CONTRACT NO. 500306
(RFQ 811274)

RIGHT OF WAY INVENTORY & ASSET MANAGEMENT SOFTWARE
(SOURCEWELL CONTRACT NO. 060624-TTI)

CONTRACTOR:

Tyler Technologies
5101 Tennyson Pkwy
Plano, TX 75024
Rep: Craig Dixon
Phone: (760)960-6354
Email: craig.dixon@tylertech.com

AWARD DATE:	**February 3, 2026**
CONTRACT TERM:	**One (1) Year from Notice to Proceed** **(February 12, 2026, through February 11, 2027)**
PRICE:	**NOT TO EXCEED: $373,636.00**

PROJECT MANAGER:	**Christopher Rompel**
Telephone #	**(512) 856-1533**
Email Address	christopher.rompel@capmetro.org
BUYER:	**Danny Solano**
Telephone #	**(512) 389-7446**
Email Address	danny.solano@capmetro.org

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

CONTRACT NO. 500306
(RFQ 811274)

RIGHT OF WAY INVENTORY & ASSET MANAGEMENT SOFTWARE
(OMNIA PARTNERS CONTRACT # 060624-TTI)

TABLE OF CONTENTS

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY
AUSTIN, TEXAS

AWARD/CONTRACT

1. SOLICITATION NO:	2. CONTRACT NO.:	3. EFFECTIVE DATE:
811274	500306	Upon Issuance of Notice to Proceed

4. BUYER

NAME:	Danny Solano	PHONE:	(512) 389-7446

5. SHIP TO ADDRESS:	6. DELIVERY TERMS:
Capital Metro 2910 East 5th Street Austin, Texas 78702	FOB Destination **7. DISCOUNTS FOR PROMPT PAYMENT:** None

8. CONTRACTOR NAME & ADDRESS:	9. REMITTANCE ADDRESS: (If different from Item 8)
Tyler Technologies 5101 Tennyson Pkwy Plano, TX 75024	
PHONE: (972) 713-3700	
FAX:	

10. DBE GOAL: N/A

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.

X	NEGOTIATED AGREEMENT:	(Contractor is required to sign below and return an original document to the Contracting Officer within five (5) calendar days of receipt.)

Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified below and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this Award/Contract, (b) the solicitation, as amended, and (c), such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein.

SIGNATURE OF CONTRACTOR:

Name/Title: Erik Graney-Senior Corporate Attorney Signature: Erik Graney Date: 02 / 03 / 2026

X	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 shall have the same force and effect as an original document.

ALTERATIONS IN CONTRACT:

1. Refer to Exhibit E - Contractual Terms and Conditions; Exhibit is being replaced with Exhibit E-Revised-1 - Contractual Terms and Conditions, attached hereto and made a part hereof for all pertinent purposes.
2. Refer to Exhibit IT- Additional Terms and Conditions for Hosted Solutions; Exhibit is being replaced with Exhibit IT-Revised-1 - Additional Terms and Conditions for Hosted Solutions, attached hereto and made a part hereof for all pertinent purposes.
3. Refer to Exhibit IT- Proprietary Rights and Data Security Addendum; Exhibit is being replaced with Exhibit IT-Revised-1- Proprietary Rights and Data Security Addendum, attached hereto and made a part hereof for all pertinent purposes.
4. Refer to Exhibit IT- Access and Use Agreement; Exhibit is being replaced with Exhibit IT-Revised-1 - Access and Use Agreement, attached hereto and made a part hereof for all pertinent purposes.

ACCEPTED AS TO: Exhibit A, Pricing Schedule, Dated, 1/8/2026, Section 7, Pricing: Base Year, Item 3, for a Grand Total Not to Exceed Amount of $373,636.

SIGNATURE OF CONTRACTING OFFICER:

Typed Name: Danny Solano Contracting Officer	Signature: E-SIGNED by Danny Solano on 2026-02-11 18:58:52 GMT Date: February 11, 2026

EXHIBIT A
PRICING SCHEDULE
RFP 811274

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)	Tyler Technologies		
Address	5101 Tennyson Pkwy		
City, State, Zip	Plano, TX 75024		
Phone, Fax, Email	(972) 713-3700		
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)	Erik Graney-Senior Corporate Attorney		
Signature and Date	Erik Graney		01/09/2026

2 ACKNOWLEDGEMENT OF AMENDMENTS

The offeror must acknowledge amendment(s) to this solicitation in accordance with the ACKNOWLEDGMENT OF AMENDMENTS section of Exhibit C.

3. PROMPT PAYMENT DISCOUNT

# of Days	N/A	Percentage	N/A

4. SBE GOAL (TO BE COMPLETED UPON AWARD BY CAPITAL METRO)

The SBE participation commitment for this contract is the following percentage of the total contract:

N/A

5. 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:	

6. DOCUMENTS ENCLOSED WITH THE PROPOSAL

Mark X each box below, to indicate that the submittals have been included in the offer. See Exhibit C, Solicitation Instructions and Conditions, Section 4, PREPARATION OF PROPOSALS for a description of the required proposal format.

- ☑ **Exhibit A – Pricing Schedule**
- ☒ **Exhibit B – Representations and Certifications**
- ☒ **Exhibit IT – Consultant Access-Disclosure Agreement**

Note: Failure to submit the required submittals along with the offer may result in rejection of the offer.

Remainder of page left blank intentionally

Signature of Authorized Agent: _____ **Date:** 01/09/2026

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/

EXHIBIT B

REPRESENTATIONS AND CERTIFICATIONS

(LOCALLY FUNDED SUPPLY/SERVICE/CONSTRUCTION CONTRACTS)

M U S T B E R E T U R N E D W I T H T H E O F F E R

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:

Delaware

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:

[redacted]

(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:

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 _Tyler Technologies, Inc._ [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. CERTIFICATION OF PROPOSED PRICING

The offeror certifies that the pricing offered in Exhibit A - Pricing Schedule, as amended, is exclusive of any sales tax.

5. 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.

(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.

6. 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.)

7. 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.

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

8. 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.

(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.

(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)]

(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.

(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:

(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, 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 2276 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 2276.002 of the Texas Government Code, or

(b) the verification required by Section 2276.002 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.

15. CRITICAL INFRASTRUCTURE PROHIBITION

Pursuant to Chapter 2275 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 2275 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 (C.F.R.) 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

☐ will
☒ will not

provide covered telecommunications equipment or services to the Authority in the performance of any contract, subcontract 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);

(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.

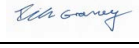
Name of Offeror:

Tyler Technologies, Inc.

Type/Print Name of Signatory:

Erik Graney

Signature:



Date:

January 9, 2026

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

WHEREAS, THE AUTHORITY IS A MEMBER OF SOURCEWELL ("SOURCEWELL") UNDER MEMBER NUMBER 46462

WHEREAS, TYLER PARTICIPATED IN THE COMPETITIVE BID PROCESS IN RESPONSE TO SOURCEWELL RFP #060624 BY SUBMITTING A PROPOSAL, ON WHICH SOURCEWELL AWARDED TYLER A SOURCEWELL CONTRACT, NUMBERED 060624-TTI (HEREINAFTER, THE "SOURCEWELL CONTRACT");

WHEREAS, DOCUMENTATION OF THE SOURCEWELL COMPETITIVE BID PROCESS, AS WELL AS TYLER'S CONTRACT WITH AND PRICING INFORMATION FOR SOURCEWELL IS AVAILABLE AT HTTPS://WWW.SOURCEWELL-MN.GOV/COOPERATIVE-PURCHASING/060624-TTI; AND

WHEREAS, CLIENT DESIRES TO PURCHASE OFF THE SOURCEWELL CONTRACT TO PROCURE CERTAIN SOFTWARE FUNCTIONALITY INDICATED IN THE INVESTMENT SUMMARY FROM TYLER, WHICH TYLER AGREES TO DELIVER PURSUANT TO THE SOURCEWELL CONTRACT AND UNDER THE TERMS AND CONDITIONS SET FORTH BELOW.

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" means all data, content and information submitted by or on behalf of the Authority or its customers to the Contractor or loaded into the System that is necessary for the use of the Application.

(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, wars within the continental United States, riots or insurrections; embargos, natural disasters, including but not limited to landslides, earthquakes, floods 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) “FTA” means the Federal Transit Administration.

(r) “Fully Burdened Hourly Labor Rate” means an hourly rate that includes all salary, overhead costs, general and administrative expenses, and profit.

(s) “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.

(t) “Notice of Award” means formal notice of award of the Contract to the Contractor issued by the Contracting Officer.

(u) “Notice to Proceed” means written authorization for the Contractor to start the Services.

(v) “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.

(w) “Proposal” means the offer of the proposer, submitted on the prescribed form, stating prices for performing the work described in the Scope of Services.

(x) “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, but not SaaS Services.

(y) “Subcontract” means the Contract between the Contractor and its Subcontractors.

(z) "Subcontractor" means subcontractors of any tier.

(aa) RESERVED.
(bb) "Business Travel Policy means Contractor's business travel policy, available at https://www.tyler-tech.com/portals/0/terms/Tyler-Business-Travel-Policy.pdf
(cc) "Data Storage Capacity" means the contracted storage capacity for Authority Data, if any, identified in the Investment Summary.
(dd) "Defect" means a failure of the Tyler Software to substantially conform to the functional descriptions set forth in Contractor's written proposal, or the Documentation in the absence of a written proposal, or their functional equivalent. Future functionality may be updated, modified, or otherwise enhanced through our maintenance and support services, and the governing functional descriptions for such future functionality will be set forth in the then-current Documentation.
(ee) "Documentation" means any online or written documentation related to the use or functionality of the Tyler Software that Contractor provides or otherwise makes available to the Authority, including instructions, user guides, manuals and other training or self-help documentation.
(ff) "Investment Summary" means the cost proposal for the products and services included in Exhibit E.1.
(gg) "SaaS Fees" means the fees for the SaaS Services identified in the Investment Summary.
(hh) "SaaS Services" means software as a service consisting of system administration, system management, and system monitoring activities that Contractor performs for the Tyler Software and includes the right to access and use the Tyler Software, receive maintenance and support on the Tyler Software, including downtime resolution under the terms of the SLA, and Data storage and archiving. SaaS Services do not include support of an operating system or hardware, support outside of our normal business hours, or training, consulting, or other Professional Services.
(ii) "SLA" means the Service Level Agreement, attached hereto as Exhibit E.4.
(jj) "Statement of Work" means the industry standard implementation plan describing how Contractor's Professional Services will be provided to implement the Tyler Software and outlining both parties' roles and responsibilities in connection with that implementation. The Statement of Work is attached as Exhibit E.6.
(kk) "Support Call Process" means the support call process applicable to the Authority. The current Support Call Process is available here: https://www.tylertech.com/portals/0/terms/Tyler-Support-Call-Process.pdf.
(ll) "Third-Party Hardware" means the third-party hardware, if any, identified in the Investment Summary.
(mm) "Third-Party Products" means the Third-Party Software and Third-Party Hardware.
(nn) "Third-Party SaaS Services" means software as a service provided by a third party, if any, identified in the Investment Summary.
(oo) "Third-Party Services" means the third-party services, if any, identified in the Investment Summary.
(pp) "Third-Party Software" means the third-party software, if any, identified in the Investment Summary or included with the Tyler Software.
(qq) "Third-Party Terms" means the end user license agreement(s) or other terms, if any, for the Third-Party Products or other parties' products or services, as applicable, and attached or indicated at Exhibit E.5.
(rr) "Tyler Software" means the Contractor's proprietary software, including any integrations, custom modifications, and/or other related interfaces identified in the Investment Summary and licensed to the Authority through this Contract.

2. FIXED PRICE CONTRACT

This is a fixed price Contract for the Services specified and stated elsewhere in the Contract.

3. TERM

The term of the Contract shall be 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 (4) option periods for a twelve (12) month duration each at the option prices set forth in Exhibit A - Pricing Schedule upon written notice to the Contractor.

5. ADDITIONAL OPTION TO EXTEND CONTRACT PERFORMANCE

In connection with the termination of this Agreement for any reason, and only upon the execution of a mutually agreed change order or addendum, Tyler shall use commercially reasonable efforts to accomplish an adequate and timely transition from Tyler to the Client, or to any replacement providers designated by the Client (a "Disentanglement"). The parties shall reasonably cooperate during Disentanglement. Client shall reimburse Tyler for Disentanglement services provided by Tyler at Tyler's then-current rates, plus reasonable costs, and expenses, as set forth in the parties' executed change order or addendum.

6. INVOICING AND PAYMENT

(a) Invoicing and Payment shall be as set forth in Exhibit E.3 Invoicing and Payment Terms. Invoices shall be submitted for work completed and accepted by the Authority, and marked "Original" to:

Accounts Payable
Capital Metropolitan Transportation Authority
2910 E. 5th Street
Austin, Texas 78702

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

and shall conform to policies or regulations adopted from time to time by the Authority, provided to Contractor as of the effective date of this Contract, and thereafter as mutually agreed between the Parties. In addition, Invoices shall be legible and shall contain, as a minimum, the following information:

(1) the Contract and order number (if any);

(2) a complete itemization of all costs including quantities ordered and delivery order numbers (if any);

(3) any discounts offered to the Authority under the terms of the Contract;

(4) evidence of the acceptance of the Services by the Authority; and

(5) any other information necessary to demonstrate entitlement to payment under the terms of the Contract.

(b) 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) and Parties agree to follow the Texas Prompt Payment Act for nonpayment remedies.

(c) Contractor should submit an invoice to the Authority in accordance with Exhibit E.3. Each invoice must reference the applicable acceptance documentation and clearly identify the dates and scope of work performed. Failure to submit timely invoices may result in a delay of payment.

(d) 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), and all other Contractor's costs of doing business.

(e) 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 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.

(f) **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.

(g) The Authority must provide written notice within thirty (30) days of receipt of an invoice for an invoice or performance related dispute under this Agreement. All disputes are subject to Exhibit E Section 43. For invoice related disputes, the notice of dispute must include (i) the issue(s) with the invoice; (ii) the specific fee(s) at issue; and (iii) the corrective action(s) requested. Contractor will then provide a response to the notice that (i) supports the validity of the invoice as issued; (ii) adjusts the invoice; or (iii) describes Contractor's plan to address the issues identified in the dispute notice.

7. RESERVED

8. RESERVED

9. INSURANCE

(a) The Contractor shall furnish proof of CapMetro-stipulated insurance requirements specified below. Contractor's insurance is primary for claims under Contractor's Commercial General Liability or Auto policies that arise out of and relate to the contract and between Contractor and the Authority. Contractor will agree to waive subrogation for claims under the Commercial General Liability or Auto policies that arise out of or relate to the Agreement and are between Contractor and the Authority, except to the extent the damage or injury is caused by the Authority. The Contractor shall furnish to the Authority certificate(s) of insurance evidencing the required coverage and endorsement(s). Prior to the expiration of a certificate of insurance, a new certificate of insurance shall be furnished to the Authority showing continued coverage within thirty (30) days written notice of cancellation or non-renewal to the Authority. The Authority shall be added as an Additional Insured under Contractor's Commercial General Liability and Auto. All insurance policies shall be written by reputable insurance company or companies 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 in excess of the insurance required by the Authority.

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 Commercial General Liability Insurance** Coverage with limits of not less than One Million Dollars and No/100 Dollars ($1,000,000) per claim, with an aggregate of Two Million Dollars and No/100 Dollars ($2,000,000) with coverage that includes:

(i) Products and Completed Operations Liability

(ii) Independent Contractors

(iii) Personal Injury Liability extended to claims arising from employees of the Contractor and the Authority.

(iv) Contractual Liability pertaining to the liabilities assumed in the agreement.

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

(3) **Workers' Compensation Insurance** Statutory Workers' Compensation coverage in the State of Texas.

(4) **Employers Liability Insurance** with minimum limits of liability of One Million Dollars and No/100 Dollars ($1,000,000), per each accident.

(5) **Technology Errors & Omissions Insurance (this may be included in Contractor's Professional Liability Insurance)**: Combined Technology & Omissions Policy per claim, with a minimum One Million and No/100 Dollars ($1,000,000) per claim and in the aggregate limit, including:

(i) **Professional Liability Insurance** of One Million and No/100 Dollars ($1,000,000) per claim and in the aggregate, covering negligent acts, errors and omissions arising from the Contractor's work to pay damages for which the Contractor may become legally obligated (such coverage to be maintained for at least two (2) years after termination of this Contract, which obligation shall expressly survive termination of this Contract; and

(ii) **Network Privacy, Security and Media Liability Insurance** providing liability for unauthorized access or disclosure, security breaches or system attacks, as well as infringement of copyright and trademark that might result from this contract.

Cyber Terrorism Coverage should be covered under Contractor's Professional Liability/Cyber Coverage policy.

(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) 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.

(d) 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.
If any part of the Contract is sublet, the Contractor shall require that any subcontractor maintain insurance consistent with this Section 9.

