (iii) in a manner that requires Cubic to disclose any information related to any other customer of Cubic or (ii) apply to any service provider used by Cubic including but not limited to Cubic's cloud hosting provider. The Authority will not exercise such audit right more frequently than once per twelve (12) month period and the Authority will bear the full cost and expense of any such audit, unless such audit discloses a Security Incident or a material breach of this Addendum or the Agreement, in which case the Contractor will bear the full cost and expense of such audit and a further audit may be conducted by the Authority or its representatives within the current twelve (12) month period.

11. SECURITY INCIDENTS

The Contractor will timely and promptly notify the Authority upon discovering or otherwise learning of a Security Incident involving the Authority Data or the Authority Electronic Property, to the extent within the Contractor's access, possession or control. Following any Security Incident, the Contractor will consult in good faith with the Authority regarding Remediation Efforts that may be necessary and reasonable. The Contractor will:

- (a) at the Authority's direction undertake Remediation Efforts at the Contractor's sole expense and reimburse the Authority for its reasonable costs and expenses in connection with any Remediation Efforts it elects to undertake,
- (b) ensure that such Remediation Efforts provide for, without limitation, prevention of the

recurrence of the same type of Security Incident, and

- (c) reasonably cooperate with any Remediation Efforts undertaken by the Authority.
- (d) Without limiting the foregoing, the Contractor will:
 - (i) immediately undertake investigations (internal or in cooperation with a governmental body) of such Security Incident, including forensics,
 - (ii) timely share with the Authority any Security Incident-related information, reports, forensic evidence and due diligence obtained from the investigation into the Security Incident and cooperate with the Authority in response to regulatory, government and/or law enforcement inquiries and other similar actions, (iii) cooperate with the Authority with respect to any public relations and other crisis management services, and litigation with respect to such Security Incident (including, but not limited to, class action suits or similar proceedings); and in each instance of Security Incident, be liable and responsible for payment of legal costs, disbursements, fines, settlements and damages. To the extent that the Authority is bound to comply with any interlocal agreements pertaining to shared information (including the Authority Data), the Contractor agrees that it will comply with, and cooperate with the Authority in its compliance, with all rights and obligations pertaining to the Authority Data and/or the Authority Electronic Property under such interlocal agreements.

12. NOTICE TO THE AUTHORITY CUSTOMERS AND EMPLOYEES

Any notifications to any of the Authority's customers or employees regarding Security Incidents will be handled exclusively by the Authority and the Contractor may not under any circumstances contact the Authority's customers or employees relating to such Security Incident unless the Contractor is under a legal obligation to do so, in which event:

- (a) the Contractor must notify the Authority in writing promptly after concluding that the Contractor has the legal obligation to notify such customers or employees and explain in such notice to the Authority the basis for the legal obligation and
- (b) the Contractor will limit the notices to any of the Authority's customers and employees to those required by the legal obligation or as pre-approved by the Authority.
- (c) The Contractor will reasonably cooperate in connection with notices to the Authority's customers and employees regarding a Security Incident and the Contractor will assist with sending such notices if so requested by the Authority.

13. EQUITABLE RELIEF

The Contractor acknowledges that the Authority may have no adequate remedy at law if there is a breach or threatened breach of any of the obligations set forth in this Addendum and, accordingly, that the Authority may, in addition to any legal or other remedies available to the Authority, seek injunctive or other equitable relief to prevent or remedy such breach without requirement of a bond or notice. The Contractor will not object or defend against such action on the basis that monetary damages would provide an adequate remedy.

EXHIBIT I-Revised-1

IT ACCESS AND USE AGREEMENT

This Access and Use Agreement (this "Agreement") is entered into as of the effective date set forth on the signatory page between the undersigned person identified as the "Contractor" and Capital Metro Transportation Authority ("the Authority") concerning the terms and conditions under which the Authority will provide the Contractor with limited access and use of the Authority Data and/or the Authority Electronic Property in conjunction with the Contractor's performance of the Contract. The parties acknowledge and agree to the following terms and conditions:

1. DEFINITIONS

For purposes of this Agreement, capitalized terms shall have the meaning set forth below:

