METRO

CONTRACT NO. 200609

(SSP 306378)

BYTEMARK FARE SYSTEM UPGRADE

CONTRACTOR:

Bytemark, Inc
1 Pennsylvania Plaza Suite 1100
New York, NY 10119
212-206-8719

AWARD DATE: July 20, 2020

CONTRACT TERM: NTP to December 31, 2021

PRICE: $2,383,432.00

PROJECT MANAGER:

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

CONTRACT ADMINISTRATOR:

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

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

CONTRACT 200609

(SSP 306378)

BYTEMARK FARE SYSTEM UPGRADE

TABLE OF CONTENTS

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY
AUSTIN, TEXAS

AWARD/CONTRACT

1. SOLICITATION NO:	**2. CONTRACT NO.:**	**3. EFFECTIVE DATE:**
306378	200609	Upon Execution

4. BUYER

NAME:	Jeffery Yeomans	**PHONE:**	512-369-7727

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)**
Bytemark, Inc One Pennsylvania Plaza, Floor 11, Suite 1100 New York, NY 10119		
PHONE:	212-206-8719	sales@bytemark.co
FAX:	917.831.4707	

10. DBE GOAL:

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: Eric Reese, CEO
Fleur Gessner, CFO
Signature: ____________________ Date: 07/ 20 /2020

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-A-Revised-3**, Contractual Terms and Conditions, attached hereto and made a part hereof for all pertinent purposes.

2. Refer to E**xhibit-A1-Revised-1**, Contractual Terms and Conditions, attached hereto and made a part hereof for all pertinent purposes.

3. Refer to **Exhibit-E-Revised-1**, Contractual Terms and Conditions. **Ex-E-Revised-1** shall be replaced in its entirety with **Exhibit-E-Revised-2**, attached hereto and made a part hereof for all pertinent purposes.

4. Refer to **Schedule C** and **Intent to Perform** attached hereto and made a part of hereof for all pertinent purposes.

5. Refer to **Exhibit-H-Revised-2**, Contractor Performance Management Plan, Performance Deficiency Credits, attached hereto and made a part of hereof for all pertinent purposes.

ACCEPTED AS TO: Exhibit A-Revised-3, Schedule, Dated July 20, 2020, Sections 7a, Pricing, Items, 1, 2, 3, 5, 6 at the fully burdened rates specified in Section 6 for a Total Not-to-Exceed Contract Amount: $2,383,432.00.

SIGNATURE OF CONTRACTING OFFICER:

Typed Name: Muhammad Abdullah, CTCM, C.P.M. Chief Contracting Officer	Signature: E-SIGNED by Muhammad Abdullah on 2020-07-29 10:06:07 CDT Date: July 29, 2020 / /

EXHIBIT A-Revised-3-FPR

PRICING SCHEDULE

SSP 306378, BYTEMARK FARE SYSTEM UPGRADE

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)	Bytemark, Inc.		
Address	One Pennsylvania Plaza, Floor 11, Suite 1100		
City, State, Zip	New York, NY 10119		
Phone, Fax, Email	212-206-8719	917.831.4707	sales@bytemark.co
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)	Eric Reese, President / CEO		
Signature and Date			19 JUL 2020

2. ACKNOWLEDGEMENT OF AMENDMENTS

The offeror acknowledges receipt of the following amendment(s) to this solicitation (give number and date of each).

Amendment #	Date	Amendment #
1	3 July, 2020	Revised solitictation exhibits
2	16 July 2020	Revised solitictation exhibits

3. PROMPT PAYMENT DISCOUNT

# of Days		Percentage

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

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

The Authority hereby accepts this o

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

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

For further information regarding Exhibit A, you may:

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

OR

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

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

EXHIBIT B

REPRESENTATIONS AND CERTIFICATIONS

(LOCALLY FUNDED SUPPLY/SERVICE/CONSTRUCTION CONTRACTS)

MUST BE RETURNED WITH THE OFFER

1. TYPE OF BUSINESS

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

□ An individual
□ A partnership
□ A sole proprietor
☒ A corporation
□ Another entity _____

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

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:

(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:

HaCon Ingenieurgesellschaft mbH
Lister Str. 15
30163 Hannover
Germany

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 _____ [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]; **Eric Reese (CEO), Fleur Gessner (CFO)**

(ii) as an authorized agent, does certify that the principals named in subdivision (b)(2)(i) of this provision have not participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; and

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

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

4. DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION

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

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

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

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

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

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

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

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

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

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

5. COMMUNICATIONS

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

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

Individual's Name	Date/Subject of Communication
N/A	

(Attach continuation form, if necessary.)

6. CONTINGENT FEE

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

□ has
☒ has not

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

□ has
☒ has not

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

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

7. CODE OF ETHICS

(a) Statement of Purpose

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

(b) Applicability

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

(c) Standards of Ethical Conduct

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

(1) Continuously exhibit a desire to serve the public and display a helpful, respectful manner.

(2) Exhibit and embody a culture of safety in our operations.

(3) Understand, respect and obey all applicable laws, regulations and Capital Metro policies and procedures both in letter and spirit.

(4) Exercise sound judgment to determine when to seek advice from legal counsel, the Ethics Officer or others.

(5) Treat each other with honesty, dignity and respect and will not discriminate in our actions toward others.

(6) Continuously strive for improvement in our work and be accountable for our actions.

(7) Transact Capital Metro business effectively and efficiently and act in good faith to protect the Authority’s assets from waste, abuse, theft or damage.

(8) Be good stewards of Capital Metro’s reputation and will not make any representation in public or private, orally or in writing, that states, or appears to state, an official position of Capital Metro unless authorized to do so.

(9) Report all material facts known when reporting on work projects, which if not revealed, could either conceal unlawful or improper practices or prevent informed decisions from being made.

(10) Be fair, impartial and ethical in our business dealings and will not use our authority to unfairly or illegally influence the decisions of other employees or Board members.

(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 the life of the contract 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 2270.002 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. 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.

14. 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: Bytemark, Inc.

Type/Print Name of Signatory: Eric Reese

Signature:

Date: June 22, 2020

CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY

REQUIRED SUBMITTAL IF SUBCONTRACTORS ARE UTILIZED
CAPITAL METRO
Schedule C, Subcontractor Participation (Local Funds)

Instructions: The Offeror shall complete this form by listing 1) Names of all proposed subcontractors. 2) Contact information, 3) Description of work to be performed/product to be provided, 4) Age of the firm, 5) Number of employees, 6) % or $ amount of Total Contract.

NOTE: AS DEFINED BY THE SMALL BUSINESS ADMINSTRATION; A SMALL BUSINESS IS ANY BUSINESS WHOSE ANNUAL GROSS INCOME AVERAGED OVER THE PAST THREE (3) YEARS DOES NOT EXCEED THE SMALL BUSINESS ADMINISTRATION'S (SBA) SIZE STANDARDS AS SET FORTH IN 13 C.F.R., PART 121.

Size Standards for principal NAICS Sectors: **Construction** General building and heavy construction contractors: $33.5 million Special trade construction contractors: $14 million Land subdivision: $7 million Dredging: $20 million **Services** Most common: $7 million Computer programming, data processing and systems design: $25.5 million The highest annual-receipts size standard in any service industry: $35.5 million **Manufacturing** About 75 percent of the manufacturing industries: 500 employees A small number of industries: 1,500 employees The balance: either 750 or 1,000 employees **All Other Types of Small Business** Less than 500 employees or three years of gross receipts under $10 Million.

Name of Prime Contractor (Offeror):

Project Name: BYTEMARK, INC. FARE SYSTEM UPGRADE REQUIREMENTS

SSP 306378

1) Name of Subcontractor	2) Address, Telephone # of Sub Firm (Including name of contact person)	3) Description of Work, Services Provided. Where applicable, specify "supply" or "Install" or both.	4) SBE or non-SBE	5) Age of Firm	6) Number of employees	7) Sub % or $ amount of Total Contract
Five23 Group, Inc. d/b/a Lumenor Consulting Group	2111 Commerce Street Alpharetta, GA 30009	Project management, management and technical consulting services	SBE	13	22	$250,000

This form must be completed as instructed above and include every subcontractor proposed on this project.

The undersigned will enter into a formal agreement with Subcontractors for work listed in this form upon execution of a contract with Capital Metro.

Signature of Authorized Representative of Offeror

7/15/2020

Date Signed

REQUIRED SUBMITTAL

CAPITAL METRO
(Local) Intent to Perform as a SBE Contractor/SBE Subcontractor
SSP 306378

1. TO: (name of Offeror/Prime Contractor) ____Bytemark____________________

2. The undersigned is either currently certified as a SBE or will be at the time this solicitation is due.

The undersigned is prepared to perform the following described work with their own workforce and/or supply the material listed in connection with the above project (where applicable specify "supply" or "install" or both) _Five23 Group, Inc. d/b/a Lumenor Consulting Group will provide professional consulting services to include project management, management and technical consulting and training with our own workforce.____________________

and at the following price $_250,000____________ and/or _______% of the total contract amount (should be the same $ or % found on Schedule C). With respect to the proposed subcontract described above, the undersigned SBE anticipates that __0__________% of the dollar value of this subcontract will be sublet and/or awarded to other contractors. Any and all subcontractors that a SBE subcontractor uses must be listed in Schedule C and must also be SBE certified. (The SBE subcontractor should complete this section only if the SBE is subcontracting any portion of its subcontract.)

Five23 Group, Inc. d/b/a Lumenor Consulting Group		404.918.9078	7/15/2020
(Name of SBE Firm)	(Signature of Authorized Representative)	(Phone Number)	(Date Signed)
Bytemark Inc		312 617 1315	15 JUL 2020
(Name of Offeror/Prime Contractor)	(Signature of Authorized Representative)	(Phone Number)	(Date Signed)

EXHIBIT E-Revised-2
CONTRACTUAL TERMS AND CONDITIONS
(SERVICES CONTRACT)

1. DEFINITIONS

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

(a) "Applicable Anti-Corruption and Bribery Laws" means international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the Contractor's provision of goods and/or services to Authority, including without limitation "FCPA" or any applicable laws and regulations, including in the jurisdiction in which the Contractor operates and/or manufactures goods for the Authority, relating to anti-corruption and bribery.

(b) "Authority," "Capital Metro," "Cap Metro," "CMTA" means Capital Metropolitan Transportation Authority.

(c) "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.

(d) "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.

(e) "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.

(f) "Contract Modification" means any changes in the terms or provisions of the Contract which are reduced to writing and fully executed by both parties.

(g) "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.

(h) "Contract Term" means period of performance set forth in the paragraph entitled "Term" contained in Exhibit E.

(i) "Contracting Officer" means a person with the authority to enter into, administer, and/or terminate contracts and make related determinations and finding 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.

(j) "Contractor" means the entity that has assumed the legal obligation to perform the Services as identified in the Contract.

(k) "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.

(l) "FAR" means the Federal Acquisition Regulations codified in 48 C.F.R. Title 48.

(m) "FCPA" means the United States Foreign Corrupt Practices Act, 15 U.S.C. §§ 78dd-1, et seq., as amended.

(n) "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.