(e) 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.

10. REMOVAL OF ASSIGNED PERSONNEL

The Authority 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.

11. REPRESENTATIONS AND WARRANTIES

Contractor warrants that the Tyler Software will perform without Defects during the term of this Contract. If the Tyler Software does not perform as warranted, Contractor will use all reasonable efforts, consistent with industry standards, to cure the Defect in accordance with Contractor's then-current Support Call Process.
If any breach of the representations and warranties is discovered by the Authority during the Contract Term 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. Contractor will perform Professional Services in a professional, workmanlike manner, consistent with industry standards. In the event that Professional Services are provided in a manner that do not conform to this warranty, Contractor will re-perform such services at no additional cost.

EXCEPT FOR THE EXPRESS WARRANTIES PROVIDED IN THIS AGREEMENT AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES, DUTIES, OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

12. 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.

13. RESERVED

14. PERSONNEL ASSIGNMENTS

(a) The Contractor shall perform the Services in an orderly and professional manner and shall employ persons skilled and qualified for the performance of the Services assigned to such persons under the Contract. CapMetro will have the right to review the experience of each candidate. The Contractor certifies that the Contractor has established a criminal history background policy that complies with guidance issued by the U.S. Equal Employment Opportunity Commission and that the Contractor 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 work being performed, considering the risk and liability to the Contractor and CapMetro.

15. 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.

16. CHANGES

(a) This Contract may be modified in writing, signed by an authorized representative of both parties. Purchase orders or change orders submitted by either party, if any, are for internal administrative purposes only, and the terms and conditions contained in those purchase orders will have no force or effect.
(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.

17. TERMINATION FOR DEFAULT

(a) The Authority may 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;

(2) if the Contractor fails to perform any of the other provisions of this Contract and does not cure such failure within a period of ten (10) days (or such longer period as the Authority may authorize in writing) after receipt of notice from the Authority specifying such failure.

(3) Force Majeure. Either party has the right to terminate this Contract if a Force Majeure Event suspends performance of the SaaS Services for a period of forty-five (45) days or more.

(4) Lack of Appropriations. If Authority should not appropriate or otherwise make available funds sufficient to utilize the SaaS Services, it may unilaterally terminate this Contract upon thirty (30) days written notice. Authority will not be entitled to a refund or offset of previously paid, but unused, SaaS Fees. Termination for lack of appropriations may not be used as a substitute for termination for convenience.

(e) In the event of termination, the Authority will pay for all undisputed fees and expenses related to the software, products, and/or services received, or that Contractor has incurred or delivered, prior to the effective date of termination. Disputed fees and expenses in all termination other than fees disputed for termination for cause must have been submitted as invoice disputed in accordance with the invoice dispute process at Section 43.
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.

(f) 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.

18. 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 sixty (60) 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.

(c) The total sum to be paid the Contractor under this Section shall not exceed the total Contract Sum plus the reasonable settlement costs of the Contractor reduced by the amount of payments otherwise made and the contract price of orders not terminated.

19. 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.

20. DATA PRIVACY PROVISIONS

(a) The Contractor and its subcontractors and their respective employees and personnel may have access to the Authority Data (including without limitation, personally identifiable information ("PII")) in connection with the performance of the Contract. PII shall be any information that identifies or describes a person or can be directly linked to a specific individual, including ridership and usage data. Examples of PII include, but are not limited to, name, address, phone or fax number, signature, date of birth, e-mail address, method of payment, ridership and travel pattern data. Customer Personally Identifiable Information, or Customer PII, means any PII relating to the Authority's customers. To the extent any Authority Data (including PII) is made available to the Contractor under the Contract, the Contractor shall take reasonable steps to maintain the confidentiality, security, safety, and integrity of all PII and other Authority Data in accordance with the Authority's Proprietary Rights and Data Security Addendum, which will be attached as an addendum to the Contract, as applicable.

(b) The Contractor and its subcontractors, employees and consultants may require access to the Authority Electronic Property and related Authority Data in connection with the performance of services under the Contract. In such event, the Contractor agrees that it will, and it will cause its subcontractors and any of their respective employees and personnel to, execute the Authority's Access and Use Agreement, which will be attached as an addendum to the Contract, as applicable.

(c) This Section will survive termination or expiration of this Agreement for any reason.

21. 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.

22. 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 as set forth in Exhibit E.6, Statement of Work.

(b) If any of the Services do not conform with Contract requirements, 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 (1) require the Contractor to take necessary action to ensure that future performance conforms to Contract requirements and (2) reduce the Contract Sum to reflect the reduced value of the Services performed.

23. RESERVED

24. 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 § 37.10.

25. 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.

26. 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.

27. 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.

28. 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 Authority 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.

29. REQUEST FOR INFORMATION

(a) Both parties recognize that their respective employees and agents, in the course of performance of this Agreement, may be exposed to confidential information and that disclosure of such information could violate rights to private individuals and entities, including the parties. Confidential information is nonpublic information that a reasonable person would believe to be confidential and includes, without limitation, personal identifying information (e.g., social security numbers) and trade secrets, each as defined by applicable state law. Each party agrees that it will not disclose any confidential information of the other party and further agrees to take all reasonable and appropriate action to prevent such disclosure by its employees or agents. The confidentiality covenants contained herein will survive the termination or cancellation of this Agreement. This obligation of confidentiality will not apply to information that:

i) Is in the public domain, either at the time of disclosure or afterwards, except by breach of this Contract by a party or its employees or agents;
ii) A party can establish by reasonable proof was in that party's possession at the time of initial disclosure;
iii) A party receives from a third party who has a right to disclose it to the receiving party; or
iv) Is the subject of a legitimate disclosure request under the Texas Public Information Act; provided, however, that in the event such a request is received, the Authority will provide prompt notice to Contractor and otherwise perform the functions required by applicable law.

30. RIGHTS TO PROPOSAL AND CONTRACTUAL MATERIAL

(a) All 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.

31. LIMITATION OF LIABILITY

NOTWITHSTANDING ANYTHING TO THE CONTRARY SET FORTH IN THIS AGREEMENT, CONTRACTOR'S LIABILITY FOR DAMAGES ARISING OUT OF THIS AGREEMENT, WHETHER BASED ON A THEORY OF CONTRACT OR TORT, INCLUDING NEGLIGENCE AND STRICT LIABILITY, SHALL BE LIMITED TO THE AUTHORITY'S ACTUAL DIRECT DAMAGES, NOT TO EXCEED (i) DURING THE INITIAL TERM, TOTAL FEES PAID AS OF THE TIME OF THE CLAIM; OR (ii) DURING ANY RENEWAL TERM, THE THEN-CURRENT ANNUAL SAAS FEES PAYABLE IN THAT RENEWAL TERM. THE PARTIES ACKNOWLEDGE AND AGREE THAT THE PRICES SET FORTH IN THIS AGREEMENT ARE SET IN RELIANCE UPON THIS LIMITATION OF LIABILITY AND TO THE MAXIMUM EXTENT ALLOWED UNDER APPLICABLE LAW, THE EXCLUSION OF CERTAIN DAMAGES, AND EACH SHALL APPLY REGARDLESS OF THE FAILURE OF AN ESSENTIAL PURPOSE OF ANY REMEDY. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO CLAIMS THAT ARE SUBJECT TO CONTRACTOR'S INDEMNIFICATION OBLIGATIONS IN THIS CONTRACT.TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT WHATSOEVER, EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

32. 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.

33. CLAIMS

In the event that any publicly filed 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 ten (10) working days after being notified of such claim, demand, suit, or action. 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.

34. 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.

35. 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.

36. PUBLICITY RELEASES

Except for identifying the Authority in Contractor's client lists, 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.

37. 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.

38. INDEMNIFICATION

(a) **INTELLECTUAL PROPERTY INFRINGEMENT INDEMNIFICATION.**

(b) **CONTRACTOR WILL DEFEND THE AUTHORITY AGAINST ANY THIRD-PARTY CLAIM(S) THAT THE TYLER SOFTWARE OR DOCUMENTATION INFRINGES THAT THIRD-PARTY'S PATENT, COPYRIGHT, OR TRADEMARK, OR MISAPPROPRIATES ITS TRADE SECRETS, AND WILL PAY THE AMOUNT OF ANY RESULTING ADVERSE FINAL JUDGMENT (OR SETTLEMENT TO WHICH CONTRACTOR CONSENTS). THE AUTHORITY MUST NOTIFY CONTRACTOR PROMPTLY IN WRITING OF THE CLAIM AND GIVE CONTRACTOR SOLE CONTROL OVER ITS DEFENSE OR SETTLEMENT. THE AUTHORITY AGREES TO PROVIDE CONTRACTOR WITH REASONABLE ASSISTANCE, COOPERATION, AND INFORMATION IN DEFENDING THE CLAIM AT CONTRACTOR'S EXPENSE.**

(c) **CONTRACTOR'S OBLIGATIONS UNDER THIS SECTION 43(a) WILL NOT APPLY TO THE EXTENT THE CLAIM OR ADVERSE FINAL JUDGMENT IS BASED ON THE AUTHORITY'S USE OF THE TYLER SOFTWARE IN CONTRADICTION OF THIS CONTRACT, INCLUDING WITH NON-LICENSED THIRD PARTIES.**

(d) **IF AN INFRINGEMENT OR MISAPPROPRIATION CLAIM IS FULLY LITIGATED AND THE AUTHORITY'S USE OF THE TYLER SOFTWARE IS ENJOINED BY A COURT OF COMPETENT JURISDICITON, IN ADDITION TO PAYING ANY ADVERSE FINAL JUDGMENT (OR SETTLEMENT TO WHICH CONTRACTOR CONSENTS),**

CONTRACTOR WILL, AT ITS OPTION, EITHER: (I) PROCURE THE RIGHT TO ITS CONTINUED USE; (II) MODIFY IT TO MAKE IT NON-INFRINGING; OR (III) REPLACE IT WITH A FUNCTIONAL EQUIVALENT. CONTRACTOR MAY ELECT TO EMPLOY THESE REMEDIES IN ADVANCE OF LITIGATION IF CONTRACTOR RECEIVES INFORMATION CONCERNING AN INFRINGEMENT OR MISAPPROPRIATION CLAIM.

(e) **THIS SECTION PROVIDES THE AUTHORITY'S EXCLUSIVE REMEDY FOR THIRD-PARTY COPYRIGHT, PATENT, OR TRADEMARK INFRINGEMENT AND TRADE SECRET MISAPPROPRIATION CLAIMS.**

(f) **CONTRACTOR WILL INDEMNIFY AND HOLD HARMLESS THE AUTHORITYY AND THE AUTHORITY'S AGENTS, OFFICIALS, AND EMPLOYEES FROM AND AGAINST ANY AND ALL THIRD-PARTY CLAIMS, LOSSES, LIABILITIES, DAMAGES, COSTS, AND EXPENSES (INCLUDING REASONABLE ATTORNEY'S FEES AND COSTS) FOR (i) PERSONAL INJURY, DEATH, OR DAMAGE TO TANGIBLE PROPERTY, ALL TO THE EXTENT CAUSE BY CONTRACTOR'S NEGLIGENCE OR WILLFUL MISCONDUCT; OR (ii) CONTRACTOR'S VIOLATION OF LAW APPLICABLE TO ITS PERFORMANCE UNDER THIS AGREEMENT. THE AUTHORITY MUST NOTIFY CONTRACTOR PROMPLTY IN WRITING OF THE CLAIM AND GIVE CONTRACTOR SOLE CONTROL OVER ITS DEFENSE OR SETTLEMENT. THE AUTHORITY AGREES TO PROVIDE CONTRACTOR WITH REASONABLE ASSISTANCE, COOPERATION, AND INFORMATION IN DEFENDING THE CLAIM AT CONTRACTOR'S EXPENSE.**

(g) **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 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 THAT WOULD ENJOIN THE INDEMNIFIED PARTY OR REQUIRE THE INDEMNIFIED PARTY TO PAY ANY AMOUNT, 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 APPROPRIATE. 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.**

(h) **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) 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.**

(i) **THIS SECTION WILL SURVIVE ANY TERMINATION OR EXPIRATION OF THIS CONTRACT.**

39. RECORD RETENTION; ACCESS TO RECORDS AND REPORTS

(a) Contractor shall maintain accurate and complete books and records relating directly to this Agreement for the greater of (a) five (5) years from creation, or (b) such period as is required by applicable law, or (c) 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.
(b) The Authority may audit Contractor's books and records relating directly to the contract once per year or as otherwise agreed to on one-week advance written notice, and at Authority's expense. Unless otherwise agreed, the

location of the records will be the Contractor's office servicing the contract. The audit will not include access to Contractor's personnel records, or conditions of employment.

(c) 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.

(d) The Contractor shall maintain all books, records, accounts and reports required under this paragraph for a period of at not less than five (5) 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.

(e) 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.

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

40. EXCUSABLE DELAYS

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. In each instance, the failure to perform must be beyond the control and without the fault or negligence of the Contractor.

41. 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, to the extent 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.

42. 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 warranty provisions of this Contract.

43. INTERPRETATION OF CONTRACT – DISPUTES

The parties agree to cooperate in trying to reasonably resolve all disputes, including, if requested by either party, appointing a senior representative to meet and engage in good faith negotiations with the other party's appointed senior representative. Senior representatives will convene within thirty (30) days of the written dispute notice, unless otherwise agreed. All meetings and discussions between senior representatives will be deemed confidential settlement discussions not subject to disclosure under applicable laws. If the dispute remains unresolved, then either party may assert its respective rights and remedies in a state or federal court of competent jurisdiction. Nothing in this section shall prevent either party from seeking necessary injunctive relief during the dispute resolution process. Nothing in this section shall waive any applicable governmental immunities under applicable law.

44. 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.

45. 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. Award/ Contract Form
2. Exhibit A - Pricing Schedule
3. Exhibit E-Revised-1 - Contractual Terms and Conditions
4. Exhibit IT-Revised-1 – Additional Terms and Conditions for Hosted Solutions
5. Exhibit IT-Revised-1 – Proprietary Rights and Data Security Addendum
6. Exhibit IT-Revised-1 – Access and Use Agreement
7. Exhibit H – Authorization of Work Product
8. Exhibit B - Representations and Certifications
9. Exhibit F - Scope of Services and Compliance Matrix
10. Other provisions or attachments to the Contract

46. 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.

47. 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 may arise.

(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.

48. 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) 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.

(d) 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.

(e) 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.

(f) 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.

(g) 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.

(h) 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. 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.

(i) The failure of either party 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.

(j) 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.

(k) 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.

49. 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 E.1
INVESTMENT SUMMARY

INCORPORATED BY REFERENCE AS ATTACHED TO THE CONTRACT

remainder of page intentionally left blank

EXHIBIT E.2
TYLER SAAS TERMS

SECTION A – DEFINITIONS

- "we," "us," "our" and similar terms mean Tyler.
- "you" and similar terms mean Client.

SECTION B – SAAS SERVICES

1. Rights Granted. We grant to you the non-exclusive, non-assignable limited right to use the SaaS Services solely for your governmental purposes, subject to any limits for Defined Users or Data Storage Capacity. You may add additional users or additional data storage capacity on the terms set forth in this Agreement. In the event you regularly and/or meaningfully exceed the Defined Users or Data Storage Capacity, we reserve the right to charge you additional fees commensurate with the overage(s). You acknowledge that we have no obligation to ship copies of the Tyler Software as part of the SaaS Services. Your right to use the SaaS Services applies to releases provided as part of our Maintenance and Support Services as further detailed in this Agreement.

2. Ownership.
   2.1. We retain all ownership and intellectual property rights to the SaaS Services, the Tyler Software, and anything developed by us under this Agreement. You do not acquire under this Agreement any license to use the Tyler Software in excess of the scope and/or duration of the SaaS Services.
   2.2. The Documentation is licensed to you and may be used and copied by your employees for internal, non-commercial reference purposes only.

3. Data.
   3.1. You retain all ownership and intellectual property rights to the Data. You expressly recognize that except to the extent necessary to fulfill our obligations contained in this Agreement, we do not create or endorse any Data used in connection with the SaaS Services.
   3.2. You expressly grant to us a limited, non-exclusive license to access, copy, transmit, download, display, and reproduce your Data to provide services pursuant to this Agreement. Additionally, you agree that Tyler may use deidentified Data for Client or third-party demonstrative or training purposes.
   3.3. Our access to and use of your Data necessary to use the Tyler Software or SaaS Services will comply with applicable provisions of our Privacy Statement (available at https://www.tylertech.com/privacy) and applicable law.
   3.4. Data Breach Notification. Tyler will provide notice of a breach of Client Data in accordance with applicable state and federal data breach notification laws.