- (a) "Applicable Laws" means any and all applicable statutes, laws, treaties, rules, codes, ordinances, regulations, permits, interpretations, or orders of any Federal, state, or local governmental authority having jurisdiction over the Authority's or the Contractor's business the Contract, and the parties all as in effect as of the date of the Contract and as amended during the term of the Contract.
- (b) "Authority Data" means Customer Data as defined in the Umo Services Agreement
- (c) "Authority Electronic Property" means the Authority's CAD/AVL feeds (which are publicly available).
- (d) "Confidential Information" as used herein, shall mean and include, without limitation: (i) any information concern- ing the Authority, which is provided by or on behalf of the Authority to the Contractor, such as accounting and financial data, product, marketing, development, pricing and related business plans and budgets, and all of the information and plans related to the Authority's business, which are not published; (ii) all Authority Data; and (iii) the Authority Electronic Property and (iv) in respect of Contractor, product information, user manuals, data, pricing, financial information, end user information, software, specifications, research and development and proprietary algorithms and materials, that is (a) clearly and conspicuously marked as "confidential" or with similar designation or (b) is disclosed in a manner in which the disclosing Party reasonably communicated, or the receiving Party should reasonably have understood under the circumstances, that the disclosure should be treated as confidential, whether or not the specific designation "confidential" or any similar designation is used..
- (e) "Contract" means that certain contract for products and services entered into between the Contractor and Au- thority to which this Agreement is attached or incorporated by reference. The applicable reference number for the Contract may be set forth in the signatory page to this Agreement.
- (f) "Remediation Efforts" means, with respect to any Security Incident, activities designed to remedy a Security Incident, which may be required by Applicable Law or by the Authority's or the Contractor's policies or procedures or under the Security Requirements, or which may otherwise be necessary, reasonable or appropriate under the circumstances, commensurate with the nature of such Security Incident.
- (g) "Security Incident" means, in respect of incidents impacting Authority Data and/or the Authority Electronic Property: (i) the loss or misuse of the Authority Data and/or the Authority Electronic Property; (ii) the inadvertent, unauthorized, or unlawful processing, alteration, corruption, sale, rental, or destruction of Authority Data and/or the Authority Electronic Property; (iii) unauthorized access to internal resources; (iv) pro- grammatic manipulation of a system or network to attack a third party; (v) elevation of system privileges without authorization; (vi) unauthorized use of system resources; (vii) denial of service to a system or network; or (viii) any potential or confirmed exposure (which may stem from an act or omission to act) that would result in any of the events described in (i) through (viii).
- (h) "Security Requirements" means security measures under Applicable Laws, industry best practices and other reasonable physical, technical and administrative safeguards, procedures, protocols,

requirements and obligations related to facility and network security in order to protect the Authority Data and the Authority Electronic Property from unauthorized processing, destruction, modification, distribution and use, as approved in writing by the Authority, and all confidentiality and non-use or limited use obligations set forth in any license agreements or other third-party contracts (including interlocal agreement) applicable to the Authority Data and/or the Authority Electronic Property.

2. CONFIDENTIAL INFORMATION

The Contractor acknowledges and agrees that the Contract creates a relationship of confidence and trust on the part of the Contractor for the benefit of the Authority. During the term of the Contract, the Contractor may acquire certain Confidential Information from or regarding the Authority employees, agents and representatives or documents, or otherwise as a result of performing the services of the Contractor. The Contractor acknowledges and agrees that all such Confidential Information is and shall be deemed the sole, exclusive, confidential and proprietary property and trade secrets of the Authority at all times during the term of the Contract and following any expiration of termination thereof. Contractor may only use such information as permitted under the terms of this Contract.

3. STANDARD OF CARE

The Contractor agrees to hold in confidence without disclosing or otherwise using any Confidential Information, except as: such disclosure or use may be required in connection with and limited to the product and services of the Contractor. The Contractor acknowledges and agrees that the Authority would not have entered into the Contract unless the Authority were assured that all such Confidential Information would be held in confidence by the Contractor in trust for the sole benefit of the Authority.

4. EXCEPTIONS

The Contractor's obligation of confidentiality hereunder shall not apply to information that: (i) is already in the Contractor's possession without an obligation of confidentiality; (ii) is rightfully disclosed to the Contractor by a third party with no obligation of confidentiality; or (iii) is required to be disclosed by court or regulatory order, provided the Contractor gives the Authority prompt notice of any such order.

5. COMPLIANCE

The Contractor, as well as its agents, representatives, and employees, shall comply with all of the Authority's rules, regulations, and guidelines pertaining to the Authority Data and the Authority Electronic Property other than to extent that they conflict with Contractor's security policies and processes in respect of such Authority Data and the Authority Electronic Property and all Applicable Laws.

6. SECURITY REQUIREMENTS

The Umo Services Agreement will govern Data and Security.

Generally, Cubic shall maintain and operate the Umo Services in compliance with the Cubic's security and information security management policies that at a minimum will address a.) Compliance with applicable statutory, regulatory, legal and contractual requirements, including PCI-DSS; b.) how Cubic implements and maintains security practices in compliance with industry best practice; c.) organizational and risk management context for the establishment and maintenance of the security management process; d.) and Security monitoring practices and policies.