(o) "FTA" means the Federal Transit Administration.

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

(q) "Intellectual Property Rights" means the worldwide legal rights or interests evidenced by or embodied in: (i) any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery, or improvement, including any patents, trade secrets, and know-how; (ii) any work of authorship, including any copyrights, moral rights or neighboring rights, and any derivative works thereto; (iii) any trademark, service mark, trade dress, trade name, or other indicia of source or origin; (iv) domain name registrations; and (v) any other proprietary or similar rights. The Intellectual Property Rights of a party include all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.

(r) "Manufacturing Materials" mean any completed or partially completed supplies and materials, parts, dies, jigs, fixtures, plans, drawings, information, and contract rights specifically produced or specially acquired by the Contractor for the performance of the Contract.

(s) "Notice of Award" means formal notice of award of the Contract to the Contractor issued by the Contracting Officer.

(t) "Notice to Proceed" means written authorization for the Contractor to start the Services.

(u) "Project Manager" means the designated individual to act on behalf of the Authority, to monitor and certify the technical progress of the Contractor's Services under the terms of this Contract.

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

(w) "Services" means the services to be performed by the Contractor under this Contract, and includes services performed, workmanship, and supplies furnished or utilized in the performance of the Services.

(x) "Subcontract" means the Contract between the Contractor and its Subcontractors.

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

(z) "Works" means any tangible or intangible items or things that have been or will be prepared, created, maintained, serviced, developed, incorporated, provided or obtained by the Contractor (or such third parties as the Contractor may be permitted to engage) at any time following the effective date of the Contract, for or on behalf of the Authority under the Contract, including but not limited to any (i) works of authorship (such as literary works, musical works, dramatic works, choreographic works, pictorial, graphic and sculptural works, motion pictures and other audiovisual works, sound recordings and architectural works, which includes but is not limited to manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer software, scripts, object code, source code or other programming code, HTML code, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, and (vii) all other goods, services or deliverables to be provided to the Authority under the 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 from the Contract notice to proceed to December 31, 2021. 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 three 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

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

6. INVOICING AND PAYMENT

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

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

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

and shall conform to policies or regulations adopted from time to time by the Authority. Invoices shall be legible and shall contain, 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 supplies or Services by the Authority; and

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

(b) 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).

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

(d) 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.

7. PERFORMANCE BOND

(a) The Contractor shall provide a Performance Bond in an amount equal to one-hundred (100%) of the contract amount. The Contractor shall be required to submit the required bond to the Contracting Officer within ten (10) days from the date of Contract Award Date. The surety company providing the bond must be listed in the latest United States Treasury Department Circular 570, be authorized to do business in Texas and have an underwriting limitation equal to or greater than the penal sum of the bond. If any surety upon any bond furnished in connection with the Contract becomes insolvent, or otherwise not authorized to do business in the State, the Contractor shall promptly furnish equivalent security to protect the interest of the Authority and of persons supplying labor, materials and/or equipment in the prosecution of the Work.

(b) The bond shall be accompanied by a valid Power-of-Attorney, issued by the surety company and attached, signed and sealed, with the corporate embossed seal, to the bond, authorizing the agent who signs the bond to commit the surety company to the terms of the bond, and stating on the face of the Power-of-Attorney the limit, if any, in the total amount for which he/she is empowered to issue a single bond.

(c) A surety bond rider increasing the dollar amount of any payment and performance bond will be required for any Change that increases the contract amount.

(d) In addition, the Authority may request a surety bond increasing the dollar amount if:

(1) any surety upon any bond furnished with this Contract becomes unacceptable to the Authority;

or

(2) any surety fails to furnish reports on its financial condition as required by the Authority.

8. PAYMENT MILESTONES

Payment for each of the project phases shall be paid in the following percentages of the total contract amount:

Project Phase	Percentage
Plan	5%
Design	10%
Develop	15%
Test	15%
Deploy/Go Live	45%
Closeout	10%

9. ACCEPTANCE CRITERIA

A review of the Contractor's Services will be performed by the Authority upon delivery. If any Services performed under this Contract are deemed incomplete or unacceptable in any way, per Acceptance Criteria referenced in Exhibit F, Scope & Compliance Matrix the Authority will require the Contractor to take corrective measures at no additional cost to the Authority.

10. INSURANCE

(a) The Contractor shall furnish proof of Capital Metro-stipulated insurance requirements specified below. All insurance policies shall be primary and non-contributing with any other valid and collectible insurance or self-insurance available to the Authority and shall contain a contract waiver of subrogation in favor of the Authority. The Contractor shall furnish to the Authority certificate(s) of insurance evidencing the required coverage and endorsement(s) and, upon request, a certified duplicate original of any of those policies. Prior to the expiration of a certificate of insurance, a new certificate of insurance shall be furnished to the Authority showing continued coverage. Each policy shall be endorsed to provide thirty (30) days written notice of cancellation or non-renewal to the Authority and the Authority shall be named as an Additional Insured under each policy, Professional Liability insurance if required by this Contract. All insurance policies shall be written by reputable insurance company or companies acceptable to the Authority with a current Best's Insurance Guide Rating of ~~A+~~ **A** and Class XIII 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.

CAPITAL METRO MINIMUM COVERAGE REQUIREMENTS

(1) **Commercial General Liability Insurance** Coverage with limits of not less than One Million Dollars and No/100 Dollars ($1,000,000) 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) **Workers' Compensation Insurance** coverage in the State of Texas Statutory Workers' Compensation coverage in the State of Texas. Employers Liability Insurance with minimum limits of liability of One Million Dollars_ and No/100 Dollars ($1,000,000)

(3) **Technology Errors & Omissions Insurance**: Combined Technology & Omissions Policy with a minimum One Million and No/100 Dollars ($1,000,000) claim limit, including (a) Professional Liability Insurance covering negligent acts, errors and omissions arising from the Contractor's work to pay damages for which the Contractor may become legally obligated (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 (b) 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.~~

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

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

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

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

(f) If any part of the Contract is sublet, the Contractor shall be liable for its Subcontractor's insurance coverages of the types and in the amounts stated above, and shall furnish the Authority with copies of such Certificates of Insurance. No delay in the Services caused by the Contractor's enforcement of its Subcontractor's insurance requirements shall be excusable delay in the Contract. In the event a Subcontractor is unable to furnish insurance in the limits required under the Contract, the Contractor shall endorse the Subcontractor as an ADDITIONAL INSURED on the Contractor's policies.

(g) All insurance required to be maintained or provided by the Contractor shall be with companies and through policies approved by The Authority. The Authority reserves the right to inspect in person, prior to the commencement of the Services, all of the Contractor's insurance policy required under this Contract.

(h) The Contractor must furnish proof of the required insurance within five (5) 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.

(i) The Contractor and its lower tier Subcontractors are required to cooperate with the Authority and report all potential claims (workers' compensation, general liability and automobile liability) pertaining to this Contract to the Authority's Risk Management Department at (512) 389-7549 within two (2) days of the incident.

11. PERFORMANCE OF SERVICES BY THE CONTRACTOR

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

12. REMOVAL OF ASSIGNED PERSONNEL

The Authority may require, in writing, that the Contractor remove from the Services any employee or Subcontractor of the Contractor that the Authority deems inappropriate for the assignment.

13. REPRESENTATIONS AND WARRANTIES

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

14. 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.

15. COMPOSITION OF CONTRACTOR

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

16. SUBCONTRACTORS AND OUTSIDE CONSULTANTS

Any Subcontractors and outside associates or consultants required by the Contractor in connection with the Services covered by the Contract will be limited to such individuals or firms as were specifically identified and agreed to by the Authority in connection with the award of this Contract. Any substitution in such Subcontractors, associates, or consultants will be subject to the prior approval of the Authority.

17. EQUITABLE ADJUSTMENTS

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

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

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

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

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

18. PERSONNEL ASSIGNMENTS

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

(b) The Contractor certifies that the Contractor, and each Subcontractor, have established a criminal history background policy that complies with guidance issued by the U.S. Equal Employment Opportunity Commission and that the Contractor and each Subcontractor conducts criminal history checks on its assigned personnel in accordance with such policy to identify, hire and assign personnel to work on this Contract whose criminal backgrounds are appropriate for the Services being performed, considering the risk and liability to the Contractor and the Authority. The Authority reserves the right to require the Contractor and any Subcontractor to disclose any criminal or military criminal convictions of assigned personnel and the right to disapprove the use of assigned personnel with criminal or military convictions.

(c) At the commencement of the Contract, the Contractor shall provide a list of candidates to be used to provide the Services and shall certify that a criminal history background check has been completed on each candidate within the preceding 6-month period Thereafter during the Term, the Contractor shall submit quarterly report containing a list of all persons (including Subcontractors) assigned to perform Services under the Contract and a certification that each named person has undergone a criminal background check as required by this Contract. The Authority shall have the right to audit the Contractor's records for compliance with the provisions of this Section. Criminal background checks shall include the following:

(1) State Criminal History: The Contractor shall research criminal history, including driving records (where applicable), covering all jurisdictions within the state, including local counties and municipalities.

(2) Out of State Criminal History: The Contractor shall research criminal history, including state driving records (where applicable), for all 50 states.

(3) National Sex Offender Registry

(4) Military Discharge: For any candidates that have served in the military, the Contractor shall review the DD Form 214 "Certificate of Release or Discharge from Active Duty" (Long Form).

*Matters identified on the Long Form as military discipline will be considered in accordance with the corresponding crime listed below with respect to classification, severity and time elapsed.

The Contractor shall disclose to the Authority the type of arrests with pending dispositions and convictions for crimes according to the classification of offense and the timetable below:

Offense Type	**Action Required**
Crimes Against the Person (other than sex crimes)	
Felony	Submit to Capital Metro for review if less than 10 years from date of **release from confinement**
Class A or B Misdemeanor	Submit to Capital Metro for review if less than 7 years from date of **conviction**
Class C Misdemeanor	Submit to Capital Metro for review if less than 5 years from date of **conviction**
Crimes Against the Person - Sex Crimes/Registered Sex Offenders	
ALL	Submit to Capital Metro for review
Crimes Against Property	
Felony	Submit to Capital Metro for review if less than 10 years from date of **release from confinement**
Moral Crimes, including, but not limited to: Drug Crimes, Prostitution, Bigamy, Illegal Gambling, Child Pornography	
Felony	Submit to Capital Metro for review if less than 10 years from date of **release from confinement**
Class A or B Misdemeanor	Submit to Capital Metro for review if less than 7 years from date of **conviction**
Class C Misdemeanor	Submit to Capital Metro for review if less than 5 years from date of **conviction**
Driving Offenses	
Class A or B Misdemeanor, DWI/DUI or other "serious driving offense"	Disqualified if less than 7 years from date of conviction or deferred adjudication. Submit to Capital Metro for review if between 7-10 years since conviction or deferred adjudication or more than 2 convictions in a lifetime

Class C Misdemeanor Moving Violations	Disqualified from driving if more than 2 moving violations in the past 5 years (Any more than one driving safety course taken for a moving violation that appears on a five (5) year record will be treated as a moving violation and will count against the employee)

The Contractor may not assign an employee to provide Services if the employee has any conviction in the applicable categories listed above, unless an exception is granted by the Authority in accordance with subparagraph (d).