4. Restrictions.
   4.1. You may not:
      4.1.1. make the Tyler Software or Documentation resulting from the SaaS Services available in any manner to any third party for use in the third party's business operations;
      4.1.2. modify, make derivative works of, disassemble, reverse compile, or reverse engineer any part of the SaaS Services;
      4.1.3. access or use the SaaS Services to build or support, and/or assist a third party in building or supporting, products or services competitive to us; or
      4.1.4. license, sell, rent, lease, transfer, assign, distribute, display, host, outsource, disclose, permit timesharing or service bureau use, or otherwise commercially exploit or make the SaaS Services, Tyler Software, or Documentation available to any third party other than as expressly permitted by this Agreement.
      4.1.5. Notwithstanding anything to the contrary in this Section 4.1, you may disclose, with our written consent, not to be unreasonably withheld, the Tyler Software, SaaS Services, or Documentation to a third party you consult with regarding the implementation or use of the Tyler Software and SaaS Services. You must ensure that any such third-party's use is subject to the terms of this Agreement, and you acknowledge and agree that you are liable for any breach of the terms of this Agreement by such third party.

5. Software Warranty. We warrant that the Tyler Software will perform without Defects during the term of this Agreement. If the Tyler Software does not perform as warranted, we will use all reasonable efforts, consistent with industry standards, to cure the Defect in accordance with our then-current Support Call Process.

6. SaaS Services.
   6.1. *Audit & Compliance*. Our SaaS Services are audited at least yearly in accordance with the AICPA's Statement on Standards for Attestation Engagements ("SSAE") No. 21. We have attained, and will maintain, SOC 1 and SOC 2 compliance, or their equivalent, for so long as you are timely paying for SaaS Services. The foregoing notwithstanding, you acknowledge that the scope of audit coverage varies depending on the specific Tyler Software solution. We will provide you with a summary of our current compliance report(s) or its equivalent, upon your request. For the avoidance of doubt, if our SaaS Services are provided using a third-party data center, the compliance report may be for that third-party provider and be subject to confidential treatment in accordance with applicable law. If you want us to provide our compliance reports to a third-party auditor or similar entity, we reserve the right to require execution of an NDA by that third party.
   6.2. *Service Levels*. The Tyler Software will be made available to you according to the terms of the SLA. Tyler SaaS Services will be provided via a third-party data center. Your Data will be inaccessible to our other customers.
   6.3. *Business Continuity*. Data centers used to deliver SaaS Services for this Agreement have redundant telecommunications access, electrical power, and the required hardware to provide access to the SaaS Services in the event of a disaster or component failure. We test our disaster recovery plan on an annual basis. The plan is not client specific and is detailed in Tyler's System & Organization Control reports or their equivalent. In the event of a data center failure, we reserve the right to employ our disaster recovery plan for resumption of the SaaS Services. In that event, we commit to a Recovery Point Objective ("RPO") of 24 hours and a Recovery Time Objective ("RTO") of 24 hours. RPO represents the maximum duration of time between the most recent recoverable copy of your hosted Data and subsequent data center failure. RTO represents the maximum duration of time following data center failure within which your access to the Tyler Software must be restored. If we employ our disaster recovery plan, we will be responsible for restoring your Data and ensuring that the SaaS Services are online, and you will be responsible for validating your Data and confirming the functioning of the SaaS Services, including any integrations.
   6.4. *Security Measures*. We provide secure Data transmission paths between your devices and the data center used to provide SaaS Services to you. Data centers used to provide SaaS Services are accessible only by authorized personnel with a unique key entry or comparable security. We conduct annual penetration testing of either the production network and/or web application to be performed. We will maintain industry standard intrusion detection and prevention systems to monitor malicious activity in the network and to log and block any such activity. You may not attempt to bypass or subvert security restrictions in the SaaS Services or environments related to the Tyler Software. Unauthorized attempts to access files, passwords, or other confidential information, and vulnerability and penetration test scanning of our network and systems (hosted or otherwise) are prohibited. Where applicable with respect to our applications that take or process card payment data, we comply with applicable requirements of PCI DSS. We agree to supply the then-current status of our PCI DSS compliance program in the form of an official Attestation of Compliance, which can be found at https://www.tylertech.com/about-us/compliance and, in the event of any change in our status, we will comply with applicable notice requirements.
   6.5. *Password Security*. You are responsible for:
      6.5.1. keeping your and your representatives' passwords secure and confidential;
      6.5.2. any account activity or access that occurs pursuant to you and your representatives' passwords, its account or IdPs; and
      6.5.3. notifying us of any unauthorized access to your account.

SECTION C – PROFESSIONAL SERVICES

1. Professional Services. We will provide you the various implementation-related services itemized in the Investment Summary and if applicable, described in the Statement of Work.

2. Professional Services Fees. You agree to pay us the services fees in the amounts set forth in the Investment Summary. You acknowledge that the fees stated in the Investment Summary, unless expressly stated otherwise, are good-faith estimates of the amount of time and materials required for your implementation. We will bill you the actual fees incurred based on the in-scope services provided to you. Any discrepancies in the total values set forth in the Investment Summary will be resolved by multiplying the applicable rate by the quoted units.

3. Additional Services. The Investment Summary contains, and the Statement of Work describes, the scope of services and related costs (including programming and/or interface estimates) required for the project based on our understanding of the specifications you supplied. If additional work is required, or if you use or request additional services, we will provide you with an addendum or change order, as applicable, outlining the costs for the additional work. The price quotes in the addendum or change order will be valid for thirty (30) days from the date of the quote.

4. Cancellation. If you cancel services less than four (4) weeks in advance (other than for Force Majeure or breach by us), you will be liable for all (i) daily fees associated with cancelled professional services if we are unable to reassign our

personnel and (ii) any non-refundable travel expenses already incurred by us on your behalf. We will make all reasonable efforts to reassign personnel in the event you cancel within four (4) weeks of scheduled commitments.

5. Services Warranty. We will perform services in a professional, workmanlike manner, consistent with industry standards. In the event we provide services that do not conform to this warranty, we will re-perform such services at no additional cost to you.

6. Site Access and Requirements. At no cost to us, you agree to provide us with reasonable access to your personnel, facilities, and equipment as may be reasonably necessary for us to provide implementation services, subject to any reasonable security protocols or other written policies provided to us as of the Effective Date, and thereafter as mutually agreed to by you and us.

7. Background Checks. All of our employees undergo criminal background checks prior to hire. All employees sign our confidentiality agreement and security policies.

8. Client Assistance. You acknowledge that the implementation of the Tyler Software is a cooperative process requiring the time and resources of your personnel. You certify that you will use reasonable efforts to cooperate with us and make your resources available for the performance of the Agreement in accordance with its terms and the mutually agreed project schedule. Additionally, you agree to use all reasonable efforts to cooperate with and assist us as may be reasonably required to support the efficient execution of the activities required for this Agreement. Accordingly, you will provide notice of any known inability to timely meet a project commitment so that appropriate project adjustments can be made. We will not be liable for failure to meet any project deadlines or milestones when such failure is due to Force Majeure or to the failure by you to comply with the requirements of this paragraph.

9. Maintenance and Support Services.
    9.1. For the duration of this Agreement, consistent with the terms set forth in our then-current Support Call Process, we will:
        9.1.1. perform our maintenance and support obligations in a professional and workmanlike manner, consistent with industry standards, to provide support and resolve Defects in the Tyler Software (subject to any applicable release life cycle policy);
        9.1.2. provide telephone support during our established support hours as indicated in our then-current Support Call Process;
        9.1.3. maintain personnel that are sufficiently trained to be familiar with the Tyler Software and Third-Party Software, if any, in order to provide maintenance and support services;
        9.1.4. provide releases to the Tyler Software (including updates and enhancements) that we make generally available without additional charge to customers with a current SaaS Agreement.
    9.2. Your use of Tyler Software or SaaS Services requires that you remain current with supported releases of Tyler Software as indicated in any applicable release lifecycle policy. Our warranty and support commitments are contingent upon you using a supported version of the Tyler Software. Tyler may require you to update to a current version of the Tyler Software to address a critical issue (for example, to address an identified security vulnerability in the Tyler Software or a third-party component). Tyler will use commercially reasonable efforts to (i) minimize the number of such instances and (ii) provide as much advance notice as possible.
    9.3. We will use all reasonable efforts to perform support services remotely. We reserve the right to use secure third-party connectivity tools to deliver maintenance and support services. We also reserve the right to collect Tyler Software or SaaS Services telemetry for product evaluation, quality assurance, and security monitoring and enhancement purposes. You agree to reasonably cooperate with us in providing access to your environments and Data for the purposes of providing maintenance and support services and acknowledge that our warranty, support, and service level obligations under this Agreement are contingent upon receiving reasonable access to your Data and systems.
    9.4. For the avoidance of doubt, SaaS Fees do not include the following services: (a) onsite support; (b) application design; (c) other consulting services; or (d) telephone support outside our normal business hours as listed in our then-current Support Call Process.

EXHIBIT E.3
INVOICING AND PAYMENT TERMS

We will provide you with the software and services set forth in the Investment Summary of the Agreement. Capitalized terms not otherwise defined will have the meaning assigned to such terms in the Agreement.

Invoicing: We will invoice you for the applicable software and services in the Investment Summary as set forth below. Your rights to dispute any invoice are set forth in the Agreement.

1. Tyler Annual Services.
   1.1. *SaaS Services*. SaaS Fees are invoiced on an annual basis, beginning on the commencement of the initial term as set forth in Section E(1) of this Agreement. Your annual SaaS fees for the initial term are set forth in the Investment Summary. Upon expiration of the initial term, your annual SaaS fees will be as set forth in the Investment Summary. SaaS Fees for any renewal terms beyond the fourth option term will be at our then-current rates.
   1.2. *Other Annual Services*. Fees for annual services other than SaaS Services are invoiced on an annual basis, beginning with the availability of the service. Your annual fees for the initial term are set forth in the Investment Summary. Upon expiration of the initial term, your annual fees will be as set forth in the Investment Summary. Annual fees for any renewal terms beyond the fourth option term will be at our then-current rates.

2. Tyler Services.
   2.1. *Professional Services Generally*: Unless otherwise indicated below, fees for Tyler services are invoiced as delivered.
   2.2. *Consulting Services*: Fixed fee Consulting Services will be invoiced 50% upon your acceptance of the Best Practice Recommendations, by module, and 50% upon your acceptance of custom desktop procedures, by module.
   2.3. *Conversions*: Fixed-fee conversions are invoiced 50% upon initial delivery of the converted Data, by conversion option, and 50% upon Client acceptance to load the converted Data into Live/Production environment, by conversion option. Where conversions are quoted as estimated, we will bill you the actual services delivered on a time and materials basis. Any additional hours for conversions services will be added via an amendment as outlined in Section 16 of this Contract.
   2.4. *Requested Modifications to the Tyler Software*: Requested modifications to the Tyler Software are invoiced (i) 50% upon delivery of specifications and (ii) 50% upon delivery of the applicable modification. You must report any failure of the modification to conform to the specifications within thirty (30) days of delivery; otherwise, the modification will be deemed to be in compliance with the specifications after the 30-day window has passed. You may still report Defects to us as set forth in this Agreement.
   2.5. *Other Fixed Price Services*: Other fixed price services are invoiced as delivered. For the avoidance of doubt, where "Project Planning Services" are provided, payment will be due upon delivery of the Implementation Planning document. Dedicated Project Management services, if any, will be billed monthly in arrears, beginning on the first day of the month immediately following initiation of project planning. Strategic Program Management Services, if any, will be billed monthly in arrears, beginning on the first day of the month immediately following initiation of program planning.

3. Hardware & Third-Party Products.
   3.1. *Hardware*: Hardware costs, if any, are invoiced upon delivery.
   3.2. *Hardware Maintenance*: The first year maintenance fee for hardware is invoiced upon delivery of the hardware. Subsequent annual maintenance fees for hardware are invoiced annually, in advance, at then-current rates, upon each anniversary thereof.
   3.3. *Third-Party Services*: Fees for Third-Party Services, if any, are invoiced as delivered, along with applicable expenses, at the rates set forth in the Investment Summary.
   3.4. *Third Party Software*. License Fees for Third Party Software, in any, are invoiced when the applicable Third Party Software is made available to you for download.
   3.5. *Third Party Software Maintenance*: The first year maintenance fee for the Third Party Software is invoiced when it is made available to you for downloading. Subsequent annual maintenance fees for Third Party Software are invoiced annually, in advance, at then-current rates, upon each anniversary thereof.
   3.6. *Third-Party SaaS Services*. Third-Party SaaS Services fees, if any, are invoiced on an annual basis, commencing with availability of the respective Third-Party SaaS Services. Pricing for the first year of Third-Party SaaS Services is indicated in the Investment Summary. Unless express stated otherwise, pricing for subsequent years will be at then-current rates.

4. Transaction Fees. Unless paid directly by an end user at the time of transaction, per transaction (call, message, etc.) fees are invoiced on a monthly basis. Fees are indicated in the Investment Summary and may be increased by Tyler upon notice of no less than thirty (30) days.

5. Expenses. The service rates in the Investment Summary do not include travel expenses. Expenses for Tyler delivered services will be billed as incurred and only in accordance with our then-current Business Travel Policy.

Payment. Payment for undisputed invoices is due within forty-five (45) days of the invoice date. We prefer to receive payments electronically. Our electronic payment information is available by contacting AR@tylertech.com.

EXHIBIT E.4
SERVICE LEVEL AGREEMENT

Agreement Overview

This SLA operates in conjunction with, and does not supersede or replace any part of, the Agreement. It outlines the information technology service levels related to the availability of the Tyler SaaS Services that you have requested us to provide. All other support services are documented in the Support Call Process. This SLA does not apply to any Third-Party SaaS Services.

II. Definitions. Except as defined below, all defined terms have the meaning set forth in the Agreement.

Actual Attainment: The percentage of time the Tyler Software is available during a calendar month, calculated as follows: (Service Availability – Downtime) ÷ Service Availability.
Client Error Incident: Any service unavailability resulting from your applications, content or equipment, or the acts or omissions of any of your service users or third-party providers over whom we exercise no control.
Downtime: Those minutes during Service Availability, as defined below, when all users cannot launch, login, search or save primary data in the Tyler Software. Downtime does not include those instances in which only a Defect is present.
Emergency Maintenance Window: (1) maintenance that is required to patch a critical security vulnerability; (2) maintenance that is required to prevent an imminent outage of Service Availability; or (3) maintenance that is mutually agreed upon in writing by Tyler and the Client.
Planned Downtime: Downtime that occurs during a Standard or Emergency Maintenance window.
Service Availability: The total number of minutes in a calendar month that the Tyler Software is capable of receiving, processing, and responding to requests, excluding Planned Downtime, Client Error Incidents, denial of service attacks and Force Majeure. Service Availability only applies to Tyler Software being used in the production environment.
Standard Maintenance: Routine maintenance to the Tyler Software and infrastructure. Standard Maintenance is limited to five (5) hours per week.

III. Service Availability

a. Your Responsibilities

Whenever you experience Downtime, you must make a support call according to the procedures outlined in the Support Call Process. You will receive a support case number.

b. Our Responsibilities

When our support team receives a call from you that Downtime has occurred or is occurring, we will work with you to identify the cause of the Downtime (including whether it may be the result of Planned Downtime, a Client Error Incident, denial of service attack or Force Majeure). We will also work with you to resume normal operations.

c. Client Relief

Our targeted Attainment Goal is 100%. You may be entitled to credits as indicated in the Client Relief Schedule found below. Your relief credit is calculated as a percentage of the SaaS Fees paid for the calendar month.
In order to receive relief credits, you must submit a request through one of the channels listed in our Support Call Process within fifteen (15) days of the end of the applicable month. We will respond to your relief request within thirty (30) days of receipt.
The total credits confirmed by us will be applied to the SaaS Fee for the next billing cycle. Issuing of such credit does not relieve us of our obligations under the Agreement to correct the problem which created the service interruption.
Credits are only payable when Actual Attainment results in eligibility for credits in consecutive months and only for such consecutive months.

Client Relief Schedule	
Actual Attainment	**Client Relief**
99.99% - 99.70%	Remedial action will be taken
99.69% - 98.50%	2% of SaaS Fees paid for applicable month
98.49% - 97.50%	4% of SaaS Fees paid for applicable month
97.49% - 96.50%	6% of SaaS Fees paid for applicable month
96.49% - 95.50%	8% of SaaS Fees paid for applicable month
Below 95.50%	10% of SaaS Fees paid for applicable month

* Notwithstanding language in the Agreement to the contrary, Recovery Point Objective is one (1) hour.

IV. Maintenance Notifications

We perform Standard Maintenance during limited windows that are historically known to be reliably low-traffic times. If and when maintenance is predicted to occur during periods of higher traffic, we will provide advance notice of those windows and will coordinate to the greatest extent possible with you.

Not all maintenance activities will cause application unavailability. However, if Tyler anticipates that activities during a Standard or Emergency Maintenance window may make the Tyler Software unavailable, we will provide advance notice, as reasonably practicable, that the Tyler Software will be unavailable during the maintenance window.