Cubic must ensure that it takes reasonable pre-cautions to ensure that facilities and systems are protected from loss, damage or other occurrence, including fire and environmental hazards and power interruptions, that may result in any of those facilities and systems being unavailable when required to provide the Umo Services.

7. SECURITY INCIDENT

The Contractor will timely and promptly notify the Authority upon discovering or otherwise learning of any Security Incident involving Authority Data but in no event shall such notice exceed the time periods for notice required under Applicable Laws. Following any Security Incident, the Contractor will consult in diligent good faith with the Authority regarding Remediation Efforts that may be necessary and reasonable. Without limiting the foregoing, the Contractor will (i) immediately undertake investigations (internal or in cooperation with a governmental body) of such Security Incident, including forensics, (ii) timely share with the Authority any Security Incident-related information, reports, forensic evidence and due diligence obtained from the investigation into the Security Incident and cooperate with the Authority in response to regulatory, government and/or law enforcement inquiries and other similar actions, (iii) co-operate with the Authority with respect to any public relations and other crisis management services, and litigation with respect to such Security Incident (including, but not limited to, class action suits or similar proceedings); and in each instance of Security Incident, be liable and responsible for payment of legal costs, disbursements, fines, settlements and damages. To the extent that the Authority is bound to comply with any interlocal agreements pertaining to shared information (including the Authority Data), the Contractor agrees that it will comply with, and cooperate with the Authority in its compliance, with all rights and obligations pertaining to the Authority Data under such interlocal agreements. The Contractor will timely and promptly notify the Authority upon discovering or otherwise learning of any Security Incident involving Authority Data but in no event shall such notice exceed the time periods for notice required under Applicable Laws. Following any Security Incident, the Contractor will consult in diligent good faith with the Authority regarding Remediation Efforts that may be necessary and reasonable. Without limiting the foregoing, the Contractor will (i) immediately undertake investigations (internal or in cooperation with a governmental body) of such Security Incident, including forensics, (ii) timely share with the Authority any Security Incident-related information, reports, forensic evidence and due diligence obtained from the investigation into the Security Incident and cooperate with the Authority in response to regulatory, government and/or law enforcement inquiries and other similar actions, (iii) cooperate with the Authority with respect to any public relations and other crisis management services, and litigation with respect to such Security Incident (including, but not limited to, class action suits or similar proceedings); and in each instance of Security Incident, be liable and responsible for payment of legal costs, disbursements, fines, settlements and damages. To the extent that the Authority is bound to comply with any interlocal agreements pertaining to shared information (including the Authority Data), the Contractor agrees that it will comply with, and cooperate with the Authority in its compliance, with all rights and obligations pertaining to the Authority Data under such interlocal agreements.

8. LIMITED ACCESS AND USE

The Authority authorizes the Contractor to access and use and to the extent necessary to perform the Services to install and use the Authority Data and/or Authority Electronic Property provided or made available by the Authority solely for the purposes of providing products and services for the benefit of or on behalf of the Authority under and during the term of the Contract and to improve the products and

services. The Umo Services Agreement shall govern Data and Security. Generally, between the Parties, Customer shall own all right, title, and interest in and to the Customer's Data.

Customer Data shall be treated as Customer's Confidential Information and Cubic Data shall be treated as Cubic's Confidential Information

9. NO OWNERSHIP

The Umo Services Agreement shall govern Proprietary rights of the parties. Specifically, the Umo Services Agreement, provides in pertinent part, as follows:

Authority acknowledges and agrees that Contractor and/or its licensors own all Intellectual Property Rights in the Services, the Documentation, and all modifications, improvements and derivative works thereof. Except to the extent expressly set forth in this Umo Services Agreement, (a) Contractor does not grant to Authority any license, express or implied, to Contractor's Intellectual Property Rights and (b) nothing in these terms or the performance thereof, or that might otherwise be implied by law, will operate to grant Authority any right, title, or interest, implied or otherwise, in or to Contractor's intellectual property. Contractor, on behalf of itself and its licensors, expressly reserves all Intellectual Property Rights not expressly granted under the Contracts.

10. RESERVED RIGHTS

The Authority reserves the right to suspend or terminate the Contractor's access and use of the Authority Data and/or the Authority Electronic Property subject to the Contractor being granted equitable relief where to the extent such termination or suspension is not due to a Contractor default. As soon as reasonably practical but within twenty (20) business days of the Authority's written request, the Contractor will return or destroy all written or recorded materials comprising any Confidential Information of the Authority, together with all copies, summaries, compilations or analyses incorporating such information (whether held in computer, electronic or similar format), and certify the same in writing to the Authority; provided that all confidentiality obligations and ownership rights shall survive the return of such materials and the termination of this Agreement indefinitely or for as long as such information qualifies as a trade secret or confidential information under applicable law.