(d) The Contractor may request the Authority perform an individual assessment of a candidate with a criminal conviction meeting one of the above categories. In conducting an individual assessment, the Authority's review will include, but not be limited to, the following factors:

(1) The nature and gravity of the offense or conduct;

(2) The degree of harm caused by the offense or conduct;

(3) The time that has elapsed since the conviction or completion of probation or jail time;

(4) The nature of the job sought, including the job duties, environment and level of supervision;

(5) Any incorrect criminal history;

(6) Wrongful identification of the person;

(7) The facts and circumstances surrounding the offense or conduct;

(8) The number of offenses for which the candidate was convicted;

(9) The subsequent conviction for another relevant offense;

(10) The age of the person at the time of conviction or completion of probation or jail time;

(11) Evidence that the person performed the same type of work, post-conviction, with the same or different employer, with no known incidents of criminal conduct;

(12) The length and consistency of employment history before and after the conviction in a similar field as the current position sought;

(13) Rehabilitation efforts, e.g., education, treatment, training;

(14) Employment or character references and any other information regarding fitness for the particular position;

(15) Whether the person is bonded or licensed under any federal, state or local program or any licensing authority;

(16) The person's statement of the circumstances surrounding the offense and conviction and relevant factors is consistent with publicly available record related to the crime and conviction; and

(17) Any other factors deemed relevant in the consideration of a particular assessment.

At the time a request is made for an individual assessment, the Contractor must include the following documentation:

- the candidate's application/resume;
- a copy of the criminal conviction history, including those tried in a military tribunal;

- available court information related to the conviction;
- any publicly available information related to the offense and conviction;
- a statement from the candidate addressing any/all factors set forth above and explaining why the person is qualified for the assignment notwithstanding the conviction; and
- a statement from the candidate explaining why the person is an acceptable risk for the work to be performed by the candidate.

The Authority will provide a written decision to the Contractor within five (5) working days of receipt of all required documentation from the Contractor.

(e) The Contractor will conduct new criminal history background checks on all assigned personnel every two (2) years during the Contract to ensure the preceding criterion are still met by the assigned personnel and notify the Authority if an employee has a subsequent arrest with pending disposition or conviction (or change in driving record, as applicable) that requires further review by the Authority using the criterion set forth above. The Authority reserves the right to request that the assigned individual be removed from performing work under this Contract.

19. BADGES AND ACCESS CONTROL DEVICES

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

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

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

20. CHANGES

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

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

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

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

(e) If any change under this paragraph causes an increase or decrease in the Contractor's cost of, or the time required for, the performance of any part of the Services under this Contract, whether or not changed by any such order, the Contracting Officer may make an equitable adjustment and modify the Contract in writing in accordance with the provisions in paragraph entitled “Equitable Adjustments” contained in Exhibit E.

21. TERMINATION FOR DEFAULT

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

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

(2) if the Contractor 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.

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

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

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

(e) 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.

22. 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 written notice of the termination to the Contractor specifying the part of the Contract terminated and when termination becomes effective.

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

(c) The Authority may require the Contractor to transfer title and deliver to the Authority in the manner and to the extent directed by the Authority: (1) any completed supplies; and (2) such partially completed supplies and materials, parts, tools, dies, jigs, fixtures, plans, drawings, information and contract rights (hereinafter called "Manufacturing Materials") as the Contractor has specifically produced or specially acquired for the performance of the terminated part of this Contract. The Contractor shall, upon direction of the Authority, protect and preserve property in the possession of the Contractor in which the Authority has an interest. If the Authority does not exercise this right, the Contractor shall use its best efforts to sell such supplies and Manufacturing Materials.

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

(1) Contract prices for supplies accepted under the Contract;

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

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

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

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

23. 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.

~~24. INTELLECTUAL PROPERTY PROVISIONS~~

~~(a) As between the Contractor and the Authority, the Works and Intellectual Property Rights therein are and shall be owned exclusively by Capital Metro, and not the Contractor. The Contractor specifically agrees that all Works shall be considered "works made for hire" and that the Works shall, upon creation, be owned exclusively by the Authority. To the extent that the Works, under applicable law, may not be considered works made for hire, the Contractor hereby agrees that this Contract effectively transfers, grants, conveys, assigns, and relinquishes exclusively to the Authority all right, title and interest in and to all worldwide ownership rights in the Works, and all Intellectual Property Rights in the Works, without the necessity of any further consideration, and the Authority shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Works.~~

~~(b) The Contractor, upon request and without further consideration, shall perform any acts that may be deemed necessary or desirable by the Authority to evidence more fully the transfer of ownership of all Works to the Authority to the fullest extent possible, including but not limited to the execution, acknowledgement and delivery of such further documents in a form determined by the Authority. In the event the Authority shall be unable for any reason to obtain the Contractor's signature on any document necessary for any purpose set forth in the foregoing sentence, the Contractor hereby irrevocably designates and appoints the Authority and its duly authorized officers and agents as the Contractor's agent and the Contractor's attorney-in-fact to act for and in the Contractor's behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by the Contractor.~~

~~(c) To the extent that any pre-existing rights and/or third party rights or limitations are embodied, contained, reserved or reflected in the Works, the Contractor shall either:~~

~~(1) grant to the Authority the irrevocable, perpetual, non-exclusive, worldwide, royalty-free right and license to:~~

~~(i) use, execute, reproduce, display, perform, distribute copies of, and prepare derivative works based upon such pre-existing rights and any derivative works thereof in connection with the sale, offering for sale, marketing, advertising, and promotion of the Authority's goods and services, and in all forms of media, media channels and/or publicity that may now exist or hereafter be created or developed, including but not limited to television, radio, print, Internet, and social media (e.g., Facebook, Twitter, YouTube, etc.) and~~

~~(ii) authorize others to do any or all of the foregoing, or~~

~~(2) where the obtaining of worldwide rights is not reasonably practical or feasible, provide written notice to the Authority of such pre-existing or third party rights or limitations, request the Authority's approval of such pre-existing or third party rights, obtain a limited right and license to use such pre-existing or third party rights on such terms as may be reasonably negotiated, and obtain the Authority's written approval of such pre-existing or third party rights and the limited use of same. The Contractor shall provide the Authority with documentation indicating a third party's written approval for the Contractor to use any pre-existing or third party rights that may be embodied, contained, reserved or reflected in the Works.~~ ~~**THE CONTRACTOR SHALL INDEMNIFY, DEFEND AND HOLD THE AUTHORITY HARMLESS FROM AND AGAINST ANY AND ALL CLAIMS, DEMANDS, REGULATORY PROCEEDINGS AND/OR CAUSES OF ACTION, AND ALL LOSSES, DAMAGES, AND COSTS (INCLUDING ATTORNEYS' FEES AND SETTLEMENT COSTS) ARISING FROM OR RELATING TO, DIRECTLY OR INDIRECTLY,**~~

~~**ANY CLAIM OR ASSERTION BY ANY THIRD PARTY THAT THE WORKS INFRINGE ANY THIRD-PARTY RIGHTS.** The foregoing indemnity obligation shall not apply to instances in which the Authority either:~~

~~(i) exceeded the scope of the limited license that was previously obtained by the Contractor and agreed to by the Authority, or~~

~~(ii) obtained information or materials, independent of the Contractor's involvement or creation, and provided such information or materials to the Contractor for inclusion in the Works, and such information or materials were included by the Contractor, in an unaltered and unmodified fashion, in the Works.~~

~~(d) The Contractor hereby warrants and represents to the Authority that individuals or characters appearing or depicted in any advertisement, marketing, promotion, publicity or media, of any type or form that may now exist or hereafter be created or developed by or on behalf of the Contractor for the use by or benefit of the Authority, have provided their written consent for the use, reproduction, display, performance, and distribution of, and/or preparation of derivative works to, their persona or personality rights, including name, biographical information, picture, portrait, likeness, performance, voice and/or identity ("Personality Rights"), and have been compensated for such Personality Rights, if appropriate. If such permission has been obtained for a limited time, the Contractor shall be responsible for any costs associated with claims resulting from such use, etc., of the Personality Rights after the expiration of those time limits**. THE CONTRACTOR AGREES TO DEFEND, INDEMNIFY AND HOLD THE AUTHORITY HARMLESS FROM ANY CLAIMS, INCLUDING BUT NOT LIMITED TO CLAIMS FOR INVASION OF PRIVACY, INFRINGEMENT OF THE RIGHT OF PUBLICITY, LIBEL, UNFAIR COMPETITION, FALSE ADVERTISING, INTENTIONAL OR NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS, COPYRIGHT OR TRADEMARK INFRINGEMENT, AND/OR CLAIMS FOR ATTORNEY'S FEES, RESULTING FROM SUCH USE, ETC., OF THE PERSONALITY RIGHTS.**~~

~~(e) The Contractor hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Works which the Contractor may now have or which may accrue to the Contractor's benefit under U.S. or foreign copyright laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. The term "Moral Rights" shall mean any and all rights of paternity or integrity of the Works and the right to object to any modification, translation or use of the Works, and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a Moral Right.~~

~~(f) The Contract is intended to protect the Authority's proprietary rights pertaining to the Works, and the Intellectual Property Rights therein, and any misuse of such rights would cause substantial and irreparable harm to the Authority's business. Therefore, the Contractor acknowledges and stipulates that a court of competent jurisdiction should immediately enjoin any material breach of the intellectual property and confidentiality provisions of this Contract, upon a request by the Authority, without requiring proof of irreparable injury as same should be presumed.~~

~~(g) Upon the request of the Authority, but in any event upon termination of this Contract, the Contractor shall surrender to the Authority all documents and things pertaining to the Works, including but not limited to drafts, memoranda, notes, records, drawings, manuals, computer software, reports, data, and all other documents or materials (and copies of same) generated or developed by the Contractor or furnished by the Authority to the Contractor, including all materials embodying the Works, any Authority confidential information, or Intellectual Property Rights, regardless of whether complete or incomplete. This paragraph is intended to apply to all Works made or compiled by the Contractor, as well as to all documents and things furnished to the Contractor by the Authority or by anyone else that pertains to the Works.~~

25. 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.

26. INSPECTIONS AND APPROVALS

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

(b) The Contractor shall provide and maintain an inspection system acceptable to the Authority covering the Services under this Contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the Authority during Contract performance and for as long afterwards and the Contract requires.

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

(d) If any of the Services do not conform with Contract requirements, 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.

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

27. <u>SUSPENSION OF SERVICES</u>

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

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

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

28. <u>PAYMENT TO SUBCONTRACTORS</u>

(a) Payments by contractors to subcontractors associated with Authority contracts are subject to the time periods established in the Texas Prompt Payment Act, Tex. Gov’t Code § 2251.

(b) A false certification to the Authority under the provisions of the paragraph entitled "Invoicing and Payment" hereof may be a criminal offense in violation of Tex. Penal Code § 10.

29. 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.

30. 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.

31. 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.

32. 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.

33. PUBLICATIONS

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

34. REQUEST FOR INFORMATION

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

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

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

35. 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.