EXHIBIT E.5
THIRD-PARTY TERMS

DocOrigin Terms. Your use of Tyler Forms software and forms is subject to the DocOrigin End User License Agreement available for download here: https://eclipsecorp.us/eula/. By signing a Tyler Agreement or Order Form including Tyler forms software or forms, or accessing, installing, or using Tyler Forms software or forms, you agree that you have read, understood, and agree to such terms.

ThinPrint Terms. Your use of Tyler Forms software and forms is subject to the End User License Agreement terms for ThinPrint Engine, ThinPrint License Server, and Connected Gateway found here: https://www.thinprint.com/en/legal-notes/eula/. By signing a Tyler Agreement or Order Form, or accessing, installing, or using Tyler Forms software or forms, you agree that you have read, understood, and agree to such terms.

EXHIBIT E.6
STATEMENT OF WORK

INCORPORATED BY REFERENCE AS ATTACHED TO THE CONTRACT

remainder of page intentionally left blank

1.0	**Overview**
1.1	**Introduction:** Capital Metropolitan Transportation Authority (hereinafter "CMTA" or "Capital Metro") is requesting proposals to provide a Right of Way (ROW) Licensing Software solution that meets the core functionality and integra configuration and no reliance on future customization to meet baseline needs. The selected Contractor shall supply all software, proper licensing, and necessary services to fully configure and integrate the ROW Licensing solution wit The platform must provide a centralized, web-based environment accessible to internal and external users for managing ROW applications, approvals, time-based licenses, payments, and stakeholder coordination. Core, out-of-the-b * Capital Metro's ESRI GIS system, * Oracle Financial system, * Secure online payment processing platforms, * Enterprise document/content management systems, * Electronic signature software, and * Internal databases or APIs as necessary to support workflows, reporting, and auditing. To support a complete property lifecycle management process, Capital Metro also seeks the optional inclusion of a Real Estate Asset Management module. This module should integrate directly with the ROW Licensing module to sup compliance monitoring, and associated document and financial tracking—all within the same system environment. CMTA is the regional public transportation leader for Central Texas headquartered in Austin, Texas, with 30.5 million boardings each year across bus, rail, and paratransit services. See https://www.capmetro.org/facts for additional b
1.2	Architecture Requirements Capital Metro prefers a web-based solution that is scalable, secure, and integrated with existing systems, including the ESRI GIS platform. The solution should support internal and external users via modern web browsers and be depl Capital Metro's preferences. The proposals shall include the following, but not be limited to: * Description and costs for all implementation tasks to complete the setup and integration of the ROW Licensing Software and Real Estate module, if selected. * Meet all requirements outlined in this document, including the integration with ESRI GIS and support for role-based access control (RBAC). * Costs for all required licenses for the ROW Licensing Software, as well as options for the Real Estate module, if necessary. * Any other software needed to meet the functional and technical requirements outlined in this scope. * Costs for hosting the solution, whether on Capital Metro's infrastructure or a cloud-based solution (AWS, Azure, Google Cloud, etc.). * Maintenance and support based on the SLA requirements mentioned in this document. Contractor shall provide a visual schematic of the system architecture, including all vendor components, third-party components, integration interfaces (including GIS integration), security protocols, disaster response plans, and notif
1.3	Completion Date. Installation and full operation must be completed on or before TBD

Instructions:

•Columns C and D are used during the proposal/pre-award period. Proposers shall submit all questions using these columns with the corresponding Compliance Term. If a question is not specific to a compliance term herein, proposers shall er
document and paragraph reference for which the question pertains.
•For each Compliance Term, select "C-Comply", "N-Cannot Comply" or "A-Will Comply with Alternative"
•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. •Do not add comments for "C" or "N."
• The selected Contractor ("Contractor") must deliver a system encompassing all requirements including delivery of third-party products to make the solution fully functional.
• 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 Right of Way Licensi
carry out the intent herein. The Contractor shall document and discuss said needs with CMTA and implement the agreed-upon solution accordingly.
•Contractor must deliver all Compliance Terms unless it is within a section marked "Optional" that is not exercised or CMTA agrees to an alternative.
•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.
•The Project and Project Schedule shall use the Enterprise Project and Portfolio Phase Tasks and Deliverables shown on Appendix A.
•Answer all questions on Appendix B Technical Questions

	Compliance Term	Compliance	Vendor Comments
2.0	**Right of Way Licensing Software -** Minimum Requirements:		
2.1	The software must support the management and tracking of property parcels, including ownership details, legal boundaries, and easement information.		
2.2	The system must store and retrieve key ROW documents, including deeds, contracts, permits, and surveys.		
2.3	The software must provide workflow management tools for acquiring land rights, including functionality to manage offers, negotiations, and acquisitions.		
2.4	The system must generate standard reports, including landowner status, project progress, and financial tracking.		
2.5	The system must support role-based user access to ensure sensitive data is restricted to authorized personnel.		
2.6	The system must include an audit trail to track all changes made to records, supporting compliance and accountability.		

	Compliance Term	Compliance	Vendor Comments
2.7	The system must provide encryption for both stored and transmitted data to protect sensitive information.		
2.8	The system must support basic authentication mechanisms such as secure username/password login.		
2.9	The system must track ROW compliance with applicable federal, state, and local regulations.		
2.10	The system must include automated data backup features to support disaster recovery and data retention policies.		
2.11	The system must allow for the storage and management of regulatory documents such as permits, environmental assessments, and compliance certificates.		
2.12	The system must support integration with common GIS platforms (e.g., ArcGIS, Google Maps) for visualization of parcels and ROW boundaries.		
2.13	The system should support export of key data in common formats such as CSV and PDF for reporting and sharing.		
2.14	The system must be web-accessible to support users from multiple devices and locations.		
2.15	The system must make available basic mobile access for field workers to view and update parcel and ROW data in the field.		
2.16	The system must have an intuitive, user-friendly interface requiring minimal training for essential tasks.		
2.17	The system must support flexible deployment options (cloud or on-premise) to align with CMTA's infrastructure and preferences.		
2.18	The system must track property acquisitions, leases, and contractual agreements for land use as part of long-term real estate or ROW obligations.		
2.19	The Contractor must provide a support and maintenance plan, including security updates, performance patches, and issue resolution timelines.		
2.20	The system must support the generation of reports compliant with federal or regulatory standards, such as those from FHWA or FTA.		
2.21	The platform must be configurable to support large-scale infrastructure projects such as rail corridors or high-speed transportation initiatives.		
3.0	**Real Estate Asset Management Module -** Minimum Requirements: While the core function of this system is to manage the lifecycle of Right-of-Way permits and licenses, CMTA encourages the inclusion of a Real Estate Asset Manag enabling management of leased properties, acquired parcels, long-term asset tracking, and compliance post-license issuance. *** This module is not required for base system compliance but is strongly preferred to support end-to-e**		
3.1	The system must automatically transition approved license/permit data into the Real Estate module without manual data entry. This includes: Parcel and ownership information, License/permit terms, Applicant/licensee details, Associated documents, etc.		
3.2	The module must support full lifecycle tracking of real estate assets, including licensed, acquired, or leased parcels; ownership records; and easement boundaries.		
3.3	The module must support acquisition workflows including offer creation, negotiation tracking, and contract approvals.		
3.4	The module must manage leases including: Terms and expiration dates, Renewal tracking, Amendments and financial obligations, etc.		
3.5	The system must store and retrieve key documents such as deeds, lease agreements, amendments, and environmental assessments.		
3.6	The system must generate standard reports including lease status, asset utilization, financial summaries, and compliance milestones.		
3.7	The module must integrate with the GIS system to provide parcel visualization of real estate holdings.		
3.8	The system must provide configurable dashboards and alerts for lease expirations, contract milestones, and compliance deadlines.		
3.9	This module must enforce role-based access and audit trails specific to Real Estate data access and edits.		
3.10	The Real Estate module must tightly integrate with the ROW Licensing module to enable automated workflow handoffs and shared data access.		
3.11	The platform must prevent redundant data entry and ensure data consistency across both modules.		
3.12	Changes to parcel ownership or status must automatically synchronize between both modules in real-time.		
3.13	The system must generate event-driven notifications for key handoff points (e.g., "license granted," triggering RE workflow).		
3.14	The system must include Audit trails that track all data transfers, edits, and transitions between ROW and Real Estate records.		

	Compliance Term	Compliance	Vendor Comments
3.15	Cross-module workflows must allow task assignments from ROW users to RE staff, and vice versa.		
3.16	The system must support dashboards dashboards that provide a unified view of parcel/project status across both ROW and Real Estate modules.		
3.17	The system must function as a unified platform, ensuring a seamless experience and "low-touch" transitions between departments.		
3.18	Updates made in one module must be reflected immediately in the other for consistent data visibility.		
3.19	The audit trail must capture data creation, updates, deletions, and user actions across both modules.		
3.20	The system must support compliance tracking for all parcel lifecycle stages in accordance with applicable federal, state, and local laws.		
3.0	**Real Estate Module Minimum Requirements**		
3.1	The software must allow for the **management and tracking of property parcels**, including ownership, legal boundaries, easement details, and leased properties		
3.2	Ability to store and retrieve key ~~ROW~~ documents (e.g., deeds, contracts, permits, surveys).		
3.3	The system must support management of leases associated with properties, owned assets, or locations, including detailed records.		
3.4	Must have basic workflow management for acquisition of *properties to include tracking of pre and post activities.*		
3.5	The system should be able to generate standard reports (e.g., landowner status, project progress, and financial tracking).		
3.6	Must have role-based user access to ensure sensitive data is protected and only accessible to authorized personnel.		
3.7	Must include a basic audit trail to track changes made to data within the system for compliance and accountability.		
3.8	Basic encryption for both stored and transmitted data to protect sensitive information.		
3.9	Must support basic authentication mechanisms, such as username/password login.		
3.10	The software should have a basic capability to track ~~ROW~~ compliance with applicable federal, state, and local regulations.		
3.11	Must provide basic data backup features to ensure data protection and disaster recovery.		
3.12	Ability to store and manage regulatory documents like permits, environmental impact assessments, and compliance certificates.		
3.13	Must support integration with common GIS platforms (e.g., ArcGIS, Google Maps) for mapping and visualizing parcels and ROW areas.		
3.14	Should allow for exporting key data in common file formats (e.g., CSV, PDF) for reporting and sharing purposes.		
3.15	The system must be accessible via a web browser to support easy access from multiple devices and locations.		
3.16	Basic mobile access for field workers to update parcel and ROW data while in the field.		
3.17	The system should have a straightforward, intuitive interface that allows users to perform essential tasks without extensive training.		
3.18	Must provide flexibility in deployment options (cloud or on-premise) based on the organization's preference or existing infrastructure.		
3.19	The software must have an ongoing support and maintenance plan, including regular updates to address security vulnerabilities and performance issues.		
4.0	**Permit, License, Violation, and Lease Management**		
4.1	The system must track and manage multiple fee types and structures per application, including incremental license increases, recurring charges, and renewal-based fee calculations.		
4.2	The system must track and manage multiple fee types and structures per application, including incremental license increases, recurring charges, and renewal-based fee calculations.		
4.3	The system must digitize manual, paper-based processes into automated, configurable digital workflows.		
4.4	The system must allow authorized users to create, edit, and update permits and licenses directly through the interface without requiring IT intervention or back-end modifications.		
4.5	The system must support multiple review cycles per application and track each cycle's status, due dates, comments, and responsible reviewers or departments.		
4.6	The system must integrate with Esri ArcGIS (Online and Enterprise) for location-based mapping and geographic data visualization.		
4.7	he system must allow applications to be linked to specific geographic locations and track associated statuses, approvals, inspections, and corrective actions.		

	Compliance Term	Compliance	Vendor Comments
4.8	The system must maintain a searchable inventory of issued licenses, each with a system-generated unique identifier.		
4.9	The system must track license status, key dates (e.g., expiration, renewal), and associated features such as physical assets or geographic areas.		
4.10	The system must support linking of physical assets or features (e.g., parcels, infrastructure, or work orders) to licenses for enhanced asset management and historical tracking.		
4.11	he system must support searching, filtering, and viewing of licenses by key criteria such as type, status, expiration date, and associated assets.		
4.12	The system must support management of leases associated with properties, assets, or locations, including full documentation and historical tracking.		
4.13	The system must allow leases to be linked to specific rail ROW, physical assets, geographic areas, or right-of-way segments.		
4.14	The system must provide map-based visualization of lease areas, with the ability to overlay related permits and licenses for cross-referencing.		
4.15	The system must support multiple lease types and configurations, including the ability to track varying payment schedules, terms, and conditions.		
4.16	The system must integrate with CMTA's existing payment processing systems to track lease payments, reconcile transactions, and manage overdue or delinquent payments.		
4.17	The system must support configurable reminders and automatic notifications for lease renewals, upcoming payments, or approaching expirations.		
4.18	The system must be scalable, supporting a minimum of 25 active licenses at launch, with the ability to scale up or down based on organizational needs.		
4.19	The system must allow for temporary user access roles (e.g., guest access or limited-duration permissions) without compromising data security.		
4.20	The system must track the full lifecycle of leases and contracts, including payment schedules, amendments, renewals, and version history.		
4.21	The system must support tracking and management of all permits, licenses, and legal documentation associated with railroad assets and ROW use.		
5.0	**User Interface (UI) and User Experience (UX)**		
5.1	The system must provide a clean, modern, and user-friendly interface with easily identifiable icons for core functions (e.g., Submit Application, Action Items, Status, Profile, Documents).		
5.2	The system must have an intuitive and logically structured layout that minimizes the learning curve and includes a searchable knowledge base and integrated support/help module.		
5.3	The system must guide users through a step-by-step application process from initiation to completion, with clearly labeled steps and progress indicators.		
5.4	The system must automatically save user progress at regular intervals to prevent data loss due to unexpected termination or inactivity.		
5.5	The system must pre-populate application fields with data from the user's profile (e.g., name, contact information) to streamline application submission.		
5.6	The system must allow users to create, update, and manage their profiles. Customer profile information must integrate with Oracle Receivables automatically and in real time.		
5.7	The system must display, within the user profile, the real-time status of all submitted applications, action items, approvals, and associated payment information.		
5.8	The system must allow users to select a geographic location using an interactive map or to manually enter an address, without requiring access to internal systems.		
5.9	The system must include: * External search functionality for location-based searches (by address, coordinates, or landmarks). * Internal search functionality to display license-related data within the system.		
5.10	The system must be fully responsive and accessible from both desktop and mobile devices, providing a consistent experience across platforms.		
5.11	The system must allow users to download relevant regulations, guidelines, and documentation during the application process.		
5.12	The system must support user uploads of supporting documents in various formats (e.g., PDF, JPG, Excel), and must validate file types to prevent incompatible or corrupted uploads.		
5.13	The system must provide secure user authentication and comply with industry best practices for data privacy and cybersecurity.		
5.14	The system must allow internal users to directly contact applicants via email through the platform (e.g., for requesting missing documentation).		

	Compliance Term	Compliance	Vendor Comments
5.15	The system must allow internal users to track applications in real time and take actions (e.g., reject, close, return for revision) at any stage of the review process.		
5.16	The system must provide automated alerts and notifications to applicants at critical milestones (e.g., submission confirmation, approval notice, missing items) to ensure timely follow-up and regulatory compliance.		
5.17	The system must allow applicants and internal users to configure notification preferences, including email and SMS alerts.		
5.18	The system must support a live chat feature or support ticket submission system to provide users with personalized assistance.		
5.19	The system must maintain a complete and auditable log of all user activities and interactions, in compliance with applicable regulations.		
5.20	The system must be compliant with current accessibility standards (e.g., WCAG 2.1 or higher) to support users with disabilities.		
5.21	The system must support user-defined/custom fields to allow administrators to tailor forms and workflows based on agency-specific terminology or operational needs.		
6.0	**User Roles and Permissions**		
6.1	The system must allow for the definition of user roles with specific access levels (e.g., read-only, full access, no access) to ensure proper segregation of duties.		
6.2	The system must support granular, screen-level and field-level permissions to allow fine-tuned control over user access to data and actions within the system.		
6.3	The system must enable system administrators to create, manage, and modify user roles and permissions efficiently, with a clear and auditable process.		
6.4	The system must support external departments (e.g., Legal, Safety) with customizable guest access or limited roles, granting them appropriate but restricted access to relevant data.		
6.5	The system must provide functionality to create and manage security groups to ensure that only authorized users have access to sensitive data or critical functionalities.		
6.6	The system must allow for adding, deactivating, or temporarily disabling user accounts without the need for full deletion (e.g., for cases when an employee leaves the organization).		
6.7	The system must support the modification of user permissions and roles at any time, with a clear and auditable trail of changes made.		
7.0	**Workflows and Automation -** Note: For automation and alerts triggered by updates from integrated external systems (e.g., GIS, financial platforms, e-signature tools), refer to Section 11.8 under System Integration and Data Management.		
7.1	The system must allow the configuration of workflows based on predefined criteria (e.g., location, application type, license status) to ensure that tasks are routed and executed according to organizational rules.		
7.2	The system must support multi-approver workflows, including automatic notifications to stakeholders at each approval stage, along with follow-up reminders to prevent delays in the process.		
7.3	The system must enable the delegation of tasks to internal and external users, and provide real-time tracking of task completion, ensuring accountability and visibility across teams.		
7.4	The system must automatically perform document checks to ensure completeness and compliance with application requirements before allowing progress to the next stage.		
7.5	The system must send automated external notifications for critical events, such as expiring licenses, permits, leases, outstanding balances, and missing required documents, to reduce manual tracking and improve compliance.		
7.6	The system must support customizable reminders (e.g., "ticklers") to notify users of upcoming review dates, deadlines, or other key actions based on defined schedules, minimizing the risk of missed tasks.		
7.7	The system must allow for dynamic adjustment of notification conditions, content, and delivery methods (e.g., email, SMS), so users can modify reminders and alerts based on operational needs.		
7.8	The system must allow for the creation, management, and modification of document templates (e.g., permits, letters, notices), ensuring consistency and reducing the need for manual document generation.		
7.9	The system must auto-populate dynamic data fields within document templates (e.g., applicant name, dates, license details) to facilitate the automated generation of documents such as invoices, agreements, and regulatory notices, and must integrate with Oracle Receivables for invoicing.		