11. SPECIFIC PERFORMANCE

The Contractor recognizes that the restrictions and covenants contained in this Exhibit are reasonable and necessary for the protection of the Authority's legitimate business interests, goodwill and trade secrets and confidential information. The Contractor acknowledges that the breach or threatened breach of this Agreement can cause irreparable damages to the Authority, and that in addition to and not in lieu of all other rights available at law or in equity, the Authority may have the right to temporary and permanent injunctive relief to prevent the breach of this Agreement by the Contractor, without posting of bond and proving actual damages. the Authority will be entitled to recover its reasonable and substantiated costs and expenses, including reasonable attorneys' fees, in enforcing its rights under this Agreement.

EXHIBIT L-Revised-1
MAINTENANCE AND SERVICES AGREEMENT

This Maintenance and Services Agreement (“M&SA”) is made effective upon date of signature

BETWEEN:

Offeror
("Contractor")

- and -

CapMetro
("Client")

In consideration of the mutual covenants set out in this M&SA and for other good and valuable consideration (the receipt and sufficiency of which is hereby acknowledged), the parties agree as follows:

1. **Services.** In accordance with the terms of this M&SA, Contractor shall furnish the Services to Client.
2. **Not Used.**
3. **Definitions.** The following words shall be defined as set forth herein:
 - a. **Back Office** is defined as an Internet accessible site for administration and reporting features available to the Client User. The Back Office is hosted by Contractor on one or more cloud-hosted servers.
 - b. **Client** is defined as Capital Metropolitan Transportation Authority, a political subdivision of the State of Texas.
 - c. **Client User(s)** is defined as any staff member of Client who accesses the Back Office or a Client User App in order to perform his or her job responsibilities.
 - d. **Client User App(s)** are defined as Contractor developed mobile apps for Client Users, for example, a fare inspection app to identify if a ticket is valid. Client User Apps may be referred to by their functional name (e.g., web app).
 - e. **Contractor** is defined as Company Name, a Texas Corporation with its principal place of business at address. This includes any and all subcontractors.
 - f. **Contractor Network Monitoring** is defined as a software solution which monitors network infrastructure and Internet connection for errors, intrusion detection and packet loss.
 - g. **Critical Updates** are defined as updates to the Services or Services' infrastructure which are required to patch known security vulnerabilities or software bugs.
 - h. **End User** is defined as anyone that accesses Contractor provided services through a web browser or mobile app. (e.g., a customer of Client that is accessing Client services through a mobile app or web portal). End Users may be referred to as customers in this M&SA.
 - i. **End User Apps** are defined as Contractor developed mobile apps for End Users to access or use

Client's services such as for buying and using fare media. End User Apps may be branded for the Client's services and be referred to as such.

- j. **External Interface** is defined as a third party's software that communicates to the Services.
 - k. **Help Desk** is defined as a component of Client's customer service center focused on End User support and may include phone, email, and online support directly for End Users for issues and questions with use of Client's services. The Help Desk is typically regarded as Level 1 troubleshooting before being escalated to the Service Desk.
 - l. **Level 1** is defined as an initial response to reported issues, providing basic support and troubleshooting, such as password resets, break/fix instructions, ticket routing and escalation to the Service Desk.
 - m. **Maintenance Services** shall have the meaning ascribed to it in Section 5 of this M&SA.
 - n. **Non-Critical Update** is defined as an Update to the Services or Services' infrastructure which is recommended to patch a software bug which may or may not affect a small number of users or systems.
 - o. **Outage** is defined as the unavailability of the basic functionalities and shall include the unavailability of the website for customer service, management, finance staff, the inability for End Users to establish an account and purchase mobile tickets, the inability of customers to redeem mobile tickets, and inability for End Users to plan a trip from A to B using a scheduled time.
 - p. **Patch Management** is defined as the process of managing recommended critical and non-critical updates while minimizing the effect to the Services.
 - q. **Services** is defined as all hosting services, Support Services and the Maintenance Services.
 - r. **Service Desk** is defined as the Contractor's single primary point of contact for all issues and questions from Client. All issues, including issues related to subcontractor software (e.g. related software name), are automatically logged and tracked by the Service Desk. Unresolved or ongoing issues are automatically escalated within the Service Desk to the appropriate resources and management. The Service Desk is available to Client according to the coverage schedule outlined in this M&SA.
 - s. **Software** is defined as the collective Contractor-provided solution, which includes, but is not limited to, the Back Office, Client User App, and any other Contractor mobile apps for smartphones.
 - t. **Support Services** shall have the meaning ascribed to it in Section 4 of this M&SA.
 - u. **Update(s)** is defined as software modifications to maintain functionality or address bugs.
 - v. **Upgrades** are defined as Software modifications which introduce new features or functionality.
 - w. **User Acceptance Testing** is defined as a phase of software development in which the Software is tested by Client Users prior to release to the production environment.
 - x. **Vulnerabilities** is defined as a weakness in the Software in which an attacker with knowledge and means may exploit.
 - y. **Workaround** is defined as a solution to remedy an issue in order that the Software can perform basic functionality.
4. **Support Services.** Contractor shall furnish all of the following support services in connection with the M&SA (the "Support Services"):