(b) All documents, reports, data, graphics and other materials produced under this Contract shall become the sole possession of the Authority upon receipt and payment, subject only to the Contractor's professional obligation to maintain copies of its work product.

36. LIMITATION OF LIABILITY

In no event shall the Authority or its officers, directors, agents or employees be liable in contract or tort, to the Contractor or its Subcontractors for special, indirect, incidental or consequential damages, resulting from the Authority's performance, nonperformance, or delay in performance of its obligations under this Contract, or the Authority's termination of the Contract with or without cause, or the Authority's suspension of the Services. This limitation of liability shall not apply to intentional tort or fraud. The Contractor shall include similar liability provisions in all its Subcontracts.

37. 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.

38. CLAIMS

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

39. 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.

40. 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.

41. PUBLICITY RELEASES

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

42. 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.

43. INDEMNIFICATION

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

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

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

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

(4) ANY ACT OR OMISSION OF THE CONTRACTOR OR ANY OF ITS SUBCONTRACTORS OR ANY

OF THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, CUSTOMERS, INVITEES, REPRESENTATIVES OR VENDORS.

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

(c) "DAMAGES" MEANS ALL DIRECT OR INDIRECT DAMAGES, LOSSES, LIABILITIES, DEFICIENCIES, SETTLEMENTS, CLAIMS, AWARDS, INTEREST, PENALTIES, JUDGMENTS, FINES, OR OTHER COSTS OR EXPENSES OF ANY KIND OR NATURE WHATSOEVER, WHETHER KNOWN OR UNKNOWN, CONTINGENT OR VESTED, MATURED OR UNMATURED, AND WHETHER OR NOT RESULTING FROM THIRD-PARTY CLAIMS, INCLUDING COSTS (INCLUDING, WITHOUT LIMITATION, REASONABLE FEES AND EXPENSES OF ATTORNEYS, OTHER PROFESSIONAL ADVISORS AND EXPERT WITNESSES) RELATED TO ANY INVESTIGATION, ACTION, SUIT, ARBITRATION, APPEAL, CLAIM, DEMAND, INQUIRY, COMPLAINT, MEDIATION, INVESTIGATION OR SIMILAR EVENT, OCCURRENCE OR PROCEEDING.

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

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

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

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

44. RECORD RETENTION; ACCESS TO RECORDS AND REPORTS

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

(b) If this is a cost-reimbursement, incentive, time and materials, labor hour, or price determinable Contract, or any combination thereof, the Contractor shall maintain, and the Authority and its representatives shall have the right to examine, all books, records, documents, and other evidence and accounting procedures and practices sufficient to reflect properly all direct and indirect costs of whatever nature claimed to have been incurred and anticipated to be incurred for the performance of this Contract.

(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 three (3) years after the date of termination or expiration of this Contract, except in the event of litigation or settlement of claims arising from the performance of this Contract, in which case records shall be maintained until the disposition of all such litigation, appeals, claims or exceptions related thereto.

(e) The Contractor agrees to provide sufficient access to the Authority and its contractors to inspect and audit records and information related to performance of this Contract as reasonably may be required.

(f) The Contractor agrees to permit the Authority and its contractors access to the sites of performance under this Contract as reasonably may be required.

(g) 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.

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

45. EXCUSABLE DELAYS

(a) Except for defaults of Subcontractors at any tier, the Contractor shall not be in default because of any failure to perform this Contract under its terms if the failure arises from Force Majeure Events. In each instance, the failure to perform must be beyond the control and without the fault or negligence of the Contractor. "Default" includes failure to make progress in the performance of the Services.

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

(1) the subcontracted supplies or services were obtainable from other sources;

(2) the Authority ordered the Contractor in writing to obtain these services from the other source; and

(3) the Contractor failed to comply reasonably with this order.

(c) Upon the request of the Contractor, the Authority shall ascertain the facts and extent of the failure. If the Authority determines that any failure to perform results from one or more of the causes above, the delivery schedule or period of performance shall be revised, subject to the rights of the Authority under this Contract.

46. LOSS OR DAMAGE TO PROPERTY

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

47. CONTRACTOR CONTACT/AUTHORITY DESIGNEE

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

48. QUALITY ASSURANCE

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

49. INTERPRETATION OF CONTRACT – DISPUTES

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

50. 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 Capital Metro 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 Capital Metro owned or leased property, including personal vehicles parked in Capital Metro parking lots.

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

51. ORDER OF PRECEDENCE

In the event of any inconsistency between the provisions of this Contract, the inconsistency shall be resolved by giving precedence in the following order:

1. Exhibit A – Pricing Schedule
2. Exhibit A-1 – Pricing Supplement
3. Exhibit E – Contractual Terms and Conditions
4. Exhibit F – Scope of Services and Compliance Matrix
5. Exhibit B – Representations and Certifications
6. Other provisions or attachments to the Contract

52. 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.

53. ACCESS REQUIREMENTS TO INDIVIDUALS WITH DISABILITIES

The Contractor shall comply with all applicable requirements of the Americans with Disabilities Act of 1990 (ADA), 42 U.S.C. 12101 et seq. and 49 U.S.C. § 322; Section 504 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794; Section 16 of the Federal Transit Act, as amended, 49 U.S.C. app. 1612; and the following regulations and any amendments thereto:

(a) U.S. DOT regulations, "Transportation Services for Individuals with Disabilities (ADA)," 49 C.F.R. Part 37;

(b) U.S. DOT regulations, "Nondiscrimination on the Basis of Handicap in Programs and Activities Rece3iving or Benefiting from Federal Financial Assistance," 49 C.F.R. Part 27;

(c) U.S. DOT regulations, "Americans With Disabilities (ADA) Accessibility Specifications for Transportation Vehicles," 49 C.F.R. Part 39;

(d) Department of Justice (DOJ) regulations, "Nondiscrimination on the Basis of Disability in State and Local Government Services," 28 C.F.R. Part 36;

(e) DOJ Regulations, "Nondiscrimination on the Basis of Disability by Public Accommodations and in Commercial Facilities," 28 C.F.R. Part 36;

(f) General Services Administration regulations, "Construction and Alteration of Public Buildings," "Accommodations for the Physically Handicapped," 41 C.F.R. Parts 101-10;

(g) Equal Employment Opportunity Commission (EEOC) "Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act," 29 C.F.R. Part 1630;

(h) Federal Communications Commission regulations, "Telecommunications Relay Services and Related Customer Premises Equipment for the Hearing and Speech Disabled," 47 C.F.R. Part 64, Subpart F; and

(i) FTA regulations, "Transportation for Elderly and Handicapped Persons", 49 C.F.R. Part 609.

54. ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

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

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

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

55. MISCELLANEOUS

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

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

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

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

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

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

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

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

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

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

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

(i) The Contractor shall not assign the whole or any part of this Contract or any monies due hereunder without the prior written consent of the Contracting Officer. No assignment shall relieve the Contractor from any of its obligations hereunder. Any attempted assignment, transfer or other conveyance in violation of the foregoing shall be null and void.

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

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

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

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

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

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

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

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

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

56. FUNDING AVAILABILITY

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

57. PERFORMANCE MANAGEMENT DISINCENTIVES

Severity Level	Acknowledgement Time	Target Workaround Time	Target Resolution Time	Disincentive Assessed

1 -Blocker	15 minutes	6 hours	24 hours	$500/event / $1000 per 24- hour day it remains out of service.
2 - Major	15 minutes	12 hours	Current Planned release	$250 per event / $500 per 24-hour day it remains out of service.
3 - Medium	1 hour	5 business days	Scheduled as part of next release	$100 per event / $200 per 24-hour day it remains out of service.
4 - Minor	2 hours	N/A	Incorporated into future release	N/A

*The disincentive assessed per an event is defined as every reported incident that exceeds the target resolution time. An additional assessment is issued for every 24-hour day that passes from when the incident was reported.

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

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

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

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

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

Severity Level Definitions	Issues Impacting System
1 – Blocker*	*End Users cannot use or purchase fare media *Issue preventing validation of active fare media *Inability for End Users to plan a trip from A to B using a scheduled time *Significant percentage (more than 10%) of End Users are affected (e.g. cannot use or purchase fare media) *The financial impact of the incident is likely to be high (greater than $10,000) *The damage to the reputation of the business is likely to be high
2 – Major	*End Users cannot create an account or login *Trip planning tools no longer provide real time information *Ability to lookup End Users *Current product configuration issues *Prevents Client User from recording fare evasion citations *Prevents Client User from distributing inventory to partner organization. *The financial impact of the incident is likely to be high (more than $1,000 but not greater than $10,000) *The damage to the reputation of the business is likely to be moderate
3 - Medium	*Ticket activation and purchasing issues affecting minority percentage of End Users. *Financial reporting inaccuracies *Client User unable to issue refunds *Errors – incorrect billing and settlement *Client or End User App settings screen issues *Future schedule inaccuracies or errors *Prevents Client User from creating and managing notifications *Prevents Client User from creating and listing orders *Prevents Client User from modifying End User details *Prevents Client User from managing and creating products *Prevents Client User from managing and creating campaigns *Prevents Client User from Client User App features *Prevents Client User from managing partner organization related features *Prevents Client User accessing stock reports *Reporting inaccuracies *Existing data export process fails to execute *Device management and monitoring issues *Clients account user management *Impacts third-party access of Contractor systems

4 - Minor	*Value add functions are not accessible or result in errors *Cosmetic defects *Feature functions but fails on data variation *Multi/intermodal third-party API's or errors *Statistic tool *Backend Error Messages: GTFS upload information tool *Real Time cockpit

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

58. DATA PRIVACY

The Contractor may have access to personally identifiable information ("PII") in connection with the performance of the Agreement. PII is 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 cus-tomers. The Contractor shall take reasonable steps maintain the confidentiality, security, safety, and integrity of all Customer PII, Notwithstanding the above, the Parties hereby expressly acknowledge and agree that Contrac-tor shall not be responsible for any security for the transmission of data over the internet, payment processing or credit or debit card transactions or the data security or data privacy associated with the services of third-party vendors performing payment processing, hosting, or cloud vendor services. Notwithstanding the foregoing, Con-tractor will adhere to the following requirements concerning Customer PII:

(a) The Contractor shall take reasonable steps to maintain the confidentiality of and will not reveal or divulge to any person or entity any Customer PII that becomes known to it during the term of this Agreement.

(b) The Contractor must maintain policies and programs that prohibit unauthorized disclosure of Customer PII by its employees and sub-Contractors and promote training and awareness of information security policies and practices. The Contractor must comply, and must cause its employees, representatives, agents, and sub-Contractors to comply, with such commercially and operationally reasonable directions as the Authority may make to promote the safeguarding or confidentiality of Customer PII.

(c) The Contractor must conduct background checks for employees or sub-Contractors that have access to Customer PII or systems hosting Customer PII.

(d) The Contractor must limit access to computers and networks that host Customer PII, including without limitation through user credentials and strong passwords, data encryption both during transmission and at rest, fire-wall rules, and network-based intrusion detection systems.

(e) This Section will survive termination or expiration of this Agreement.