	Compliance Term	Compliance	Vendor Comments
7.10	The system must include functionality for managing utility relocations, with automated task assignments and notifications for coordination with internal stakeholders (e.g., engineering) and external parties (e.g., utility companies).		
	The system must automatically trigger workflow tasks or notifications for Real Estate staff once a license is granted, ensuring seamless transition from the ROW process to real estate management.		
	Tasks initiated in one module (e.g., ROW licensing) must flow automatically into workflows in the other module (e.g., lease setup or property tracking), ensuring minimal manual intervention and improved data consistency across modules.		
8.0	**GIS Integration and Mapping**		
8.1	The system must integrate with external GIS platforms and image services (e.g., Nearmap, Esri ArcGIS Online/Enterprise, internal GIS systems), ensuring accurate geospatial data and real-time imagery access.		
8.2	The system must support the creation and display of interactive maps for various use cases (e.g., parcel tracking, asset management). * External users must only see non-sensitive, publicly available data. * Internal users must have access to full map datasets, including sensitive or proprietary information, based on their role permissions.		
8.3	The system must support user-driven selection of map layers or filtering by predefined criteria, with strict role-based access controls that ensure: * External users can only access public-facing map layers. * Internal users can access all relevant geospatial layers based on their assigned security level.		
8.4	The system must allow publishing of map history and updates to the internal GIS system, with read-only and locked permissions to maintain data integrity and prevent unauthorized edits.		
8.5	The system must validate location-based data against GIS layers during application submission to ensure spatial accuracy, zoning consistency, and regulatory compliance.		
8.6	The system must allow external users to create and save temporary map features using ArcGIS Online (AGO) or similar tools, enabling interactive mapping during the permit application process without affecting permanent GIS records.		
8.7	The system must support GIS-enabled lease management by linking lease records to corresponding GIS layers or map features, allowing internal users to trace, visualize, and manage leased parcels spatially within the system.		
9.0	**Document and File Management**		
9.1	The system must provide robust, scalable storage capacity to support long-term retention of large volumes of documents, images, drawings, and records related to permits, licenses, leases, surveys, and other asset-related documentation.		
9.2	The system must allow users to upload and validate required documents during the application process, ensuring proper formatting, completeness, and association with the correct application or asset.		
9.3	The system must integrate with third-party e-signature platforms (e.g., OneSpan, DocuSign) to facilitate secure and legally compliant digital signing of contracts, agreements, and other official documents.		
9.4	The system must centralize all comments, feedback, and revision history related to an application or record within a single, auditable document trail to ensure version control and transparency.		
9.5	The system must integrate with internal content management platforms (e.g., SharePoint) to enable direct linking to externally stored documentation, avoiding duplication and ensuring single-source-of-truth access.		
9.6	The system must include validation checks to ensure all required documents are uploaded and complete prior to application submission or workflow advancement, preventing bottlenecks or rejection due to missing files.		
9.7	The system must securely store, manage, and index all lease-related documents—including deeds, amendments, payment records, and termination notices—with access controls and long-term retrieval capability to support audit and compliance functions.		
10.0	**Reporting and Analytics**		
10.1	The system must allow generation of detailed, filterable reports on all records and associated data, including permits, licenses, leases, acquisitions, and violations.		

	Compliance Term	Compliance	Vendor Comments
10.2	The system must support customizable reports based on user-defined filters (e.g., application type, status, geographic location, department), enabling tailored reporting for diverse stakeholder needs.		
10.3	The system must allow users to export reports in multiple industry-standard formats (e.g., Excel, CSV, PDF) to support offline analysis and formal documentation.		
10.4	The system must provide real-time, interactive dashboards that visually present key metrics and trends related to applications, licenses, permits, lease revenue, current payment compliance, future payment forecasts, and project status.		
10.5	The system must allow for secure sharing of dynamic reports with external stakeholders, ensuring access to up-to-date data without requiring system login or backend access.		
10.6	The system must generate comprehensive reports on licenses and leases, including current status, term start/end dates, renewal deadlines, and compliance with contractual terms.		
10.7	The system must support license and lease reporting that includes tracking of historical and future payment schedules, pending renewals, missed deadlines, and potential compliance risks.		
10.8	The system must support integration with external business intelligence and analytics tools (e.g., Power BI, Microsoft Excel, Tableau) to enable enhanced data modeling, dashboard creation, and customized visualizations.		
10.9	The system must include detailed audit and compliance reporting capabilities that track workflow activity, document changes, user actions, and regulatory status across all modules.		
10.10	The system must provide reporting on asset usage along the right-of-way corridor (e.g., utility crossings, telecommunications infrastructure), including asset type, status, ownership, and associated permits or leases.		
10.11	The system must allow authorized users to create new reports and modify existing report templates without requiring vendor or IT intervention.		
10.12	The system must support detailed reporting on property acquisitions and right-of-way management activities for use in project oversight, audit preparation, and grant compliance reporting.		
11.0	**System Integration and Data Management**		
11.1	The system must support secure, bi-directional (two-way) integration with critical platforms including, but not limited to: * Esri ArcGIS for spatial data and mapping, * Oracle Financials for billing, receivables, and general ledger, * E-signature platforms (e.g., OneSpan, DocuSign) for digital document execution. This integration must ensure real-time data exchange without requiring duplicate entry.		
11.2	The system should support direct integration with external governmental and regulatory agencies to enable collaborative application reviews, automated license status verification, and tracking of disciplinary or legal actions associated with applicants or licensees.		
11.3	The system must integrate with the organization's asset management platform (HxGN EAM) to ensure real-time tracking of leased assets, including physical condition, status, and assignment within the ROW environment.		
11.4	The system must integrate with external financial and payment platforms (e.g., eGov, Bytemark) to enable tracking, reconciliation, and reporting of incoming lease payments, missed payments, and delinquent accounts.		
11.5	The system must link licenses and lease agreements to external data repositories to support seamless data exchange, legal compliance, and up-to-date reporting. This integration must include automated synchronization of key fields (e.g., payment terms, obligations, expiration dates), enabling full audit readiness and lifecycle tracking.		
11.6	The system must provide full cross-module integration across all internal functions, including but not limited to: acquisition tracking, environmental documentation, utility relocation coordination, and ROW permit/license workflows. Integration must allow data and workflows to pass automatically between these modules.		
11.7	The system must include configurable APIs or middleware support for secure integration with additional external systems and third-party databases, allowing for future scalability and compliance with evolving operational or regulatory requirements.		

	Compliance Term	Compliance	Vendor Comments
11.8	The system must support event-driven automation and alerts based on updates received from integrated external systems. This includes, but is not limited to: * Changes in geospatial data from GIS systems (e.g., Esri ArcGIS) * Financial transactions or status updates from platforms like Oracle Financials or Bytemark * Updates in facility and asset records from CapMetro's asset management system (e.g., HxGN EAM) * Status changes or actions taken in e-signature platforms (e.g., OneSpan, DocuSign) These events must be able to trigger workflow actions, notifications, or data synchronization tasks automatically within the ROW and Real Estate system to support real-time decision-making and ensure process continuity.		
12.0	**Training and User Support**		
12.1	The vendor must provide comprehensive training for all user groups (e.g., administrators, internal staff, and external users), including initial onboarding sessions and ongoing training options throughout the system's lifecycle.		
12.2	The system must include access to up-to-date user documentation such as step-by-step user manuals, searchable video tutorials, and interactive or self-paced e-learning modules. These materials must be suitable for users with varying levels of technical proficiency.		
12.3	The vendor must provide access to a responsive help desk or technical support team with service-level commitments for issue resolution. Support must be available via multiple channels (e.g., email, phone, and online ticketing system).		
12.4	The vendor must maintain an online, continuously updated knowledge base containing FAQs, troubleshooting guides, known issues, and best practice resources. This resource must be available to both internal and external users based on permission levels.		
12.5	The vendor must deliver targeted training and updated documentation whenever new features, enhancements, or upgrades are released. Training must be delivered in a timely manner to ensure user readiness prior to deployment.		
13.0	**System Warranty**		
13.1	The system must be covered by a warranty period that guarantees the functionality of all features as described in the contract. The warranty must address any defects, issues, or non-conformance with the specified requirements.		
13.2	The vendor must provide timely resolution of bugs, defects, and security vulnerabilities during the warranty period. This includes ensuring that critical issues are addressed with appropriate urgency and that updates are made available as needed.		
13.6	The vendor must guarantee that all system bugs, defects, and security vulnerabilities identified during the warranty period are resolved in a timely manner. Security patches and updates must be provided to maintain system integrity.		
	The vendor must clearly define response and resolution times for all technical issues and support requests. Critical issues must be addressed promptly, with escalation procedures clearly outlined for unresolved matters.		
	The vendor must provide a defined escalation process for issues that cannot be resolved within the agreed-upon response times. Escalation must ensure that appropriate resources are allocated to resolve high-priority issues efficiently.		
	The warranty period must extend for a minimum of **[insert duration] months/years** from the system's final acceptance. This period must cover all aspects of system functionality and support.		
	The vendor must provide continuous support throughout the warranty period, ensuring any system failures, outages, or issues are promptly addressed to minimize operational disruptions.		
	During the warranty period, the vendor must provide detailed documentation of all updates, fixes, and changes made to the system, including release notes and the nature of the fixes. This documentation should be easily accessible to Capital Metro for auditing and review.		
	The vendor must commit to delivering system performance and uptime as specified in the Service Level Agreement (SLA). If performance metrics are not met during the warranty period, there should be clear penalties or consequences.		
	The warranty must be transferable to Capital Metro in the event of organizational changes, mergers, or project handoffs, ensuring that Capital Metro maintains coverage regardless of internal transitions.		

	Compliance Term	Compliance	Vendor Comments
	The vendor should provide options for extended post-warranty support at a predefined cost or as part of an ongoing service agreement to ensure continued system maintenance and issue resolution beyond the warranty period.		
14.0	**Ongoing Support**		
14.1	The system must provide comprehensive post-implementation support, including options for continued support and service-level agreements (SLAs) after the warranty period expires, ensuring that support remains available throughout the system's lifecycle.		
14.2	The system must provide ongoing technical support, including regular updates, patches, and maintenance.		
	The vendor must offer ongoing technical support, encompassing regular software updates, bug fixes, security patches, and system enhancements. Support must be proactive, with notifications provided for scheduled updates and critical patches.		
	The vendor must guarantee the availability of a dedicated support team, accessible during standard business hours (e.g., 8 AM to 6 PM local time) and, if required, outside of business hours for critical issues.		
	The system must include a structured process for reporting and resolving technical issues, including response time commitments and escalation protocols for high-priority incidents. Response times must be specified (e.g., critical issues resolved within 4 hours, non-urgent issues within 24 hours).		
	The system must provide a clear and detailed knowledge base, including articles, tutorials, and FAQs, for self-service support and to assist internal staff in troubleshooting.		
	The vendor must offer a robust process for handling escalated support requests, including dedicated technical specialists for critical issues and an established escalation path for rapid resolution. Critical issues must be prioritized with immediate escalation to appropriate technical resources.		
	The system must include a mechanism for tracking and prioritizing support tickets, ensuring that critical issues are addressed promptly and transparently. The system must include an interface for both customers and support teams to track the status and resolution progress of open tickets.		
	The vendor must provide access to a customer portal or service desk for submitting support requests, tracking progress, and receiving notifications on the status of open issues. The portal should include features for ticket management, feedback, and resolution tracking.		
	The vendor must offer an annual review of system performance, maintenance, and future planning to ensure ongoing alignment with evolving organizational needs. This review must include a detailed assessment of system performance, user satisfaction, and recommendations for future updates or improvements.		
15.0	**Data Archiving/Disaster Recovery/System Availability** - Minimum Requirements:		
15.1	The system must ensure continuous availability (24x7x365), with a guaranteed uptime of 99.99%, excluding scheduled maintenance. The vendor must provide a Service Level Agreement (SLA) that clearly defines the availability expectations.		
15.2	In the event of system downtime or unavailability, the system must display a custom error page or an appropriate "Page Unavailable" message. This page should inform users of the downtime and provide contact information or alternative resources for assistance.		
15.3	The system must have documented procedures for handling downtime during scheduled maintenance windows or outages, with an option for performing maintenance outside of regular office hours as needed.		
15.4	The system must have well-documented procedures for handling downtime during scheduled maintenance windows or unplanned outages. These procedures should include the ability to perform maintenance outside of regular office hours to minimize disruption to operations. Additionally, users must be informed of scheduled maintenance in advance.		

	Compliance Term	Compliance	Vendor Comments
	The system must include a comprehensive Disaster Recovery Plan (DRP) to ensure the timely restoration of system services in the event of system failure, data corruption, or natural disaster. The DRP must address both technical and operational aspects and include: recovery procedures, designated roles and responsibilities, communication protocols, and testing schedules.		
	The vendor must define and meet specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to ensure that the system can recover quickly and accurately in the event of a failure or disaster. The RTO and RPO should be aligned with business needs and clearly documented in the DRP.		
	The system must provide robust data backup mechanisms to ensure that all critical data, including application, user, and transactional data, is backed up regularly. Data should be archived in accordance with industry best practices, with automated backup processes that are validated for reliability. Backup data must be securely stored offsite or in the cloud for disaster recovery purposes. Archiving processes must ensure compliance with relevant regulatory standards for data retention.		
	The vendor must provide evidence of periodic disaster recovery testing and backup restoration validation to ensure that recovery processes are functional and effective. Test results should be documented, and any identified gaps should be addressed in a timely manner.		
	The system must ensure data consistency and integrity during the recovery process, ensuring that data restored from backups or recovered systems is reliable and accurate.		
	In the event of a system failure or disaster, the vendor must promptly inform relevant stakeholders and provide clear communication throughout the recovery process. This communication should include the status of the recovery efforts, estimated resolution times, and steps taken to prevent future occurrences.		
	The vendor must implement continuous system performance monitoring to detect and address potential issues proactively before they result in significant downtime or performance degradation. This includes monitoring for resource usage, system errors, and any anomalies that could impact uptime. Alerts must be sent to relevant stakeholders in case of critical performance issues.		
	The system must have regular, automated health checks to ensure that all system components (hardware, software, databases) are functioning optimally. These checks should detect and report on potential failures, minimizing the risk of unplanned outages. Any identified issues should trigger preemptive maintenance or corrective action.		
16.0	**Data Migration**		
16.1	The vendor must provide a comprehensive data migration plan that ensures all relevant data from the existing system is accurately and completely migrated to the new system. The plan must address, at a minimum, the following:		
16.2	Data Mapping: The vendor must create a detailed mapping of all data fields from the current system to the new system. This mapping should ensure compatibility and proper alignment of data types, structures, and formats between the old and new systems.		
16.3	Data Extraction: The vendor must perform a full extraction of all data, including documents, records, and associated metadata, from the current system. This process must ensure that no relevant data is missed.		
16.4	Data Cleansing: The vendor must thoroughly identify and resolve any data inconsistencies, errors, duplicates, or outdated information before migration. This process must ensure that only accurate and high-quality data is migrated to the new system.		
16.5	Data Transformation: The vendor must transform the data into the format required by the new system, ensuring that all data is structured and formatted in compliance with the system's specific requirements and functionality.		
16.6	Data Validation: The vendor must perform continuous validation of the data during the migration process to ensure that the data is accurate, complete, and properly mapped to the new system. This process should include checks to guarantee that no data is lost, corrupted, or altered inappropriately.		
16.7	Migration Testing: The vendor must conduct thorough testing of the migration process. This includes performing test migrations, verifying data accuracy, and ensuring that the migrated data is fully operational and integrated within the new system's workflows.		