- a. End User Support. End Users shall be directed to Help Desk as a Level 1 customer support. If the issue is found to be a technical issue related to the Software, including but not limited to the Back Office, mobile app, the Client customer service representative should open a ticket by using the Service Desk.
 - b. Client User App Support.
 - 1) Client User support referred to Contractor shall be provided by Contractor via phone, email or web to the extent of troubleshooting the Client User Apps.
 - 2) Tablet operating systems and hardware support will not be provided by Contractor and should be directed to the manufacturer of the mobile device.
 - c. Client User Support.
 - 1) Client User support shall be provided only to the extent it requires troubleshooting functionality related to the Software and the troubleshooting cannot be accomplished by the Client.
 - 2) Client Users shall direct all support requests to the Service Desk. Such requests shall be resolved based on their priority level as defined below.
 - 3) Hardware and operating systems support will not be provided by Contractor and should be directed to Client's internal IT resources.
5. **System Maintenance Services.** Contractor shall furnish all of the following maintenance services in connection with the M&SA (the "**Maintenance Services**"):
- a. General Maintenance. Contractor shall complete all routine maintenance for all hosted systems and infrastructure. The need for and schedule of routine maintenance shall be determined by Contractor in its sole and absolute discretion.
 - b. Updates.
 - 1) Critical Updates shall be performed by Contractor as soon as possible, but not later than twenty-four (24) hours after Contractor is notified by Client of an issue requiring a Critical Update to resolve. Whether a Critical Update is required to resolve a reported issue shall be determined by the Contractor in its sole and absolute discretion.
 - 2) Non-Critical Updates will be performed by Contractor on a pre-determined schedule mutually agreed to by the parties to minimize impact to production environment. The need for Non-Critical updates shall be determined by Contractor in its sole and absolute discretion.
 - 3) Patch Management shall be provided by Contractor, including critical security patch updates for Contractor server operating systems applied and managed, including scheduled server restarts. The need for Patch Management shall be determined by Contractor in its sole and absolute discretion.
 - 4) Contractor Network Monitoring shall be provided by Contractor, including router and firewall and Internet connection monitoring.
6. **Client Responsibilities.**
- a. Authorized Users. The Client shall administer user access to the Contractor's Software. The Client acknowledges and agrees it is solely responsible for maintaining the confidentiality and security of system access credentials, including usernames and passwords.
 - b. Acceptable Usage. The Client shall ensure Contractor's Software is used only in accordance with its intended use and shall ensure Contractor's Software is used in accordance with any terms and

conditions or instructions provided by Contractor related to the use thereof. The Client is responsible for all activity that occurs under their account.

- c. **Point of Contact.** The Client shall designate one primary and one alternate point of contact and communicate the initial contacts to Contractor in writing. The Client will have the ability to modify their primary and alternate contact points through the Service Desk.

7. Service Level Objectives.

Severity Level	Acknowledgement Time	Target Workaround Time*	Target Resolution Time*
1 – Blocker	15 Minutes	6 hours	24 hours
2 – Major	1 Hour	24 Hours	Current planned release
3 – Medium	1 Business Day	30 Business Days	Scheduled as part of next release
4 – Minor	5 Business Days	N/A	Incorporated into future release

Service hours for Blocker and Major severity levels are defined as 24x7x365.

In addition, for Blocker and Major severity level issues, Contractor shall provide Client regular updates every thirty (30) minutes until a Workaround has been implemented.

Medium and Minor severity level issues are handled during normal business hours: 8 a.m. to 5 p.m. Central Time, Monday-Friday, excluding U.S. National Holidays.