59. DATA SECURITY

Contractor shall take reasonable steps to maintain the confidentiality, security, safety, and integrity of the Authority's data. Notwithstanding the above, the Parties hereby expressly acknowledge and agree that Contractor shall not be responsible for any security for the transmission of data over the internet, payment processing or credit or debit card transactions or the data security or data privacy associated with the services of third-party vendors performing payment processing, hosting, or cloud vendor services. This section will survive the termination of this Agreement.

Instructions:
1. For each Compliance Term, select "C-Comply," "N-Cannot Comply," or "A-Will Comply with Alternative." If "N" or "A" are selected, comments are required, however Capital Metro strongly recommends that comments be added for each item.
2. Bytemark must deliver a system encompassing all hardware, software, license, and service requirements including delivery of third-party products to make the solution fully functional.
3. The requirements in the Scope of Services and Compliance Matrix are functional in nature and do not encompass all requirements. Bytemark shall determine, through the Plan and Design phases, the technical modifications needed to carry out the intent herein. Bytemark shall document and discuss said needs with Capital Metro and implement the agreed-upon solution accordingly.
4. Bytemark must deliver all Compliance Terms unless it is within a section marked "Optional" that is not exercised by Capital Metro or Capital Metro agrees to an alternative.
5. The column entitled "Release" shall be used to indicate the product release number when the requirement will be delivered.
6. 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 corresponds with each line.
7. The Project and Project Schedule shall use the Enterprise Project and Portfolio Phase Tasks and Deliverables shown on Appendix A - EPPM Phases.
8. Answer all questions in Appendix B1 & B2

1.0	**Overview**
1.1	Introduction. The Capital Metropolitan Transportation Authority (“Capital Metro”) is requesting a proposal from Bytemark, Inc. for services to upgrade their existing customer account based fare system from smart phone validation to account validation thereby enabling additional fare programs and features along with the ability to have application program interfaces (APIs) to allow for integration and build a customer experience that limits the time / creates physical separation during the onboard fare collection process. This initiative is an upgrade of the existing Bytemark mobile ticketing system installed on Capital Metro's vehicles. Bytemark shall upgrade or replace all hardware, software, licenses and services to fully configure, integrate, and rollout to Capital Metro, the proposed Solution within Capital Metro's environment. Bytemark shall coordinate and subcontract as necessary with all vendors and subcontractors required for the architecture, configuration, testing, and acceptance of the integrated components required to achieve the required functionality.
1.2	Fare Strategy Vision. Capital Metro seeks to upgrade its existing mobile ticketing fare equipment/systems and implement an account-based, multimodal fare collection system ("System") using open architecture that is flexible and scalable to support growth and business changes, and capable of accepting a variety of payments, bringing Capital Metro and the region into the next generation of fare payment technology and offerings. The system shall be simple to use, convenient for the customer, and cost-effective to maintain. The upgrade will meet Capital Metro's Fare Strategy by providing the following prime objectives: •Fast and Easy payment options •Equity in payment options •Retail network with reloadable smart cards and virtual account •Account-based system integrated to all fare systems to increase fare options and programs •Faster boarding •Simplify fares to increase adoption and build ridership •Accept payment in as many forms as possible •Simple and straightforward operation so that Capital Metro can troubleshoot customer problems •Open APIs for integration with other systems (e.g. third-party bike sharing, ride sharing, mobility as a service, and parking)
1.3	These are targeted dates. Please confirm your ability to meet or provide alternative timelines. Projected go-live and project completion dates: Estimated Notice of Award (NOA) / Notice to Proceed (NTP): July 21, 2020 / July 31, 2020 Release 1 (Product Based Fare Capping): 2 Months from NTP Release 2 (Transit Account Upgrade): 10 months from NTP Release 3 (Validator Upgrade): 12 months from NTP Release 4 (Open Payments): 14 months from NTP Project Completion: December 31, 2021
1.4	Please note that the following needs to be included in your proposal: - Design, Development and Release Schedule - Technical Approach - Installation Plan - Project staff - a detail of staff hours including subcontractors dedicated to this project, with position title and resume.