	Compliance Term	Compliance	Vendor Comments
16.8	Data Reconciliation: The vendor must reconcile the migrated data with the original system's data to ensure that all records are transferred correctly. This process must guarantee that the migrated data matches the original data in both quantity and quality.		
16.9	Post-Migration Review: The vendor must provide a structured post-migration review period where the migrated data is thoroughly reviewed by the client. The review will verify data accuracy, completeness, and functionality within the new system, and any discrepancies identified must be promptly resolved.		
	Data Backup: Prior to starting the migration process, the vendor must ensure that a complete backup of all current system data is created and securely stored. This backup must be available for recovery in the event of any migration failure or data loss.		
	Data Migration Timeline: The vendor must provide a clear timeline for the entire migration process, including the estimated duration for each phase (data extraction, transformation, validation, testing, etc.). The timeline should be realistic, with built-in contingencies for addressing unexpected issues.		
	Change Management and Communication: The vendor must implement a change management process for keeping stakeholders informed of the progress of the data migration. Regular status updates and communication should be provided, especially during critical milestones.		
	Rollback Plan: The vendor must provide a rollback plan to revert to the original system in the event of a critical failure during the migration process. This plan should include specific steps to restore functionality and data integrity if the migration is unsuccessful.		
16.10	Ongoing Support: The vendor must offer post-migration support to address any issues or discrepancies related to the migrated data. This support must be available for a defined period and should ensure the system's smooth operation after the migration is completed. Additionally, any necessary data corrections or adjustments post-migration should be promptly addressed by the vendor.		

1.0	**Overview**
1.1	**Introduction:** Capital Metropolitan Transportation Authority (hereinafter "CMTA" or "Capital Metro") is reqtion requirements detailed in this Scope of Service, with minimal configuration and no reliance on future customization to meet baseline needs. The selected Contractor shallh Capital Metro's existing systems and workflows. The platform must provide a centralized, web-based environment accessible to internal and external users fox system functionality must include integration with: * Capital Metro's ESRI GIS system, * Oracle Financial system, * Secure online payment processing platforms, * Enterprise document/content management systems, * Electronic signature software, and * Internal databases or APIs as necessary to support workflows, reporting, and auditing. To support a complete property lifecycle management process, Capital Metro also seeks the optional inclusiport leased property tracking, land acquisition, contract administration, compliance monitoring, and associated document and financial tracking—all within the same system enviror CMTA is the regional public transportation leader for Central Texas headquartered in Austin, Texas, with 30.ackground including ridership and budgets.
1.2	Architecture Requirements Capital Metro prefers a web-based solution that is scalable, secure, and integrated with existing systems, incoyable in a cloud-based or on-premise environment, depending on Capital Metro's preferences. The proposals shall include the following, but not be limited to: * Description and costs for all implementation tasks to complete the setup and integration of the ROW Licer * Meet all requirements outlined in this document, including the integration with ESRI GIS and support for r * Costs for all required licenses for the ROW Licensing Software, as well as options for the Real Estate modu * Any other software needed to meet the functional and technical requirements outlined in this scope. * Costs for hosting the solution, whether on Capital Metro's infrastructure or a cloud-based solution (AWS, / * Maintenance and support based on the SLA requirements mentioned in this document. Contractor shall provide a visual schematic of the system architecture, including all vendor components, thirications of upcoming releases, patches, and fixes with details on
1.3	Completion Date. Installation and full operation must be completed on or before TBD

Instructions:

•Columns C and D are used during the proposal/pre-award period. Proposers shall submit all questions using these coter the questions at the bottom of the worksheet with the specific document and paragraph reference for which the question pertains.
•For each Compliance Term, select "C-Comply", "N-Cannot Comply" or "A-Will Comply with Alternative"
•The comments section shall be used for "A-will comply with an alternative" for explaining the alternative, or where r
• The selected Contractor ("Contractor") must deliver a system encompassing all requirements including delivery of th
• The requirements in the Scope of Services and Compliance Matrix are functional in nature and do not encompass alling Software solution and specific technical modifications needed to carry out the intent herein. The Contractor shall document and discuss said needs with CMTA and implement the agre
•Contractor must deliver all Compliance Terms unless it is within a section marked "Optional" that is not exercised or
•The final column entitled "Test #" shall be used during the Develop Phase when the Contractor will update the Comp
•The Project and Project Schedule shall use the Enterprise Project and Portfolio Phase Tasks and Deliverables shown o
•Answer all questions on Appendix B Technical Questions

	Compliance Term	CMTA Response
2.0	**Right of Way Licensing Software -** Minimum Requirements:	
2.1	The software must support the management and tracking of property parcels, including ownership details, legal boundaries, and easement information.	
2.2	The system must store and retrieve key ROW documents, including deeds, contracts, permits, and surveys.	
2.3	The software must provide workflow management tools for acquiring land rights, including functionality to manage offers, negotiations, and acquisitions.	
2.4	The system must generate standard reports, including landowner status, project progress, and financial tracking.	
2.5	The system must support role-based user access to ensure sensitive data is restricted to authorized personnel.	
2.6	The system must include an audit trail to track all changes made to records, supporting compliance and accountability.	

	Compliance Term	CMTA Response
2.7	The system must provide encryption for both stored and transmitted data to protect sensitive information.	
2.8	The system must support basic authentication mechanisms such as secure username/password login.	
2.9	The system must track ROW compliance with applicable federal, state, and local regulations.	
2.10	The system must include automated data backup features to support disaster recovery and data retention policies.	
2.11	The system must allow for the storage and management of regulatory documents such as permits, environmental assessments, and compliance certificates.	
2.12	The system must support integration with common GIS platforms (e.g., ArcGIS, Google Maps) for visualization of parcels and ROW boundaries.	
2.13	The system should support export of key data in common formats such as CSV and PDF for reporting and sharing.	
2.14	The system must be web-accessible to support users from multiple devices and locations.	
2.15	The system must make available basic mobile access for field workers to view and update parcel and ROW data in the field.	
2.16	The system must have an intuitive, user-friendly interface requiring minimal training for essential tasks.	
2.17	The system must support flexible deployment options (cloud or on-premise) to align with CMTA's infrastructure and preferences.	
2.18	The system must track property acquisitions, leases, and contractual agreements for land use as part of long-term real estate or ROW obligations.	
2.19	The Contractor must provide a support and maintenance plan, including security updates, performance patches, and issue resolution timelines.	
2.20	The system must support the generation of reports compliant with federal or regulatory standards, such as those from FHWA or FTA.	
2.21	The platform must be configurable to support large-scale infrastructure projects such as rail corridors or high-speed transportation initiatives.	
3.0	**Real Estate Asset Management Module -** Minimum Requirements: While the core function of this system i:ement module. This module would extend platform functionality by enabling management of leased properties, acquired parcels, long-term asset tracking, and compliance post**nd, lifecycle-based property management.**	
3.1	The system must automatically transition approved license/permit data into the Real Estate module without manual data entry. This includes: Parcel and ownership information, License/permit terms, Applicant/licensee details, Associated documents, etc.	
3.2	The module must support full lifecycle tracking of real estate assets, including licensed, acquired, or leased parcels; ownership records; and easement boundaries.	
3.3	The module must support acquisition workflows including offer creation, negotiation tracking, and contract approvals.	
3.4	The module must manage leases including: Terms and expiration dates, Renewal tracking, Amendments and financial obligations, etc.	
3.5	The system must store and retrieve key documents such as deeds, lease agreements, amendments, and environmental assessments.	
3.6	The system must generate standard reports including lease status, asset utilization, financial summaries, and compliance milestones.	
3.7	The module must integrate with the GIS system to provide parcel visualization of real estate holdings.	
3.8	The system must provide configurable dashboards and alerts for lease expirations, contract milestones, and compliance deadlines.	
3.9	This module must enforce role-based access and audit trails specific to Real Estate data access and edits.	
3.10	The Real Estate module must tightly integrate with the ROW Licensing module to enable automated workflow handoffs and shared data access.	
3.11	The platform must prevent redundant data entry and ensure data consistency across both modules.	
3.12	Changes to parcel ownership or status must automatically synchronize between both modules in real-time.	
3.13	The system must generate event-driven notifications for key handoff points (e.g., "license granted," triggering RE workflow).	
3.14	The system must include Audit trails that track all data transfers, edits, and transitions between ROW and Real Estate records.	

	Compliance Term	CMTA Response
3.15	Cross-module workflows must allow task assignments from ROW users to RE staff, and vice versa.	
3.16	The system must support dashboards dashboards that provide a unified view of parcel/project status across both ROW and Real Estate modules.	
3.17	The system must function as a unified platform, ensuring a seamless experience and "low-touch" transitions between departments.	
3.18	Updates made in one module must be reflected immediately in the other for consistent data visibility.	
3.19	The audit trail must capture data creation, updates, deletions, and user actions across both modules.	
3.20	The system must support compliance tracking for all parcel lifecycle stages in accordance with applicable federal, state, and local laws.	
3.0	**Real Estate Module Minimum Requirements**	
3.1	The software must allow for the **management and tracking of property parcels**, including ownership, legal boundaries, easement details, and leased properties	
3.2	Ability to store and retrieve key ~~ROW~~ documents (e.g., deeds, contracts, permits, surveys).	
3.3	The system must support management of leases associated with properties, owned assets, or locations, including detailed records.	
3.4	Must have basic workflow management for acquisition of *properties to include tracking of pre and post activities.*	
3.5	The system should be able to generate standard reports (e.g., landowner status, project progress, and financial tracking).	
3.6	Must have role-based user access to ensure sensitive data is protected and only accessible to authorized personnel.	
3.7	Must include a basic audit trail to track changes made to data within the system for compliance and accountability.	
3.8	Basic encryption for both stored and transmitted data to protect sensitive information.	
3.9	Must support basic authentication mechanisms, such as username/password login.	
3.10	The software should have a basic capability to track ~~ROW~~ compliance with applicable federal, state, and local regulations.	
3.11	Must provide basic data backup features to ensure data protection and disaster recovery.	
3.12	Ability to store and manage regulatory documents like permits, environmental impact assessments, and compliance certificates.	
3.13	Must support integration with common GIS platforms (e.g., ArcGIS, Google Maps) for mapping and visualizing parcels and ROW areas.	
3.14	Should allow for exporting key data in common file formats (e.g., CSV, PDF) for reporting and sharing purposes.	
3.15	The system must be accessible via a web browser to support easy access from multiple devices and locations.	
3.16	Basic mobile access for field workers to update parcel and ROW data while in the field.	
3.17	The system should have a straightforward, intuitive interface that allows users to perform essential tasks without extensive training.	
3.18	Must provide flexibility in deployment options (cloud or on-premise) based on the organization's preference or existing infrastructure.	
3.19	The software must have an ongoing support and maintenance plan, including regular updates to address security vulnerabilities and performance issues.	
4.0	**Permit, License, Violation, and Lease Management**	
4.1	The system must track and manage multiple fee types and structures per application, including incremental license increases, recurring charges, and renewal-based fee calculations.	
4.2	The system must track and manage multiple fee types and structures per application, including incremental license increases, recurring charges, and renewal-based fee calculations.	
4.3	The system must digitize manual, paper-based processes into automated, configurable digital workflows.	
4.4	The system must allow authorized users to create, edit, and update permits and licenses directly through the interface without requiring IT intervention or back-end modifications.	
4.5	The system must support multiple review cycles per application and track each cycle's status, due dates, comments, and responsible reviewers or departments.	
4.6	The system must integrate with Esri ArcGIS (Online and Enterprise) for location-based mapping and geographic data visualization.	
4.7	he system must allow applications to be linked to specific geographic locations and track associated statuses, approvals, inspections, and corrective actions.	

	Compliance Term	CMTA Response
4.8	The system must maintain a searchable inventory of issued licenses, each with a system-generated unique identifier.	
4.9	The system must track license status, key dates (e.g., expiration, renewal), and associated features such as physical assets or geographic areas.	
4.10	The system must support linking of physical assets or features (e.g., parcels, infrastructure, or work orders) to licenses for enhanced asset management and historical tracking.	
4.11	he system must support searching, filtering, and viewing of licenses by key criteria such as type, status, expiration date, and associated assets.	
4.12	The system must support management of leases associated with properties, assets, or locations, including full documentation and historical tracking.	
4.13	The system must allow leases to be linked to specific rail ROW, physical assets, geographic areas, or right-of-way segments.	
4.14	The system must provide map-based visualization of lease areas, with the ability to overlay related permits and licenses for cross-referencing.	
4.15	The system must support multiple lease types and configurations, including the ability to track varying payment schedules, terms, and conditions.	
4.16	The system must integrate with CMTA's existing payment processing systems to track lease payments, reconcile transactions, and manage overdue or delinquent payments.	
4.17	The system must support configurable reminders and automatic notifications for lease renewals, upcoming payments, or approaching expirations.	
4.18	The system must be scalable, supporting a minimum of 25 active licenses at launch, with the ability to scale up or down based on organizational needs.	
4.19	The system must allow for temporary user access roles (e.g., guest access or limited-duration permissions) without compromising data security.	
4.20	The system must track the full lifecycle of leases and contracts, including payment schedules, amendments, renewals, and version history.	
4.21	The system must support tracking and management of all permits, licenses, and legal documentation associated with railroad assets and ROW use.	
5.0	**User Interface (UI) and User Experience (UX)**	
5.1	The system must provide a clean, modern, and user-friendly interface with easily identifiable icons for core functions (e.g., Submit Application, Action Items, Status, Profile, Documents).	
5.2	The system must have an intuitive and logically structured layout that minimizes the learning curve and includes a searchable knowledge base and integrated support/help module.	
5.3	The system must guide users through a step-by-step application process from initiation to completion, with clearly labeled steps and progress indicators.	
5.4	The system must automatically save user progress at regular intervals to prevent data loss due to unexpected termination or inactivity.	
5.5	The system must pre-populate application fields with data from the user's profile (e.g., name, contact information) to streamline application submission.	
5.6	The system must allow users to create, update, and manage their profiles. Customer profile information must integrate with Oracle Receivables automatically and in real time.	
5.7	The system must display, within the user profile, the real-time status of all submitted applications, action items, approvals, and associated payment information.	
5.8	The system must allow users to select a geographic location using an interactive map or to manually enter an address, without requiring access to internal systems.	
5.9	The system must include: * External search functionality for location-based searches (by address, coordinates, or landmarks). * Internal search functionality to display license-related data within the system.	
5.10	The system must be fully responsive and accessible from both desktop and mobile devices, providing a consistent experience across platforms.	
5.11	The system must allow users to download relevant regulations, guidelines, and documentation during the application process.	
5.12	The system must support user uploads of supporting documents in various formats (e.g., PDF, JPG, Excel), and must validate file types to prevent incompatible or corrupted uploads.	
5.13	The system must provide secure user authentication and comply with industry best practices for data privacy and cybersecurity.	
5.14	The system must allow internal users to directly contact applicants via email through the platform (e.g., for requesting missing documentation).	