*The contents contained in the service level objectives table in columns “Target Workaround Time” and “Target Resolution Time” do not include third-party delays outside the control of Contractor (e.g., iOS & Android App release times are subject to the respective store’s app approval before publishing to the App Store) such as AWS, Apple App Store, Google Play Store, payment processors, etc.

Acknowledgement Time	The time period in which Contractor is required to respond to Client Users of reported issues.
Target Workaround Time	The amount of time in which Contractor will use commercially reasonable efforts to provide a Workaround starting from the time the issue was reported and Contractor was able to successfully reproduce the issue. If a Workaround is not available, Contractor will create a plan with Client input to minimize impact to business operations.
Target Resolution Time	The amount of time in which Contractor will use commercially reasonable efforts to provide a final resolution starting from the time the issue was reported and Contractor was able to successfully reproduce the issue. Availability of functional Workaround may result in the reclassification of the issue’s severity level.

8. Severity Level Definitions.

Severity Level	Issues Impacting System
1 – Blocker *	<ul style="list-style-type: none"> • End Users cannot use or purchase fare media. • Issue preventing validation of active fare media. • Inability for End Users to plan a trip from A to B using a scheduled time • Significant percentage (more than 10%) of End Users are affected (e.g. cannot use or purchase fare media). • The financial impact of the incident is likely to be high (greater than \$10,000) • The damage to the reputation of the business is likely to be high.
2 - Major	<ul style="list-style-type: none"> • End Users cannot create an account or login. • Trip planning tools no longer provide real time information. • Ability to lookup End Users. • Current product configuration issues. • Prevents Client User from recording fare evasion citations. • Prevents Client User from distributing inventory to partner organization. • Moderate percentage (fewer than 5%) of End Users are affected (e.g. cannot use or purchase fare media). • The financial impact of the incident is likely to be high (more than \$1,000 but not greater than \$10,000). • The damage to the reputation of the business is likely to be moderate.
3 - Medium	<ul style="list-style-type: none"> • Ticket activation and purchasing issues affecting

	<ul style="list-style-type: none"> minority percentage of End Users. Financial reporting inaccuracies. Client User unable to issue refunds. Errors - incorrect billing and settlement. Client or End User App settings screen issues. Future schedule inaccuracies or errors Trip planner inaccuracies Prevents Client User from creating and managing notifications. Prevents Client User from creating & listing orders Prevents Client User from modifying End User details. Prevents Client User from managing and creating products. Prevents Client User from managing and creating campaigns. Prevents Client User from Client User App features. Prevents Client User from managing partner organization related features Prevents Client User accessing stock reports. Reporting inaccuracies Existing data export process fails to execute. Device management and monitoring issues. Clients' account user management Impacts third-party access of Contractor systems
4 – Minor	<ul style="list-style-type: none"> Value add functions are not accessible or result in errors. Cosmetic defects. Feature functions but fails on data variation. Multi/intermodal third-party API's or errors. Statistic tool. Backend Error Messages: GTFS upload information tool. Real time cockpit.

***Issue affects greater than 10% of End Users on supported operating systems and software.**

9. **Alterations.** If any End User or Client User alters his or her own equipment beyond the manufacturer's or mobile operator's operating system so as to constitute jailbreaking or any other known or unknown hacking method, such End User or Client User does so at his or her own risk and expense and the Contractor no longer has any warranty obligations for such equipment.

10. Exclusions and Limitations to this M&SA.

a. Exclusions. The following items are specifically excluded from the Software and Services to be provided by Contractor under this M&SA:

1) **Software:** The following are excluded with respect to the Back Office and Software:

- i. Feature requests or change orders are not included as part of this M&SA; however, resulting modifications would be incorporated into this M&SA as necessary;
- ii. Third-party integration support or External Interface updates not specified in this M&SA;
- iii. Report customization; and
- iv. In-person, third-party training.

2) **Third-Party Costs:** The following are excluded under this M&SA:

- i. Any Contractor parts, hardware, and software not covered under a Contractor warranty or a separate agreement;
- ii. Any third-party parts, hardware and software not covered under a separate agreement;
- iii. Software licenses, subscription, or update fees not set forth in a separate agreement;
- iv. Manufacturer and vendor support fees;
- v. Consumable materials, including printer cartridges, paper rolls for receipt printing or removable storage tapes/disks;
- vi. Shipping and handling costs for any hardware and materials not covered under a separate agreement;
- vii. Legal or insurance costs associated with data breaches or unauthorized access that is outside the Contractor network infrastructure or the Software, except as otherwise provided in a separate contract; and
- viii. Travel costs outside the Austin metropolitan area authorized in advance by Client.

b. Limitations.