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
2.1	**Project Approach - Project Management**					
2.1-1	Bytemark shall provide a robust project management team and project management plan to support upgrade of the System. Bytemark's plan for managing the project shall clearly demonstrate an appropriate allocation of project management resources that have the ability and experience to ensure that system design and implementation will be properly coordinated and managed, and will be completed on schedule and within budget. Bytemark shall provide tools to manage tasks, schedule, risk, change, and the other items listed in this section that are required to manage the project.					
2.1-2	EPPM Phase Tasks and Deliverables, Project Management and Payment Milestones. The Contractor shall comply with all requirements of "Appendix A - EPPM Phases" which define deliverables within phases, project management requirements, and payment milestones for the project.					
2.1.1	**Project Approach - Project Management Plan**					
2.1.1-1	Bytemark shall submit a comprehensive Project Management Plan (PMP) within 2-weeks following Notice to Proceed (NTP) that details at a minimum project organization; master schedule; and how project scope, cost, risk, quality, project changes, safety, and other key aspects of the project will be managed by Bytemark.					
2.1.1-2	The project Management Plan (PMP) will include but is not limited to the following elements: • Organization chart identifying key project personnel and contact information. • Master schedule, identifying key project milestones and activities in Microsoft Projects format. • Schedule for all project design and development elements that require Capital Metro approval. • Project meetings and schedule for recurring meetings. • Methodology to control project schedule, scope, cost, and risk. • Risk management plan and risk register, including identified project risks and actions required to mitigate them. • Transition and change management processes and procedures. • Safety processes and procedures. • Quality assurance processes and procedures to confirm that the requirements of the contract are being met. • Subcontractor management and communications. • Document naming conventions and Action Items and Issues List (AIL) control processes and procedures, including version and traceability controls. • Change management plan and procedures for all deliverables and subsequent revisions. • Cost management. • Communication Plan.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
2.1.2	**Project Approach - Project Management: Design Review**					
2.1.2-1	Bytemark shall provide a robust project management team and project management plan to support the upgrade of the System. Bytemark's plan for managing the project shall clearly demonstrate an appropriate allocation of project management resources that have the ability and experience to ensure that system design and implementation will be properly coordinated and managed, and will be completed on schedule and within budget. Bytemark shall provide tools to manage tasks, schedule, risk, change, and the other items listed in this section that are required to manage the project.					
2.1.2-2	The objectives of the Preliminary Design Review (PDR) are to review progress of the System design and evaluate compliance with the requirements of this Statement of Services (SOS). PDR will represent approximately 75% completion of the total technical and operational system design. At PDR, Capital Metro needs Bytemark to demonstrate programmatic adequacy of design in meeting the requirements in this SOS. Bytemark is encouraged to categorize PDR information into logical topics for organized review and discussion.					
2.1.2-3	The objective of Final Design Review (FDR) is to finalize the detailed system design that satisfies all of the requirements in this SOS. FDR will represent 100% completion of the detailed system design with production specifications and drawings ready for release.					
2.1.2-4	Bytemark will perform third-party user functionality, user experience, and user accessibility testing as part of the design phase using prototype designs from the PDR and/or FDR. The third-party testing organization shall be approved by Capital Metro. Testing will be conducted in a lab with Capital Metro customers and non-customers for each of the products in each of the phases. Findings from the testing shall be reviewed with the third-party test provider, Capital Metro, and Bytemark to be incorporated into the design.					
2.2	**Project Approach - Installation & Transition Plans**					
2.2-1	Bytemark shall provide a detailed Installation and Transition Plan for Capital Metro review and approval at FDR, and a final version no later than 60 calendar days after notice to proceed for all releases prior to the first delivery of equipment.					
2.2-2	The Installation and Transition Plan will describe detailed installation and configuration of all software systems, including the back office, systems, interfaces and web applications, and their respective schedules.					
2.2.-3	Bytemark shall provide a detailed Upgrade Migration Plan which will detail how riders and accounts will be migrated for each phase of the project. The Plan will be reviewed during design review and updated as needed throughout the project.					
2.2-3	Bytemark shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
2.3	**Project Approach - Testing: General Requirements**					
2.3-1	Bytemark shall provide all labor and materials required for system testing, including but not limited to closed-loop fare media and bank cards, and all support services and facilities required to stage, inspect and test all hardware and software being supplied.					
2.3-2	Prior to the start of all formal testing activities that are to be witnessed and approved by Capital Metro, Bytemark shall conduct “dry-run” testing to identify and resolve any issues and avoid unexpected results during the formal testing.					
2.3-3	Bytemark shall provide Capital Metro with scripts to test all API endpoints.					
2.3-4	Bytemark shall test and verify that they can successfully utilize Capital Metro-provided and local cellular communications networks for deployment of the system as designed.					
2.3.1	**Project Approach - Testing: Test Documentation**					
2.3.1-1	Bytemark shall submit a draft inspection and test plan for Capital Metro review and approval during design review, and shall submit a final inspection and test plan to be used in connection with all inspections and tests described in this specification no less than 60 calendar days prior to the start of any testing.					
2.3.1-2	The Test Plan will include volume or stress testing for applicable devices and systems that simulates 200% of the projected peak ridership and transaction volumes in the year 2025 in Appendix C Ridership Figures. Bytemark shall detail the transaction volumes and how they will be generated in the test plan(s).					
2.3.1-3	Detailed test procedures will include mapping to the design documents and the requirements in the SOS that are related to the test.					
2.3.2	**Project Approach - Testing: Capital Metro Test Facility**					
2.3.2-1	Bytemark shall upgrade the test facility on Capital Metro property for both Bytemark and Capital Metro use. Capital Metro test facility shall be upgraded and ready for use no later than the commencement of SIT (System Integration Test).					
2.3.2-2	Beginning with SIT, all formal testing to be approved by Capital Metro prior to and following public launch of the System will be performed at Capital Metro test facility.					
2.3.2-3	Bytemark shall update Capital Metro test facility software as necessary throughout the term of the contract and software maintenance agreement to maintain a fully mirrored environment of Bytemark’s test facility.					
2.3.2-4	The test facility will be configurable to utilize one or more of the back office environments (development, test, stage, production). These back-office environments will include the account-based transaction processor and all specified support systems, which fully replicate the production environment.					
2.3.3	**Project Approach - Testing: FUT (Functional Unit Test)**					
2.3.3-1	Capital Metro shall complete functional tests for the back office applications, mobile apps, websites, and device software which demonstrate and verify all functions described in these specifications and design documents, including review of all user-accessible screens and commands.					
2.3.3-2	Successful completion of the development of back office applications, mobile apps, and website software, and installation of production equipment in Capital Metro test facility are prerequisites for the commencement of FUT.					
2.3.3-3	Bytemark will perform third-party user functionality, user experience, and user accessibility testing as part of the functional unit tests. The third-party testing organization shall be approved by Capital Metro. Testing will be conducted in a lab with Capital Metro customers and non-customers for each of the products in each of the phases. Findings from the testing shall be reviewed with the third-party test provider, Capital Metro, and Bytemark to be incorporated into the Test Failure Log for resolution.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
2.3.4	**Project Approach - Testing: SIT (System Integration Test)**					
2.3.4-1	For SIT, the test system will be provisioned with test data simulating the system's operational databases under full operational load. Full operational load will be defined in the SIT test procedure, and approved by Capital Metro prior to commencement of SIT.					
2.3.4-2	At a minimum, SIT will include: • Ten (10) days of continuous testing of all system components, during which the components will be operational 24 hours a day. • A minimum of 500 transactions at each system component type, including validators, driver displays, mobile data routers, ticket vending machines, onboard validators, customer service terminals, retail point of sale (POS)/sales terminals, mobile fare inspection devices, mobile fare validation devices, customer mobile app, testing all transaction types. • A minimum of 100 transactions each performed through the Customer Relationship Management (CRM) system, and customer and business website(s), testing all available functions. • All alarm and boundary conditions tested at a minimum of 50 times each. Specifics of SIT testing will be included in the SIT procedures to be reviewed and approved by Capital Metro.					
2.3.4-3	Bytemark shall conduct data transmission testing during SIT to demonstrate, exercise, and verify transaction processing and data uploads from all devices, and the download of configuration data to each of the various device types. Bytemark shall confirm proper data transfer rates between all devices and systems.					
2.3.4-4	SIT will include database accuracy testing, which will demonstrate the accuracy between the AUT (application under test) and the relational database in which application-generated data is stored. The testing should also demonstrate atomicity, consistency, insolation and durability of the database.					
2.3.4-5	SIT will include a full system audit and settlement test, which will demonstrate the flow of all transactions through the system with the appropriate reporting, accounting, and settlement calculations demonstrated.					
2.3.4-6	With successful completion and approval of SIT, all software and configuration files will be "frozen," and Bytemark will make no changes without Capital Metro authorization.					
2.3.4-7	The automated failover process will be exercised in multiple failover scenarios during systems integration testing to demonstrate no data loss or significant degradation in system performance. The Disaster Recovery Plan will include regular failover testing after implementation.					
2.3.5	**Project Approach - Testing: FIT (Field Integration Testing)**					
2.3.5-1	FIT is essentially a duplication of SIT in the field in which all devices, back office applications, website, mobile app(s), retail network interfaces, integrations including ticket vending machine, onboard validator, and all other aspects of the System are exercised in what will become the production environment upon successful completion of the test.					
2.3.5-2	A 30-day settling period will commence upon approval of the FIT test reports. Capital Metro may, at its sole discretion, conduct additional ad-hoc testing during the 30-day settling period. Ad-hoc testing may include limited "friendly user" testing.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
2.3.6	**Project Approach - Testing: Pilot**					
2.3.6-1	At least 90 calendar days prior to the scheduled start of the pilot, Bytemark shall submit an acceptance test plan, developed jointly with Capital Metro that includes the structure, timing, and measurement criteria for conducting and evaluating the pilot.					
2.3.6-2	The pilot will not commence until FIT has been approved, the subsequent 30-day settling period has passed, and 100% of the field equipment has been installed.					
2.3.6-3	The pilot will continue for its scheduled duration unless a critical failure or failures cause suspension of the pilot. When a critical failure has been resolved, the pilot will resume for a duration determined by Capital Metro, up to and including a full 90-day period.					
2.3.7	**Project Approach - Testing: SAT (System Acceptance Test)**					
2.3.7-1	SAT will commence upon successful completion of the pilot. SAT will be comprised of three consecutive 30-day periods in which all system components must meet or exceed all system performance requirements. The acceptance test plan will describe in detail how Bytemark will measure and report on each of the performance requirements throughout SAT.					
2.3.7-2	If the performance requirements defined in these specifications are not attained during any one of the 30-day periods, the SAT duration may be extended until all performance requirements are met during an agreed-upon duration.					
2.3.8	**Project Approach - Testing: Final System Acceptance**					
2.3.8-1	Bytemark shall submit a request for Final System Acceptance upon successful completion of SAT and the determination that all work has been completed in accordance with this Scope of Work and final design.					
2.3.8-2	Capital Metro may grant Final System Acceptance only when: • SAT has been successfully completed and approved by Capital Metro. • All system devices are delivered, installed, and operational. • All back office applications and software, including all required reports, are installed and fully functional. • The website and all mobile apps are live and fully functional. • All spare parts have been delivered. • Initial batches of fare media have been delivered and accepted by Capital Metro. • All requisite contract deliverables have been delivered to Capital Metro and accepted. • The Disaster Recovery Plan has been successfully demonstrated and approved by Capital Metro. • All required training has been provided and accepted by Capital Metro. • All required intellectual property has been delivered to Capital Metro or the escrow agent. • Final resolutions to all identified critical issues (as classified by the Test Failure Log Review Board) are fully implemented and accepted by Capital Metro. Capital Metro will issue written certification upon approval of Bytemark's request for Final System Acceptance.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
2.4	**Project Approach - Training**					
2.4-1	Bytemark shall provide a comprehensive program to educate and train personnel in all details of the System, enabling them to properly operate, service, and maintain the system and each of its components throughout its useful life.					
2.4-2	Bytemark shall develop and submit for Capital Metro review and approval a Training Plan that documents the design of the program for training personnel and each course to be delivered.					
2.4-3	The course curriculum will include instruction of personnel in at least the following broad categories using a train-the-trainer model: • Back office system administration, configuration, operations and maintenance, reporting, backup, and disaster recovery. • API use and administration. • Website administration and configuration. • Financial reporting, reconciliation, and apportionment. • Mobile apps administration. • Customer service terminal/CRM operations and maintenance. • Installation & maintenance training for equipment in accordance with installation procedures.					
2.4-4	The Training Plan will include a schedule for delivery of the training courses. The schedule will consider the sequence of training, hours of instruction, system readiness and proximity to startup, trainee availability, and venue for the training.					
2.4-5	Bytemark shall provide all necessary training materials and equipment for the delivery of each course (including Train-the-Trainer) discussed in the Training Plan. Training documentation will be separate from the operation and maintenance manuals but may reference them. Recordings of the training shall be provided by Bytemark.					
2.5	**Project Approach - Manuals**					
2.5-1	Bytemark shall provide instruction manuals that describe and illustrate in detail how to manage, operate, and maintain the System delivered under the Bytemark contract. The manuals will include detailed documentation for all equipment, systems, and software.					