	Compliance Term	CMTA Response
5.15	The system must allow internal users to track applications in real time and take actions (e.g., reject, close, return for revision) at any stage of the review process.	
5.16	The system must provide automated alerts and notifications to applicants at critical milestones (e.g., submission confirmation, approval notice, missing items) to ensure timely follow-up and regulatory compliance.	
5.17	The system must allow applicants and internal users to configure notification preferences, including email and SMS alerts.	
5.18	The system must support a live chat feature or support ticket submission system to provide users with personalized assistance.	
5.19	The system must maintain a complete and auditable log of all user activities and interactions, in compliance with applicable regulations.	
5.20	The system must be compliant with current accessibility standards (e.g., WCAG 2.1 or higher) to support users with disabilities.	
5.21	The system must support user-defined/custom fields to allow administrators to tailor forms and workflows based on agency-specific terminology or operational needs.	
6.0	**User Roles and Permissions**	
6.1	The system must allow for the definition of user roles with specific access levels (e.g., read-only, full access, no access) to ensure proper segregation of duties.	
6.2	The system must support granular, screen-level and field-level permissions to allow fine-tuned control over user access to data and actions within the system.	
6.3	The system must enable system administrators to create, manage, and modify user roles and permissions efficiently, with a clear and auditable process.	
6.4	The system must support external departments (e.g., Legal, Safety) with customizable guest access or limited roles, granting them appropriate but restricted access to relevant data.	
6.5	The system must provide functionality to create and manage security groups to ensure that only authorized users have access to sensitive data or critical functionalities.	
6.6	The system must allow for adding, deactivating, or temporarily disabling user accounts without the need for full deletion (e.g., for cases when an employee leaves the organization).	
6.7	The system must support the modification of user permissions and roles at any time, with a clear and auditable trail of changes made.	
7.0	**Workflows and Automation -** Note: For automation and alerts triggered by updates from integrated external systems (e.g., GIS, financial platforms, e-signature tools), refer to Section 11.8 under System Integration and Data Management.	
7.1	The system must allow the configuration of workflows based on predefined criteria (e.g., location, application type, license status) to ensure that tasks are routed and executed according to organizational rules.	
7.2	The system must support multi-approver workflows, including automatic notifications to stakeholders at each approval stage, along with follow-up reminders to prevent delays in the process.	
7.3	The system must enable the delegation of tasks to internal and external users, and provide real-time tracking of task completion, ensuring accountability and visibility across teams.	
7.4	The system must automatically perform document checks to ensure completeness and compliance with application requirements before allowing progress to the next stage.	
7.5	The system must send automated external notifications for critical events, such as expiring licenses, permits, leases, outstanding balances, and missing required documents, to reduce manual tracking and improve compliance.	
7.6	The system must support customizable reminders (e.g., "ticklers") to notify users of upcoming review dates, deadlines, or other key actions based on defined schedules, minimizing the risk of missed tasks.	
7.7	The system must allow for dynamic adjustment of notification conditions, content, and delivery methods (e.g., email, SMS), so users can modify reminders and alerts based on operational needs.	
7.8	The system must allow for the creation, management, and modification of document templates (e.g., permits, letters, notices), ensuring consistency and reducing the need for manual document generation.	
7.9	The system must auto-populate dynamic data fields within document templates (e.g., applicant name, dates, license details) to facilitate the automated generation of documents such as invoices, agreements, and regulatory notices, and must integrate with Oracle Receivables for invoicing.	

	Compliance Term	CMTA Response
7.10	The system must include functionality for managing utility relocations, with automated task assignments and notifications for coordination with internal stakeholders (e.g., engineering) and external parties (e.g., utility companies).	
	The system must automatically trigger workflow tasks or notifications for Real Estate staff once a license is granted, ensuring seamless transition from the ROW process to real estate management.	
	Tasks initiated in one module (e.g., ROW licensing) must flow automatically into workflows in the other module (e.g., lease setup or property tracking), ensuring minimal manual intervention and improved data consistency across modules.	
8.0	**GIS Integration and Mapping**	
8.1	The system must integrate with external GIS platforms and image services (e.g., Nearmap, Esri ArcGIS Online/Enterprise, internal GIS systems), ensuring accurate geospatial data and real-time imagery access.	
8.2	The system must support the creation and display of interactive maps for various use cases (e.g., parcel tracking, asset management). * External users must only see non-sensitive, publicly available data. * Internal users must have access to full map datasets, including sensitive or proprietary information, based on their role permissions.	
8.3	The system must support user-driven selection of map layers or filtering by predefined criteria, with strict role-based access controls that ensure: * External users can only access public-facing map layers. * Internal users can access all relevant geospatial layers based on their assigned security level.	
8.4	The system must allow publishing of map history and updates to the internal GIS system, with read-only and locked permissions to maintain data integrity and prevent unauthorized edits.	
8.5	The system must validate location-based data against GIS layers during application submission to ensure spatial accuracy, zoning consistency, and regulatory compliance.	
8.6	The system must allow external users to create and save temporary map features using ArcGIS Online (AGO) or similar tools, enabling interactive mapping during the permit application process without affecting permanent GIS records.	
8.7	The system must support GIS-enabled lease management by linking lease records to corresponding GIS layers or map features, allowing internal users to trace, visualize, and manage leased parcels spatially within the system.	
9.0	**Document and File Management**	
9.1	The system must provide robust, scalable storage capacity to support long-term retention of large volumes of documents, images, drawings, and records related to permits, licenses, leases, surveys, and other asset-related documentation.	
9.2	The system must allow users to upload and validate required documents during the application process, ensuring proper formatting, completeness, and association with the correct application or asset.	
9.3	The system must integrate with third-party e-signature platforms (e.g., OneSpan, DocuSign) to facilitate secure and legally compliant digital signing of contracts, agreements, and other official documents.	
9.4	The system must centralize all comments, feedback, and revision history related to an application or record within a single, auditable document trail to ensure version control and transparency.	
9.5	The system must integrate with internal content management platforms (e.g., SharePoint) to enable direct linking to externally stored documentation, avoiding duplication and ensuring single-source-of-truth access.	
9.6	The system must include validation checks to ensure all required documents are uploaded and complete prior to application submission or workflow advancement, preventing bottlenecks or rejection due to missing files.	
9.7	The system must securely store, manage, and index all lease-related documents—including deeds, amendments, payment records, and termination notices—with access controls and long-term retrieval capability to support audit and compliance functions.	
10.0	**Reporting and Analytics**	
10.1	The system must allow generation of detailed, filterable reports on all records and associated data, including permits, licenses, leases, acquisitions, and violations.	

	Compliance Term	CMTA Response
10.2	The system must support customizable reports based on user-defined filters (e.g., application type, status, geographic location, department), enabling tailored reporting for diverse stakeholder needs.	
10.3	The system must allow users to export reports in multiple industry-standard formats (e.g., Excel, CSV, PDF) to support offline analysis and formal documentation.	
10.4	The system must provide real-time, interactive dashboards that visually present key metrics and trends related to applications, licenses, permits, lease revenue, current payment compliance, future payment forecasts, and project status.	
10.5	The system must allow for secure sharing of dynamic reports with external stakeholders, ensuring access to up-to-date data without requiring system login or backend access.	
10.6	The system must generate comprehensive reports on licenses and leases, including current status, term start/end dates, renewal deadlines, and compliance with contractual terms.	
10.7	The system must support license and lease reporting that includes tracking of historical and future payment schedules, pending renewals, missed deadlines, and potential compliance risks.	
10.8	The system must support integration with external business intelligence and analytics tools (e.g., Power BI, Microsoft Excel, Tableau) to enable enhanced data modeling, dashboard creation, and customized visualizations.	
10.9	The system must include detailed audit and compliance reporting capabilities that track workflow activity, document changes, user actions, and regulatory status across all modules.	
10.10	The system must provide reporting on asset usage along the right-of-way corridor (e.g., utility crossings, telecommunications infrastructure), including asset type, status, ownership, and associated permits or leases.	
10.11	The system must allow authorized users to create new reports and modify existing report templates without requiring vendor or IT intervention.	
10.12	The system must support detailed reporting on property acquisitions and right-of-way management activities for use in project oversight, audit preparation, and grant compliance reporting.	
11.0	**System Integration and Data Management**	
11.1	The system must support secure, bi-directional (two-way) integration with critical platforms including, but not limited to: * Esri ArcGIS for spatial data and mapping, * Oracle Financials for billing, receivables, and general ledger, * E-signature platforms (e.g., OneSpan, DocuSign) for digital document execution. This integration must ensure real-time data exchange without requiring duplicate entry.	
11.2	The system should support direct integration with external governmental and regulatory agencies to enable collaborative application reviews, automated license status verification, and tracking of disciplinary or legal actions associated with applicants or licensees.	
11.3	The system must integrate with the organization's asset management platform (HxGN EAM) to ensure real-time tracking of leased assets, including physical condition, status, and assignment within the ROW environment.	
11.4	The system must integrate with external financial and payment platforms (e.g., eGov, Bytemark) to enable tracking, reconciliation, and reporting of incoming lease payments, missed payments, and delinquent accounts.	
11.5	The system must link licenses and lease agreements to external data repositories to support seamless data exchange, legal compliance, and up-to-date reporting. This integration must include automated synchronization of key fields (e.g., payment terms, obligations, expiration dates), enabling full audit readiness and lifecycle tracking.	
11.6	The system must provide full cross-module integration across all internal functions, including but not limited to: acquisition tracking, environmental documentation, utility relocation coordination, and ROW permit/license workflows. Integration must allow data and workflows to pass automatically between these modules.	
11.7	The system must include configurable APIs or middleware support for secure integration with additional external systems and third-party databases, allowing for future scalability and compliance with evolving operational or regulatory requirements.	

	Compliance Term	CMTA Response
11.8	The system must support event-driven automation and alerts based on updates received from integrated external systems. This includes, but is not limited to: * Changes in geospatial data from GIS systems (e.g., Esri ArcGIS) * Financial transactions or status updates from platforms like Oracle Financials or Bytemark * Updates in facility and asset records from CapMetro's asset management system (e.g., HxGN EAM) * Status changes or actions taken in e-signature platforms (e.g., OneSpan, DocuSign) These events must be able to trigger workflow actions, notifications, or data synchronization tasks automatically within the ROW and Real Estate system to support real-time decision-making and ensure process continuity.	
12.0	**Training and User Support**	
12.1	The vendor must provide comprehensive training for all user groups (e.g., administrators, internal staff, and external users), including initial onboarding sessions and ongoing training options throughout the system's lifecycle.	
12.2	The system must include access to up-to-date user documentation such as step-by-step user manuals, searchable video tutorials, and interactive or self-paced e-learning modules. These materials must be suitable for users with varying levels of technical proficiency.	
12.3	The vendor must provide access to a responsive help desk or technical support team with service-level commitments for issue resolution. Support must be available via multiple channels (e.g., email, phone, and online ticketing system).	
12.4	The vendor must maintain an online, continuously updated knowledge base containing FAQs, troubleshooting guides, known issues, and best practice resources. This resource must be available to both internal and external users based on permission levels.	
12.5	The vendor must deliver targeted training and updated documentation whenever new features, enhancements, or upgrades are released. Training must be delivered in a timely manner to ensure user readiness prior to deployment.	
13.0	**System Warranty**	
13.1	The system must be covered by a warranty period that guarantees the functionality of all features as described in the contract. The warranty must address any defects, issues, or non-conformance with the specified requirements.	
13.2	The vendor must provide timely resolution of bugs, defects, and security vulnerabilities during the warranty period. This includes ensuring that critical issues are addressed with appropriate urgency and that updates are made available as needed.	
13.6	The vendor must guarantee that all system bugs, defects, and security vulnerabilities identified during the warranty period are resolved in a timely manner. Security patches and updates must be provided to maintain system integrity.	
	The vendor must clearly define response and resolution times for all technical issues and support requests. Critical issues must be addressed promptly, with escalation procedures clearly outlined for unresolved matters.	
	The vendor must provide a defined escalation process for issues that cannot be resolved within the agreed-upon response times. Escalation must ensure that appropriate resources are allocated to resolve high-priority issues efficiently.	
	The warranty period must extend for a minimum of **[insert duration] months/years** from the system's final acceptance. This period must cover all aspects of system functionality and support.	
	The vendor must provide continuous support throughout the warranty period, ensuring any system failures, outages, or issues are promptly addressed to minimize operational disruptions.	
	During the warranty period, the vendor must provide detailed documentation of all updates, fixes, and changes made to the system, including release notes and the nature of the fixes. This documentation should be easily accessible to Capital Metro for auditing and review.	
	The vendor must commit to delivering system performance and uptime as specified in the Service Level Agreement (SLA). If performance metrics are not met during the warranty period, there should be clear penalties or consequences.	
	The warranty must be transferable to Capital Metro in the event of organizational changes, mergers, or project handoffs, ensuring that Capital Metro maintains coverage regardless of internal transitions.	

	Compliance Term	CMTA Response
	The vendor should provide options for extended post-warranty support at a predefined cost or as part of an ongoing service agreement to ensure continued system maintenance and issue resolution beyond the warranty period.	
14.0	**Ongoing Support**	
14.1	The system must provide comprehensive post-implementation support, including options for continued support and service-level agreements (SLAs) after the warranty period expires, ensuring that support remains available throughout the system's lifecycle.	
14.2	The system must provide ongoing technical support, including regular updates, patches, and maintenance.	
	The vendor must offer ongoing technical support, encompassing regular software updates, bug fixes, security patches, and system enhancements. Support must be proactive, with notifications provided for scheduled updates and critical patches.	
	The vendor must guarantee the availability of a dedicated support team, accessible during standard business hours (e.g., 8 AM to 6 PM local time) and, if required, outside of business hours for critical issues.	
	The system must include a structured process for reporting and resolving technical issues, including response time commitments and escalation protocols for high-priority incidents. Response times must be specified (e.g., critical issues resolved within 4 hours, non-urgent issues within 24 hours).	
	The system must provide a clear and detailed knowledge base, including articles, tutorials, and FAQs, for self-service support and to assist internal staff in troubleshooting.	
	The vendor must offer a robust process for handling escalated support requests, including dedicated technical specialists for critical issues and an established escalation path for rapid resolution. Critical issues must be prioritized with immediate escalation to appropriate technical resources.	
	The system must include a mechanism for tracking and prioritizing support tickets, ensuring that critical issues are addressed promptly and transparently. The system must include an interface for both customers and support teams to track the status and resolution progress of open tickets.	
	The vendor must provide access to a customer portal or service desk for submitting support requests, tracking progress, and receiving notifications on the status of open issues. The portal should include features for ticket management, feedback, and resolution tracking.	
	The vendor must offer an annual review of system performance, maintenance, and future planning to ensure ongoing alignment with evolving organizational needs. This review must include a detailed assessment of system performance, user satisfaction, and recommendations for future updates or improvements.	
15.0	**Data Archiving/Disaster Recovery/System Availability** - Minimum Requirements:	
15.1	The system must ensure continuous availability (24x7x365), with a guaranteed uptime of 99.99%, excluding scheduled maintenance. The vendor must provide a Service Level Agreement (SLA) that clearly defines the availability expectations.	
15.2	In the event of system downtime or unavailability, the system must display a custom error page or an appropriate "Page Unavailable" message. This page should inform users of the downtime and provide contact information or alternative resources for assistance.	
15.3	The system must have documented procedures for handling downtime during scheduled maintenance windows or outages, with an option for performing maintenance outside of regular office hours as needed.	
15.4	The system must have well-documented procedures for handling downtime during scheduled maintenance windows or unplanned outages. These procedures should include the ability to perform maintenance outside of regular office hours to minimize disruption to operations. Additionally, users must be informed of scheduled maintenance in advance.	

	Compliance Term	CMTA Response
	The system must include a comprehensive Disaster Recovery Plan (DRP) to ensure the timely restoration of system services in the event of system failure, data corruption, or natural disaster. The DRP must address both technical and operational aspects and include: recovery procedures, designated roles and responsibilities, communication protocols, and testing schedules.	
	The vendor must define and meet specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to ensure that the system can recover quickly and accurately in the event of a failure or disaster. The RTO and RPO should be aligned with business needs and clearly documented in the DRP.	
	The system must provide robust data backup mechanisms to ensure that all critical data, including application, user, and transactional data, is backed up regularly. Data should be archived in accordance with industry best practices, with automated backup processes that are validated for reliability. Backup data must be securely stored offsite or in the cloud for disaster recovery purposes. Archiving processes must ensure compliance with relevant regulatory standards for data retention.	
	The vendor must provide evidence of periodic disaster recovery testing and backup restoration validation to ensure that recovery processes are functional and effective. Test results should be documented, and any identified gaps should be addressed in a timely manner.	
	The system must ensure data consistency and integrity during the recovery process, ensuring that data restored from backups or recovered systems is reliable and accurate.	
	In the event of a system failure or disaster, the vendor must promptly inform relevant stakeholders and provide clear communication throughout the recovery process. This communication should include the status of the recovery efforts, estimated resolution times, and steps taken to prevent future occurrences.	
	The vendor must implement continuous system performance monitoring to detect and address potential issues proactively before they result in significant downtime or performance degradation. This includes monitoring for resource usage, system errors, and any anomalies that could impact uptime. Alerts must be sent to relevant stakeholders in case of critical performance issues.	
	The system must have regular, automated health checks to ensure that all system components (hardware, software, databases) are functioning optimally. These checks should detect and report on potential failures, minimizing the risk of unplanned outages. Any identified issues should trigger preemptive maintenance or corrective action.	
16.0	**Data Migration**	
16.1	The vendor must provide a comprehensive data migration plan that ensures all relevant data from the existing system is accurately and completely migrated to the new system. The plan must address, at a minimum, the following:	
16.2	Data Mapping: The vendor must create a detailed mapping of all data fields from the current system to the new system. This mapping should ensure compatibility and proper alignment of data types, structures, and formats between the old and new systems.	
16.3	Data Extraction: The vendor must perform a full extraction of all data, including documents, records, and associated metadata, from the current system. This process must ensure that no relevant data is missed.	
16.4	Data Cleansing: The vendor must thoroughly identify and resolve any data inconsistencies, errors, duplicates, or outdated information before migration. This process must ensure that only accurate and high-quality data is migrated to the new system.	
16.5	Data Transformation: The vendor must transform the data into the format required by the new system, ensuring that all data is structured and formatted in compliance with the system's specific requirements and functionality.	
16.6	Data Validation: The vendor must perform continuous validation of the data during the migration process to ensure that the data is accurate, complete, and properly mapped to the new system. This process should include checks to guarantee that no data is lost, corrupted, or altered inappropriately.	
16.7	Migration Testing: The vendor must conduct thorough testing of the migration process. This includes performing test migrations, verifying data accuracy, and ensuring that the migrated data is fully operational and integrated within the new system's workflows.	