1) **Patch Limitations:** Software maintenance required to maintain compatibility with future mobile operating systems may require significant changes to the Software known as Upgrades.

- i. Patch Management does not include Upgrades to support new features released as part of a new mobile operating system or hardware.
- ii. Significant changes to the mobile operating system or software development kits may result in incompatibilities with current versions of a Client User App and are not supported under this M&SA.

2) **Software Support Limitations:**

- i. The Back Office is a web-provided service and should not require significant information technology resources on the part of Client. However, access to the Back Office shall be limited to designated Client personnel. Any unauthorized access to the system via Client equipment or locations is not covered under this M&SA.
- ii. Contractor does not provide any service or repair support for Client systems or Client network infrastructure, including, but not limited to the following:
 - a. Service and repair of damage or problems caused by erroneous data, neglect, malicious activity, or misuse (including use of the system for purpose other than which it was designed by End Users, Client, its employees or third-party contractors); and
 - b. Service and repair by vendor/manufacturer made necessary by bugs released by vendors, adverse effects from installing Updates.

11. **Payment Card Industry Data Security Standard ("PCI DSS") Compliance.**

- a. PCI Coverage and Compliance. Contractor is responsible for maintaining PCI DSS compliance for Services provided by Contractor. The Contractor will host the solution, keeping storage and transmission of card data and other sensitive financial data outside of the scope of the Client's PCI DSS compliance responsibility. If necessary, Contractor and Client will establish a PCI DSS compliance responsibility matrix between the two parties.
- b. Vulnerabilities. Per PCI level 1 rules and schedules, Contractor's systems are routinely scanned by an outside firm for Vulnerabilities. All vulnerabilities discovered shall be resolved as mandated by external auditors and notification of any potential data breach shall be communicated immediately and directly with Client per PCI DSS compliance requirements.

12. **Acceptable Use Policy.** The Client shall adhere, during the term of this M&SA, to Contractor's "Services Acceptable Use Policy" in all respects as set forth and attached hereto in Appendix D.

13. **Client Minimum Standards.**

- a. The Client environment must comply with the following minimum standards related to Back Office access:
 - 1) All operating system and Internet browser software shall be within two (2) major releases of the current version, except as expressly specified by Contractor and Client (e.g., if Internet Explorer 11 is the latest release, support will extend back to Internet Explorer 9). A list of current systems that shall be supported under the terms of this M&SA is set forth in Appendix A attached hereto.
 - 2) Client will use best practices to protect their wireless network; at a minimum Client should utilize WPA2 or higher encryption on their wireless network.
 - 3) Active antivirus protection software licenses shall be provided for installation on all servers, desktops, and laptops. Antivirus software may not be turned off by End Users except for software installation purposes.
 - 4) Software shall be genuine, licensed, and vendor-supported. Operating systems and browsers shall be fully updated and patched for all known critical vulnerabilities.
 - 5) All locations for Service and environments shall be in compliance with all applicable local, state, and federal laws.
 - 6) All Client systems shall be administered only by designated Client personnel.
 - 7) All commercially reasonable efforts shall be conducted by Client to reproduce reported errors and to collect information from users including at a minimum: user contact details and description of issue.
 - 8) Client shall assign one employee to be the primary contact person to Contractor in order to make communications between both parties effective. A list of current Client Users and Contractor designated contacts is set forth on Appendix B and Appendix C attached hereto.

IN WITNESS WHEREOF, the parties hereto have duly executed this M&SA as of the Effective Date first written above:

Cubic Transportation Systems, Inc.
("Contractor")

By: _____

Name: _____

Title: _____

Email: _____

**CAPITAL METROPOLITAN
TRANSPORTATION AUTHORITY**

By: _____

Name: Muhammad Abdullah

Title: VP Procurement & Chief Contracting Officer

Email: muhammad.abdullah@capmetro.org

Appendix A – Supported Systems

Below is a list of all current systems that will be supported under the terms of the M&SA.

System or Device Name	Name	Type	Notes
End Users Apps	(System Name)	iOS and Android and Windows Apps	-Maintain feature set of app(s) for the last two versions of iOS and Android OS and Windows OS. -Maintain feature set of Back Office for the last two versions of Safari, Firefox, and Chrome browsers.
Client User App	(System Name)	Android App Android Mobile Handheld	-Patch and update Client User App to maintain feature set.
Back Office	(System Name)	Web Portal	-Maintain feature set of Back Office for the last two versions of Safari, Firefox, and Chrome browsers.