2.5-2	Disaster recovery procedures will be clearly specified in sufficient detail to consider all possible scenarios. Recovery instructions will describe detailed procedures to be followed in the event that system recovery is needed. Detailed data backup and recovery procedures will be provided.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
3.1	**System Design & Architecture - Common Design Requirements and Guidelines**					
3.1-1	Bytemark shall upgrade their existing customer account based fare system (listed below including but not limited to) from smart phone validation to account validation thereby enabling additional fare programs and features; including: • Mobile Ticketing Application Base System with unlimited site licensing to support a fully functional, PCI compliant, system. • Mobile Ticketing Back Office Management System that allows Capital Metro and customers to setup options for ticketing, information on ticket sales, customer usage, customer information, and reporting. • Mobile Ticketing Customer Application that is downloadable and/or installed on customers' mobile smart device, available in both iOS and Android versions and includes ticketing and traveler tools. • Mobile Ticketing Validation Software installed on the onboard validator of buses to validate mobile tickers. • Fare Evasion Application Software that allows fare inspectors to track and manage citations. • Hand Held Validator & Mobile POS Software that allows fare inspectors to validate or sell mobile tickets. • Hand Held Validator & Mobile POS Hardware devices that allows fare inspectors to validate mobile tickets and sell paper tickets. • On-board Validator Hardware devices that allow customers to validate tickets when boarding. • Traveler Tools Software for Capital Metro to provide real-time transit service data to riders. • Business Partnership Software for external organizations to purchase bulk tickets and distribute mobile tickets. • Characteristics that currently implemented such as usability, accessibility support, Spanish language compliance.					
3.1-2	The System will be sized such that the total number of possible accounts, and total concurrent use of accounts, will at a minimum support 200 percent of the current and anticipated ridership figures for the year 2025 (as presented in Appendix C Ridership Figures) and scalable to support up to 400% of the anticipated peak processing load.					
3.1-3	Bytemark shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services					
3.1.1	**System Design & Architecture - Maintainability and Serviceability**					
3.1.1-1	Software upgrades will be centrally managed and fully tested prior to installation. The System shall be able to roll-back to previous software versions without adversely impacting operations.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
3.1.2	**System Design & Architecture - Licensing and Ownership**					
3.1.2-1	Capital Metro shall continue to own all data that is generated from the System as described in Exhibit E section 23 "Intellectual Property Provisions" and Exhibit G section 1.7 "Intellectual Property Rights". In accordance with those provisions, Bytemark shall provide, under perpetual license to Capital Metro, the use of all open architecture interfaces, libraries, documents, and Intellectual Property (IP) for internal use and distribution to third-parties at no additional cost to Capital Metro. Data is easily accessible and documented with, at minimum, a data dictionary and Entity Relationship Diagram (ERD) that are kept up to date.					
3.1.2-2	All open architecture APIs, licensing, libraries, and Intellectual Property (IP), including data exchange formats and algorithms, will be provided to Capital Metro under a perpetual license to facilitate internal use and enable distribution to third-party partners who have signed a non-disclosure agreement (NDA) at no additional cost as described in Exhibit E section 23 "Intellectual Property Provisions" and Exhibit G section 1.7 "Intellectual Property Rights".					
3.1.3	**System Design & Architecture - Accessibility and ADA Compliance**					
3.1.3-1	Bytemark shall design the System to be compliant with current accessibility standards, laws, and regulations to ensure that the System meets or exceeds the Americans with Disabilities Act (ADA) and accessibility requirements of federal, Texas State and local laws and regulations under Exhibit E part 53 "Access Requirements To Individuals with Disabilities". Bytemark shall ensure compliance of all equipment and system ("System") interfaces and create an Accessibility Compliance Plan to document compliance. This plan will be used throughout design and implementation to ascertain that all accessibility and ADA requirements will be met and to track compliance.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
3.1.4	**System Design & Architecture - Code and Regulation Compliance**					
3.1.4-1	Bytemark shall design the System to be compliant with applicable standards, laws, and regulations to ensure that the System: • Presents no safety hazards for customers and Capital Metro employees. • Will withstand the rigors of the environments in which the equipment will be installed, and the public use to which it will be subjected. • Provides for the secure storage and transmittal of data. • Is designed using state-of-the-art methods to maximize quality. • Satisfies federal, state, and other requirements for ergonomics and usability. Applicable codes, laws, ordinances, statutes, standards, rules, and regulations include, but are not be limited to the list below (in 3.1.4-2). The latest revisions in effect at the time of Final System Acceptance will apply.					
3.1.4-2	• Americans with Disabilities Act (ADA) • Americans with Disabilities Act Accessibility Guidelines (ADAAG) • Advanced Encryption Standard • ANSI X9.24, Financial Services Retail Key Management • European Norm EN55022, Emissions standards for CE marking • European Norm EN55024, Immunity standards for CE marking • FCC Part 15 Class B – Radio Frequency Devices • FIPS 140-2 • IEEE 802.11 a/b/g/n standard for wireless data communications • IEEE 802.11 i standard for wireless data network security • IEEE 802.11-2016 • International Electrotechnical Commission Standard 529 (IEC529) • ISO/IEC 7810, Identification Cards – Physical Characteristics • ISO 9001 • ISO/IEC-8583 – Financial transaction card originated messages • ISO/IEC 14443 Parts 1 through 4 – Contactless Smart Card Standard • ISO/IEC 18092 / ECMA-340, Near Field Communication Interface and Protocol-1 • ISO/IEC 21481 / ECMA-352, Near Field Communication Interface and Protocol-2 • National Electrical Code (NFPA 70) • National Electrical Manufacturers Association Publication 250-2003 • National Electrical Safety Code (ANSI C2) • National Fire Protection Association (NFPA) 130 • NCITS 322-2002, American National Standard for Information Technology – Card Durability Test Methods • Occupational Safety and Health Administration (OSHA) • Payment Card Industry Data Security Standards (PCI-DSS) • Payment Card Industry Payment Application Data Security Standards (PA-DSS) • Society of Automotive Engineers SAE J1113-13 Electrostatic Discharge • Society of Automotive Engineers SAE J1455 Vibration and Shock • UL Standard 60950, “Information Technology Equipment – Safety”					
3.1.4-3	In the case of conflict between the provisions of codes, laws, ordinances, statutes, standards, rules, and regulations, the more stringent requirement will apply.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
3.1.5	**System Design & Architecture - Information Security**					
3.1.5-1	Bytemark shall upgrade the plan for the processes that will be used to resume operations in the event of a data loss due to a natural disaster or other emergency situation that puts operations at risk. The plan must describe how mission-critical functions will be resumed and how longer-term challenges created by an unexpected loss will be addressed. The Disaster Recovery (DR) plan will conform to the required service level agreement and be consistent with the Business Continuity Plan and recovery time capabilities that will be provided by Capital Metro.					
3.1.5-2	Bytemark shall propose a physical and logical architecture (e.g. virtualized servers, spare load balancers, etc.) that meets all redundancy capabilities for Capital Metro review and approval at design review.					
3.1.5-3	The System will support fraud prevention policies, including the ability to automatically identify suspect usage patterns based on sales and ridership data, and block the use of fare media, accounts, and fare products based on configurable fraud rules.					
3.1.5-4	The System will be designed to include the appropriate elements and processes to manage, monitor, and quickly address security issues, consistent with the expectations outlined above, to support the operation of Capital Metro's Information Security Management System (ISMS).					
3.1.5-5	In accordance with Exhibit E section 59 “Data Security”, Exhibit G section 11 “Data Security”, all fare payment data will be secured and private from the point when it is captured to when it is received by the processor and when communications are over public networks, approved secure methods will be used.					
3.1.5-6	In accordance with Exhibit E section 58 “Data Privacy”, Exhibit G section 10 “Data Privacy”, physical and logical access to components that contain Personally Identifiable Information (PII) and/or financial data will be restricted. Physical and logical security will comply with the Payment Card Industry (PCI) standards in effect at the time of Final System Acceptance.					
3.1.5-7	In accordance with Mobile Maintenance & Services Contract (200473), Exhibit J Warranty Maintenance, and Services Agreement section, 11 "Payment Card Industry Data Security Standards ("PCI DSS") Compliance", Bytemark shall be responsible for providing a PCI compliance plan during design review, and for obtaining certification for the entire system. Bytemark shall employ a certified Qualified Security Assessor (QSA), and be responsible for conducting all testing required to achieve certification prior to Final System Acceptance.					
3.1.5-8	In accordance with Mobile Maintenance & Services Contract (200473), Exhibit J Warranty Maintenance, and Services Agreement, section 11 "Payment Card Industry Data Security Standards ("PCI DSS") Compliance", Bytemark shall be responsible for proving that the System as delivered is compliant with all applicable PCI standards at the time of Final System Acceptance, and with all Capital Metro, state, and local policies for the handling of PII.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
3.1.5-9	Bytemark shall ensure that Capital Metro data is isolated from any other customer data. Additionally, production and non-production data shall be separated. Production data shall not be used in the test environment. Production data shall be isolated from Bytemark corporate user environment.					
3.1.5-10	Bytemark shall prioritize identified application vulnerability/bug fixes. Security fixes must have higher priority than product enhancements.					
3.1.5-11	Customer sensitive data such as passwords and credit card numbers shall be encrypted at rest and in transit.					
3.1.5-12	Key Management - Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage and data in transmission as per applicable legal, statutory, and regulatory compliance obligations.					
3.1.5-13	Bytemark shall provide secure coding training for developers. Provide CapMetro with a description of the Bytemark training program for developers, specifically around secure code development practices					
3.1.5-14	Code review - Bytemark shall provide an overview of their software development lifecycle showing how security is a part of the lifecycle. Specify security tests, how you determine if your code is vulnerable to the common threats facing applications today, such as cross-site scripting or SQL injection, in your quality assurance testing phase. Describe how the contractor track security flaws and flaw resolution.					
3.1.5-15	Application security testing – Bytemark shall provide an overview of their application testing including annual pen testing, testing by 3rd party, testing by security professional services, and testing that covers the common vulnerabilities as described by OWASP Top 10. Describe the process for vulnerabilities identified and remediations.					
3.1.5-16	Bytemark shall provide CapMetro with their method of detecting customer account compromises and related remediation processes.					
3.1.5-17	Bytemark shall provide an opt-in 2Factor authentication solution for all customer accounts.					
3.2	**System Design & Architecture - System Architecture**					
3.2-1	The System will be upgraded to a full account-based system built on a central back office designed and implemented by Bytemark that manages accounts, calculates fare payments based on established business rules, and processes all transactions. The centralized back office will be the system of record and take priority over any other systems/media that may hold account information. The account-based system will support multiple media types, which will serve as a credential for a back office account. Centralized fare processing will reduce the need for complex field validation devices, and enable integration with other systems. Fare data may be stored on fare media for specific functions, but the central system will take precedence for fare calculations and tariff enforcement.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
3.3	**System Design & Architecture - System Integration Services**					
3.3-1	The System will support the addition of new agencies, including fare rules that are part of the existing design.					
3.3-2	Capital Metro will be able to add new transportation connections, modes and products (e.g., parking) with unique fare pricing and all the configurability of existing modes and products through APIs provided by Bytemark.					
3.3-3	The System will integrate with Capital Metro's GTFS-RT feed and, as required, the existing and new CAD/AVL system to provide functionality such as single sign-on and geolocation data for transactions.					
3.3-4	Integrations with third-party products including, but not limited to: Ticket Vending Machine, Onboard Validator, Transit Store Point of Sale, Transit On-Demand, Data Warehouse, Enterprise Resource Planner (ERP), etc.					
3.3.1	**System Design & Architecture - APIs**					
3.3.1-1	Bytemark shall upgrade the system using Hypertext Transfer Protocol Secure (HTTPS), or Capital Metro approved modern alternative, based functional (e.g., not device- or system-specific) API that support core system functions and enable access to those functions for any device or system that requires use of them. Devices and systems may make use of more than one API to support required functionality.					
3.3.1-2	Bytemark shall develop, publish specifications for, and implement the use of APIs to support critical system functions and all interfaces between system components, and is not limited to the specific APIs described in this section. The API specifications will include all API calls, data formats, and communication and security protocols used to support the System interfaces. Any additional APIs beyond those described in this section, which are required, will be identified during design review. Bytemark shall provide Interface Control Documentation (ICD) for each system interface that describes the interface and APIs used to support it.					
3.3.1-3	The APIs will include the ability for third party vendors to add value to customer accounts and to present credentials for accounts (bar codes or NFC). This will be used to allow third parties such as trip planning applications to directly sell transit fares and present credentials without a customer needing to load the Bytemark application.					
3.3.1-4	The system will have the ability to read and validate bar codes provided by third parties e.g. Austin FC game tickets					
3.3.1-5	The API and Interface Control Documentations (ICD) will be fully owned by or licensed to Capital Metro with the right to use and distribute the specifications without further approval, license, or payment.					
3.3.1-6	Bytemark shall update the API and Interface Control Documentation (ICD) specifications as necessary throughout the warranty and Software Maintenance Agreement terms.					
3.3.1-7	Bytemark shall implement strong security controls to prevent fraudulent use of the APIs and authenticate all users.					
3.3.1-8	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
4.0	**System Components**					
4.1	**System Components - Customer Service Terminals**					
4.1-1	Bytemark shall upgrade or replace all necessary peripherals and associated software to deploy Customer Service Terminals (CST) at locations designated by Capital Metro. Capital Metro shall provide the computers, displays, keyboards, and pointing devices that the CST software and peripherals require.					
4.1-2	CSTs will be used by Capital Metro to assist customers with a wide variety of activities related to servicing their System accounts.					
4.1-3	The CST modules and key functions may include: • Computer, display, keyboard and pointing device (furnished by Capital Metro) • Closed-loop media processing • Secure cash storage • Bank card processing • Customer display • Receipt printing • Image capture (for card personalization) • EU fare media printing/encoding using Capital Metro Genfare encoding key or Bytemark ticketing system encoding • Uninterruptible power supply • Communications interfaces as necessary					