	Compliance Term	CMTA Response
16.8	Data Reconciliation: The vendor must reconcile the migrated data with the original system's data to ensure that all records are transferred correctly. This process must guarantee that the migrated data matches the original data in both quantity and quality.	
16.9	Post-Migration Review: The vendor must provide a structured post-migration review period where the migrated data is thoroughly reviewed by the client. The review will verify data accuracy, completeness, and functionality within the new system, and any discrepancies identified must be promptly resolved.	
	Data Backup: Prior to starting the migration process, the vendor must ensure that a complete backup of all current system data is created and securely stored. This backup must be available for recovery in the event of any migration failure or data loss.	
	Data Migration Timeline: The vendor must provide a clear timeline for the entire migration process, including the estimated duration for each phase (data extraction, transformation, validation, testing, etc.). The timeline should be realistic, with built-in contingencies for addressing unexpected issues.	
	Change Management and Communication: The vendor must implement a change management process for keeping stakeholders informed of the progress of the data migration. Regular status updates and communication should be provided, especially during critical milestones.	
	Rollback Plan: The vendor must provide a rollback plan to revert to the original system in the event of a critical failure during the migration process. This plan should include specific steps to restore functionality and data integrity if the migration is unsuccessful.	
16.10	Ongoing Support: The vendor must offer post-migration support to address any issues or discrepancies related to the migrated data. This support must be available for a defined period and should ensure the system's smooth operation after the migration is completed. Additionally, any necessary data corrections or adjustments post-migration should be promptly addressed by the vendor.	

EXHIBIT H – AUTHORIZATION OF WORK PRODUCT

DESCRIPTION: Right of Way Inventory Asset Management Software
CONTRACT NO.: **500306**

Authority's Contracting Officer (CO)
A. The CO for administration of this Contract is Danny Solano.
B. Phone: 512-389-7446
C. Email: danny.solano@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 Christopher Rompel.
B. Phone: 512-965-1533
C. Email: christopher.rompel@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

Erik Graney-Senior Corporate Attorney	02/05/2026
Contractor – *must sign and return with Offer*	Date
E-SIGNED by Christopher Rompel on 2026-02-05 22:38:33 GMT	February 05, 2026
Authority's Project Manager (PM)	Date
E-SIGNED by Danny Solano on 2026-02-05 22:39:03 GMT	February 05, 2026
Authority's Contracting Officer (CO)	Date

EXHIBIT IT-REVISED-1
HOSTED SOLUTIONS

ADDITIONAL TERMS AND CONDITIONS FOR THE PERFORMANCE OF INFORMATION TECHNOLOGY (IT) PRODUCTS AND SERVICES

1. DEFINITIONS

Unless otherwise specified in Exhibit E of the Contract, the following definitions shall apply, if applicable:

(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 Project, the Contract, and the parties all as in effect as of the date of the Contract and as amended during the Service Term of the Contract.

(b) "Application" means the technical system, platform, application and/or subscription services to be provided by the Contractor, as may be further described in the Technical Specifications.

(c) "Authority Data" means all data, content and information:

(i) submitted by or on behalf of the Authority or Customers to the Contractor or loaded into the System,

(ii) obtained, developed, produced or processed by the Contractor or by the Application or System in connection with the Contract, or

(d) 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"Confidential Information" shall have the meaning set forth in Section 9(b) of this Exhibit.

(e) "Contractor's Certification" shall have the meaning set forth in Section 4(d) of this Exhibit.

(f) "Contractor Technology" means:

(g) the System,

(ii) the Application, and

(iii) any technology, information, content and data, together with intellectual property rights related thereto, owned or used by the Contractor in the performance of the Services.

(i) "Customer" means any purchaser of products or services from the Authority.

(j) "Deliverables" means all information, data, materials, devices (including equipment and hardware), software (including the Application) and other items to be delivered by the Contractor to the Authority, as specified in the Project Plan.

(k) "Documentation" means the documentation provided to the Authority, including user manuals and operator instructions related to the Application furnished by the Contractor to the Authority in any format, including paper and electronic.

(l) "Malware" means any malicious data, code script, active content program, or other malicious software that could damage, destroy, alter or disrupt any computer program, data, firmware or hardware.

(m) "Process" or "Processing" means, with respect to any Authority Data, to migrate, 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 any Authority Data with information from other sources and the application of algorithmic analysis to create new or derivative data sets from any Authority Data.

(n) "Project" means the project related to the Application and the Authority's information technology systems as described in more detail in this Exhibit.

(o) "Project Plan" or "Statement of Work" means the project plan for the implementation, customization, configuration and/or installation or hosting of the Application and the Services and Deliverables required for the Project, as approved by the Authority in writing.

(p) "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.

(q) "Security Incident" means:

(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 (viiii).

(r) "Service Levels" shall have the meaning set forth in Section 11(a) of this Exhibit.

(s) "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 Authority Data and the Authority Electronic Property from unauthorized processing, destruction, modification, distribution and use, as approved in writing by the Authority.

(t) "Service Term" means:

(i) the term of the contract as set forth in Exhibits A or E to the Contract, or

(ii) with respect to any hosted service related to the Application, the specific term or period for subscription services set forth in Exhibits A or E of the Contract.

(u) "Services" means all services to be performed by the Contractor for or on behalf of the Authority or Customers, as described in the Project Plan and this Exhibit.

(v) "System" means an application, network, database or system provided or used to perform the Services by the Contractor.

(w) "Technical Specifications" means the technical specifications, functional specifications, descriptions, designs, standards, instructions, and business requirements of the Authority related to the Application and the Authority's information technology systems, as may be further described in the Contract.

(x) "Termination Assistance Services" means the Contractor's cooperation with the Authority in order to assist in the transfer of Authority Data to the Authority and to facilitate the transition to an alternative software or service for the Application at such time when the Authority may obtain authorization and/or funding for such replacement.

(y) "Updates" means all bug fixes, error corrections, patches, updates, upgrades or new releases or version of the Application during the Service Term.

2. CONTRACTOR REQUIREMENTS

(a) Unless specified in the applicable Project Plan, the Contractor shall furnish, at its own expense, all resources, personnel, equipment, tools, and supplies necessary for the full access and use of the Application and the timely performance of the Services and the Deliverables. The Contractor may use any means necessary and appropriate to perform the Services and the Deliverables under the Contract; provided, however, that in no event shall the Contractor take any action that may subject either it or the Authority to civil or criminal liability.

(b) The Contractor will establish and manage all Security Requirements necessary to protect the integrity of the Authority Data and permit appropriate access to the Application and the Authority Electronic Property. The Contractor will enable and stop access as users enter and leave the Application. The Contractor will cooperate with and assist the Authority and its other Project contractors to implement security protocols (e.g., firewalls, SSI, etc.) and take appropriate actions with respect to the Application and all Authority Data stored therein and the Authority Electronic Property so as to enable the Contractor to satisfy its obligations under the Contract and to help prevent the loss, alteration or unauthorized access to the Application and all Authority Data stored therein, or the Authority Electronic Property, to the extent within the Contractor's control. The Contractor will, upon the Authority's request, for each year of the Term of the Contract under the Project Plan, provide to the Authority copies of monthly firewall logs and third-party audit reports, summaries of test results and other equivalent evaluations with regard to security and confidentiality in connection with the Services that the Contractor provides to the Authority. The Contractor will use commercially reasonable efforts in accordance with the Security Requirements to secure the Application and all Authority Data stored therein against access by parties external to the Project and by unauthorized users, and against damage, disruption and other activity aimed at data availability or the services or other trespass or illegal actions. The Contractor will employ computer anti- Malware protections and other reasonable commercial means to ensure a safe computing environment. The Contractor agrees that it will, and it will cause its personnel and contractors to timely comply with the Authority's privacy policies and safety and network security policies, as the same may be provided to the Contractor, at all times while on-site at the Authority's facilities or remotely accessing the Authority's systems or facilities (including Authority Electronic Property). The Contractor and/or its designated third-party auditor(s) will perform all audits necessary to ensure the Authority Data integrity and adherence to the Security Requirements of the Project. As part of its routine audits, the Contractor will, on a regular basis, test the integrity of Authority Data backed up by the Authority or its Project Contractors.

(c) 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 and the Authority's information technology system provided to Contractor in advance. when on-site at the Authority's premises and all Applicable Laws.

(d) 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.

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

(i) the Contractor must notify the Authority in writing promptly after concluding that the Contractor has the legal authority to notify such Customers or employees and explain in such notice to the Authority the basis for the legal obligation and

(ii) the Contractor will limit the notices to Customers and any employees of the Authority regarding a Security Incident and the Contractor will assist with sending such notices if so requested by the Authority.

3. ADDITIONAL REPRESENTATIONS AND WARRANTIES

In addition to all other representations, warranties, and covenants included in the Contract, Contractor represents, warrants, and covenants, for itself, its employees, subcontractors and agents that:

(a) it is not contractually prohibited from engaging in the Services or providing the Deliverables, and that it is not a party to any contract or under any obligation which conflicts with the terms of the Contract or which prohibits Contractor from carrying out its responsibilities under the Contract;

(b) it is fully able to furnish the Services as contemplated by the Contract;

(c) there are no contracts to which it is a party which would prevent its timely and complete performance of the terms and conditions of the contract, and the Contractor agrees not to enter into any such contract during the pendency of the Contract;

(d) it is experienced in the type of software engineering necessary for completion of the Project, and it understands the complexity involved in this type of project and the necessity of coordination of its Services with stakeholders within which the Project will be performed;

(e) there are no contracts to which it is a party which would prevent its timely and complete performance of the terms and conditions of the contract, and the Contractor agrees not to enter into any such contract during the pendency of the Contract;

(f) the Application will not contain any Malware at all times during which the Application is made available for access and use by the Authority's user or Customers, or any Authority Data is processed using the Application. Any patches, Updates, upgrades or error corrections to the Application provided by the Contractor likewise will not contain any Malware;

(g) the Application will not contain any security mechanisms, including, but not limited to, copy protect mechanisms, encryptions, time-activated disabling devices or other codes, instructions or devices which may disable the modules or other software or erase or corrupt data;

(h) the Application will comply with all Applicable Laws at all times from the date of Acceptance to the expiration of the applicable warranty period;

(i) With respect to the Application,

(i) all modules and other materials (other than third party software and hardware approved by the Authority) will be original;

(ii) there is, and on the date of Acceptance will be, no claim, litigation or proceeding pending or threatened against the Contractor with respect to the Application, or any component thereof, alleging infringement or misappropriation of any patent, copyright, trade secret, trademark or any other personal or proprietary right of any third party in any country; and

(iii) the Application, and any use thereof, shall not infringe upon any Intellectual Property Right of any third party in any country; and

(j) The System will not contain or otherwise be developed using any Open Source Software (as defined below) in a manner that subjects the Authority to any license obligations of such Open Source Software. "Open Source Software" means any software licensed under terms requiring that other software combined or used or distributed with such software:

(ii) be disclosed or distributed in source code form, or

(iii) be licensed on terms inconsistent with the terms of the Contract.

4. OWNERSHIP OF THE AUTHORITY MARKS, AUTHORITY DATA

(a) The Contractor will not:

(i) use or register any trademark, service mark or domain name that is identical to or confusingly similar to any trademark, service mark, logo or other name owned or used by the Authority, including domain names and trade dress; or

(ii) create, acquire, license or support any internet keyword or search term that contains any such marks or other Intellectual Property Rights owned or licensed by the Authority, except as expressly provided in the Project Plan and only in the performance of the Services for the benefit of the Authority. All use thereof inures solely to the benefit of the Authority and is subject to the Authority's quality control and standard guidelines.

(b) 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 any Authority Data, together with all improvements, derivative works or enhancements to any of the foregoing and all intellectual property rights related thereto. Except as expressly authorized in this Exhibit or the Contract in the performance of the Services solely for the benefit of the Authority or Customers, 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. The Contractor will not use any Authority Data in a manner that is harmful to the Authority.

5. USE OF AUTHORITY'S NAME

The Contractor agrees not to make any written use of or reference to the Authority's name for any marketing, public relation, advertising, display or other business purpose or make any use of Authority Data for any activity unrelated to the express business purposes and interests of the Authority under the Contract, without the prior written consent of the Authority, which consent will not be unreasonably withheld. The foregoing notwithstanding, the Authority agrees that Contractor may make written use of or reference to the Authority's name for the purpose of providing a client list in response to requests for proposals.

6. APPROVAL

Any approval given by the Authority shall not relieve the Contractor of its obligations and other duties under the Contract or be construed as an assumption or waiver by the Authority.

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

EXHIBIT IT-REVISED-1

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) "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.

(b) "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.

(c) "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.

(d) "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.

(e) "Remediation Efforts" means, with respect to any Security Incident, activities designed to remedy a Security Incident which may be required by a Data Law Remediation Efforts may include:

(i) cooperation with and response to regulatory, government and/or law enforcement inquiries and other similar actions;

(ii) undertaking of investigations (internal or in cooperation with a governmental body) of such Security Incident, including forensics;

(iii) public relations and other crisis management services; and

(f) "Security Incident" means:

(g) the loss or misuse of Authority Data;

(ii) the inadvertent, unauthorized, or unlawful processing, alteration, corruption, sale, rental, or destruction of the Authority Data;

(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 (viiii).

(i) "Security Policies" means statements of direction for Security Requirements and mandating 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, statues, 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. 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. 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 if required by applicable data breach notification laws in light of Contractor's role in Processing Authority Personal Identifying Information. In Processing any Personal Identifying Information, the Contractor will reasonably support the Authority's compliance requirements 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 instruct 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,

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.

4. 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 Agreement.

5. 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 or in relation to advertisements or Internet promotions of the Authority (or its products or services) on third party websites.

6. 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

7. 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.

8. SECURITY INCIDENTS

The Contractor will timely and promptly notify the Authority upon discovering or otherwise learning of a Security Incident involving the Authority Data, 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) ensure that such Remediation Efforts provide for, without limitation, prevention of the recurrence of the same type of Security Incident, and

(b) reasonably cooperate with any Remediation Efforts undertaken by the Authority.

(c) 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.

9. 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.

EXHIBIT IT
ACCESS AND USE AGREEMENT

This Access and Use Agreement (this "Agreement") is entered into as of the effective date of the Contract to which this Agreement is attached 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 lim-ited access and use of the Authority Data 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) "Contract" means that certain contract for products and services entered into between the Contractor and Authority 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.
(c) "Security Requirements" means security measures under Applicable Laws 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 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.

2. 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 all Applicable Laws made available to Contractor as of the Effective Date, and thereafter, as mutually agreed upon by the parties.

3. SECURITY REQUIREMENTS

The Contractor will establish and manage industry standard Security Requirements necessary to protect the Authority Data integrity and permit appropriate access to the Application. The Contractor will cooperate with and assist the Authority and its contractors to implement security protocols (e.g., firewalls, SSI, etc.) and take appropriate actions with respect to all Authority Data to the extent in the Con-tractor's access, possession or control, so as to enable the Contractor to prevent the loss, alteration or unauthorized access to the Authority Data. The Contractor will employ computer anti-malware protections and other reasonable commercial means to ensure a safe computing environment. The Contractor agrees that it will, and it will cause its personnel and contractors to timely and reasonably comply with the Authority's privacy policies and safety and network security policies, as the same may be provided to the Contractor, at all times while on-site at the Authority's facilities or remotely accessing the Authority's systems or facilities (including Authority Data).

4. MISCELLANEOUS

This Agreement is made under and shall be construed in accordance with the laws of the State of Texas, and any dispute arising under this Agreement shall be settled in a state or federal court of competent jurisdiction lying in Travis County, Texas. If any of the provision of this Agreement are found to be unenforceable, the remainder shall be enforced as fully as possible and the unenforceable provision shall be deemed modified to the limited extent required to permit enforcement of the Agreement as a whole. This Agreement may be signed in multiple counterparts by hard or electronic signature (each of which shall have the same force and effect and deemed an original but all of which will together constitute but one and the same instrument).

5. SIGNATURE BLOCK

Contractor:	Tyler Technologies			**Capital Metro Transportation Authority**
By:			By:	E-SIGNED by Danny Solano on 2026-02-12 01:27:36 GMT
Print Name:	Erik Graney		Print Name:	Danny Solano
Title:	Senior Corporate Attorney		Title:	Contracting Officer
Date:	01/09/2026		Date:	12/11/2026
Address:	5101 Tennyson Pkwy, Plano TX		Address:	2910 E. 5th Street, Austin, TX
Notice:			Notice:	
Effective Date:	12/12/2026		Contract No.:	500306