Appendix B – (Company Name) Designated Contacts & Roles

Name	Email	Phone	Role
Service Desk	support@umoadminportal.zendesk.com		IT Service Desk & After Hours Support
Escalation Hotline			Program Manager
(Level 3 Contact)			Head of Programs
(Level 4 Contact)			Head of Customer Success
(Level 5 Contact)			Senior VP & General Manager
(Level 6 Contact)			Chief Growth Officer
(Level 7 Contact)			

Contact & Escalation Process

The following contact and escalation process shall be followed when contacting Contractor for any maintenance or support issues:

Who to Contact		When to Contact
Level 1 Contact	JIRA Service Desk	24 x 7 x 365
Level 2 Contact	Service Desk Phone	24 x 7 x 365
Level 3 Contact	Escalation Hotline	24 x 7 x 365
Level 4 Contact	(Name)	24 x 7 x 365
Level 5 Contact	(Name)	24 x 7 x 365
Level 6 Contact	(Name)	24 x 7 x 365

Appendix C – Client User Access & Roles

Below is a list of all Client Users that will be supported under the terms of the M&SA:

Name	Email	Phone	Client Role
CapMetro IT Service Desk	https://capmetro.servicenow.com	512-369-7570	IT Service Desk & After Hours Support
			Application Administrator III
			Application Administrator III
			Manager, Technical Product Management
			Director, Service Delivery & Operations
			SVP, CIO

Contact & Escalation Process

The following shall be followed when contacting Client for any maintenance or support issues.

Who to Contact		When to contact
Level 1 Contact	IT Service Desk	24 x 7 x 365
Level 2 Contact		24 x 7 x 365
Level 3 Contact		24 x 7 x 365
Level 4 Contact		24 x 7 x 365
Level 5 Contact		24 x 7 x 365

Appendix D – Services Acceptable Use Policy

Services Acceptable Use Policy

(Company Name), Inc. (hereafter in this Appendix D, “(Company Name)”) has prepared this Acceptable Use Policy (“AUP”) as a guide for its clients to understand the intended and permissible uses of our service. This AUP sets forth guidelines for acceptable use of the applicable (Company Name) service(s) (the “Service(s)”), by Client and its users.

Prohibited Uses

You may use the Service only for lawful purposes and in accordance with this AUP. You may not:

- Use the Service in any way that violates any applicable federal, state, local or international law or regulation (including, without limitation, any laws regarding the export of data or software to and from the US or other countries).
- Use the Service for the purpose of exploiting, harming or attempting to exploit or harm minors in any way by exposing them to inappropriate content, asking for personally identifiable information, or otherwise.
- Use the Service to transmit, or procure the sending of, any advertising or promotional material, including any “junk mail”, “chain letter”, “spam” or any other similar solicitation.
- Impersonate or attempt to impersonate (Company Name), a (Company Name) employee, another user or any other person or entity, including by utilizing another user’s identification, password, account name or persona without authorization from that user.
- Use the Service in any manner that could disrupt, disable, overburden, damage, or impair the Service for you or others (including the ability to send timely notifications through the Service), via various means including overloading, “flooding,” “mail bombing,” “denial of service” attacks, or “crashing”.
- Use any robot, spider or other automatic device, process or means to access the Service for any purpose, including monitoring or copying any of the material.
- Use any manual process to monitor or copy any of the material made available through the Service or for any other unauthorized purpose without our prior written consent.
- Use any device, software or routine, including but not limited to, any malware, viruses, trojan horses, worms, or logic bombs, that interfere with the proper working of the Service or could be technologically harmful.
- Attempt to gain unauthorized access to, interfere with, damage or disrupt any parts of the Service, the server(s) on which the Service is stored, or any server, computer or database connected to the Service.
- Attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without (Company Name)’s express written consent.
- Take any action in order to obtain services to which such client is not entitled.
- Attempt any action designed to circumvent or alter any method of measuring or billing for utilization of the Service.
- Otherwise attempt to interfere with the proper working of the Service.

(Company Name) Rights and Remedies

If Client becomes aware of any content or activity that violates this AUP, Client shall take all necessary actions to prevent such content from being routed to, passed through, or stored on the (Company Name) network, and shall immediately notify (Company Name). Should Client violate the provisions of this AUP, (Company Name) may take reasonable actions to remedy the violation, including but not limited to the issue a warning, suspension or termination of Service, and any rights and remedies as provided by applicable state and federal law. (Company Name) will provide notice to Customer prior to any suspension or termination of Service but may in its discretion immediately suspend or terminate Client's use of the Service only where continued provision of Service may cause significant harm to (Company Name), the Service or other clients.

Notices

Notices to (Company Name) shall be effective only when made in writing to support@xyz.co. Notices to Client shall be made in writing to the email address Client as noted on the signature page of the M&SA.