4.1-4	The CST will conduct a variety of functions. At a minimum, these functions include: • Sell System fare media, (and create new transit accounts) • Sell all supported fare products (e.g., stored value and passes) and load fare products to transit accounts • Sell serialized Human Services fare products to authorized Human Services representatives • Sell serialized paper tickets individually or in bulk • Query transit account status (e.g., passenger type, active/inactive, blocked/unblocked) • Query fare payment transaction history • Query sales transaction history • Query adjustment transaction history • Enable fare product for autoload (requires funding source in customer account) • Generation of fare payment reversal (e.g., cancellation) • Generation of sales reversal (e.g., refund) • Generation of an transit account adjustment (e.g., credit or debit) • Transfer of balance between two transit accounts • Block/unblock card, transit account, or individual fare product • Lost, stolen, or damaged card replacement (e.g., associate new card with existing transit account) • Make comments on customer accounts and transit accounts • Generation of an opt-out refund (e.g., close transit account and issue refund) • Create new customer account • Query customer account status/data • Modify customer account data • Register (e.g., associate) a transit account to a customer account • Unregister (e.g., disassociate) a transit account from a customer account • Add, update or remove a funding source to/from a customer account • Close or suspend a customer account • Encoding, printing, and issuance of personalized EU fare media (when configured to do so), including the addition of a photo					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
4.1-5	The CST will support blind reconciliation whereby the user at the end-of-shift enters the amount in sales by payment method into the CST. The CST will indicate if the totals entered reconcile with the System information and allow the user to correct the amount up to an Capital Metro configurable amount of times. Supervisory role logon will allow for override of the blind reconciliation feature.					
4.2	**System Components - Mobile Applications**					
4.2-1	Bytemark shall upgrade the customer mobile app to include a closed-loop fare payment credential which will be virtualized on the Near Field Communication (NFC) secure element of the mobile device, provided the mobile device is equipped with this capability. This functionality will be supported on each mobile platform once it is available. The customer mobile app will also support the display of a graphical ticket that can be used for fare payment at a fare validator via an optical interface.					
4.2-2	The customer mobile app will be tested and support the two most recent major versions of operating systems on the Android and iOS platforms on the day that the OS is released to the general public.					
4.2-3	The customer mobile app will be available in the app stores, offered and maintained by Bytemark.					
4.3	**System Components - Customer Web Portal and Capital Metro Website**					
4.3-1	The Customer Web Portal website shall be upgraded to allow all customers to access and control their customer accounts over the web. Customers include individuals and businesses. Customers will access varying functionality through the website based on their customer account type.					
4.3-2	Capital Metro will continue to use their enterprise CMS to manage website content. Bytemark's account management and value purchasing capabilities will be integrated with Capital Metro's existing website following Capital Metro's branding and design requirements.					
4.3-3	Users will access the customer website and mobile app using the same user login.					
4.4	**System Components - Account-Based Transaction Processor**					
4.4-1	The back office will manage the automatic reloading of value or fare products that are configured for autoload. Autoload will be based on configuration parameters, and will require the account to be registered with a valid funding source, such as a credit or debit card or bank account (ACH) stored in the associated customer account					
4.4-2	The autoload feature will support both threshold-based triggers (i.e. reloading when the stored value balance, remaining trip balance, or remaining validity period falls below a configurable threshold), and calendar-based triggers (i.e. reloading on a configurable date every month).					
4.4-3	The System will have the ability to segregate any value load using pre-tax dollars, including the segregation of value purchased using pre-tax transit funds and pre-tax parking funds.					
4.4-4	The System will have the ability to restrict the use of pre-tax and tax-free funds to qualified services (for example, transit/vanpool and commuter parking).					
4.4-5	The System will allow after-tax stored value to be used on all services, including transportation connections that have payment integration.					
4.4-6	The System will be upgraded to enable Capital Metro to initiate acceptance of open payments; that is, direct payment of fares at the validator using a bank-issued contactless credit card or NFC-enabled smart phone with mobile payment application.					
4.4-7	The System will have the ability to maintain an audit trail from the original transaction postings, to the final posting, to the financial management application.					
4.4-8	The back office system will provide access to no less than seven (7) years of historical data. Deletion and archiving of data will be supported as agreed by Capital Metro.					
4.4-9	The back office will retain detailed active transactions for at least 25 months.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
4.5	**System Components - Central Payment Application**					
4.5-1	Bank funding via credit cards, debit cards, and ACH will be processed through a Central Payment application that connects to a payment gateway managed by a merchant bank or third-party payment processor. The Central Payment application will support the processing of bank cards through all channels, including: • CSTs • Customer website • Customer mobile app • Validators accepting open payments Bank card processing for the retail network will be performed through their own existing POS system. The Central Payment application will be compliant with all appropriate security standards, PCI-DSS and the System ISMS. The System will support full transaction-level reconciliation of all bank card funds processed through the System, including those accepted for customer account orders. Settlement data from the bank card processor or merchant bank will be imported by the fiscal agent or captured through integration with existing financial systems. This will allow for full settlement traceability to the back office applications. The System will automatically handle non-payment and chargeback transactions, making the appropriate accounting entries and reversing sales to correct account balances as necessary					
4.6	**System Components - Customer Relationship Management Application**					
4.6-1	Capital Metro will be implementing an enterprise customer relationship management system in a future fiscal year. Bytemark shall include the following upgrades to their system to integration in Capital Metro's chosen system. This integration will be performed in an option year of the contract.					
4.6-2	Bytemark shall upgrade the system to integrate with Capital Metro's selected CRM application. The CRM application will connect to the back office through the use of the Bytemark provided APIs, and serve as the primary interface for customer service staff to view and update transit and customer accounts. The CRM application will enable customer service staff to perform the following functions: • Assign new media to customers •Register a transit account (e.g., create or update a customer account) •View transit account balance, transaction history, and fare capping status •Perform fare media and value sales •Enable the automatic reloading of value (e.g., autoload) •Modify a transit account balance as part of a balance transfer, refund, or adjustment •Modify customer account (e.g., registration) data •Modify transit and customer account attributes associated with participation in business account programs •Initiate replacement of a lost/stolen/damaged card •Close or suspend a transit account					
4.6-3	Customer Service Representatives will be able to access and manage transit and customer accounts for customers through Capital Metro's selected CRM system. The Bytemark back office CRM application will enable the tracking of all customer service contacts and requests, and the actions taken to resolve those requests, in customer service records that can be created, viewed, and modified using the CRM tool.					
4.6-4	Customer service records will be created automatically based on customer-initiated actions performed through the customer website and customer mobile app.					
4.6-5	Customer service staff will be able to manually create or update (e.g., add notes) a customer service record when responding to customer service requests in person, over the web, or by phone.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
4.6-6	The integration with Capital Metro's CRM application will support the management of customer account programs, which will allow accounts to be associated to a customer account (e.g., employer or school) for account management and the loading of value.					
4.7	**System Components - Fare Inspection and Citation Management**					
4.7-1	Bytemark shall upgrade the mobile inspection app to continue to support inspection, citation management, and sales under the new system					
4.8	**System Components - Retail Network**					
4.8-1	Capital Metro may be partnering with a retail smart card network and integrated into their system in a future fiscal year. Bytemark shall include the following upgrades to their system to integrate with Capital Metro's chosen system. This integration will be performed in an option year within the contract.					
4.8-2	Bytemark shall contract and integrate with a virtual stored value retail network service provider for the loading of transit value at the retailer to the System customer accounts and stored value wallet.					
4.8-3	Bytemark and its retail network service provider shall work with Capital Metro to identify an extensive list of retail merchant participants located throughout Capital Metro service area that include large and small grocers, drug stores and convenience stores.					
4.8-4	All merchants in the retail network shall accept cash (at a minimum) as a form of payment for stored value load transactions. The acceptance of other payment types such as bank cards and personal checks is encourage but will be at the merchant's discretion.					
4.8-5	All fees for payment processing, including interchange and acquirer fees shall be borne by the service provider or retail merchants. No fees shall be assessed to Capital Metro or the customer for the use of cash, bank cards, or checks.					
4.8-6	Bytemark shall guarantee payment of funds to Capital Metro for all completed System stored value load transactions performed via the retail network.					
4.8-7	Bytemark shall settle funds to the Capital Metro-designated bank account(s) as frequently as possible, and no later than two (2) business days following the retail network service provider’s receipt of funds from the retail merchant.					
4.9	**System Components - Media Inventory Management**					
4.9-1	Bytemark shall upgrade the back office system to include Fare Media Management (FMM) as part of the System back office. The FMM shall manage the following functions: • Credentials – management of credentials and the associated business rules. • Card inventory – management of card inventory and ordering. • Association – association of credentials with accounts and the ability to track accounts associated with physical cards and mobile apps.					
4.9-2	Media inventory shall be kept in a single system of record and updated for each transaction including purchases, sales, consignment issues and returns of inventory. Individual consignment inventory will be up-to-date based upon the inventories conducted onsite. Media product still on site will be inventoried on a regular basis. Functionality will be available to track where all media inventory is located with current status.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
4.10	**System Components - Tariff Management**					
4.10-1	Bytemark will be responsible for upgrading the back office Tariff Management capabilities of the system to support the new functionality. The Tariff Management capability will allow Capital Metro staff with appropriate security access to manage and update product tables.					
4.10-2	The fare tables will be easy to view, review, and test when entering during creation of initial tables and any future fare updates. This will be addressed during design and testing.					
4.10-3	The System will allow Capital Metro to view and compare draft fare sets and changes to active and pending fare sets by Capital Metro and regionally, by sales channel, and by fare product.					
4.10-4	The System will have the ability to roll back to a previously used fare set.					
4.10-5	All fare product configurations will be able to be performed by Capital Metro, as well as by Bytemark during implementation and throughout the warranty and software maintenance agreement terms.					
4.10-6	The System will allow fare set changes on a frequent, including daily, basis without regard to additional pending changes. For example, an Capital Metro could change fare rules regardless of other Capital Metro changes that are pending.					
4.10-7	The System will be able to manage, store, and deploy an active fare set and at least two (2) pending fare sets. An active fare set will become effective immediately upon publication. Pending fare sets will be able to be activated manually, or automatically based on a future activation date configured.					
4.11	**System Components - Financial and Enterprise Resource Planning (ERP) Application**					
4.11-1	Capital Metro will be implementing a financial and enterprise resource planning (ERP) system in a future fiscal year. Bytemark shall include the following upgrades to their system to integrate with Capital Metro's chosen system. This integration will be performed in an option year within the contract.					
4.11-2	Bytemark will upgrade the System to support a daily export of the following journal entries: -Deferred revenue -Recognized revenue -Refunds -Credits and discounts -Goodwill transactions -Cash receipts The export will be suitable for import into Capital Metro's financial systems. The data to be included and the format of the export will be approved by Capital Metro during design.					
4.11-3	The back office will have the ability to make sure that total debits equal total credits for a single journal entry (e.g., double-entry accounting) when sending data to the financial application.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
4.12	**System Components - Reporting and Data Warehouse**					
4.12-1	Capital Metro will be implementing an enterprise data warehouse system in a future fiscal year. Bytemark shall include the following upgrades to their system to integrate with Capital Metro's chosen system. This integration will be performed in an option year within the contract.					
4.12-2	Bytemark will upgrade the System to support reporting to meet all requirements of the fare system upgrade.					
4.12-3	Bytemark shall upgrade and provide Capital Metro with user level analytics of customer facing applications including mobile and web apps.					
4.12-4	Bytemark will upgrade the System to support integration with Capital Metro's enterprise data warehouse with the ability to have a real-time data interface and the option for daily data exports from the Bytemark System.					
4.13	**System Components - Integration with Cash Farebox and Vaulting System**					
4.13-1	Capital Metro will be upgrading or replacing the cash farebox and vaulting system in a future fiscal year. Bytemark shall include the following upgrades to their system to integrate with Capital Metro's chosen system. This integration will be performed in an option year within the contract.					
4.13-2	Bytemark will upgrade the System to support integration of reconciliation functions of Capital Metro's current Genfare cash farebox and vaulting system. The Genfare system will be upgraded or replaced in a future fiscal year and will require integrating with the chosen system.					
4.14	**System Components - Traveler Tools**					
4.14-1	Capital Metro will be implementing or integrating with a mobility-as-a-service platform in a future fiscal year. Bytemark shall include the following upgrades to their system to integrate with Capital Metro's chosen system. This integration will be performed in an option year within the contract.					
4.15	**System Components - Parking**					
4.15-1	Capital Metro will be implementing a parking system in a future fiscal year. Bytemark shall include the following upgrades to their system to integrate with Capital Metro's chosen system. This integration will be performed in an option year within the contract.					
5.0	**Fare Policy**					
5.1	**Fare Policy - General Requirements**					
5.1-1	The System will support the current fare structure as a foundation. Fare structure includes the supported fare policies, fare media, and fare products through which customers purchase fare media and products. The fare structure will be configurable by Capital Metro, and designed to be upgraded to a simple, unified system that enables interoperability across current and future transit modes without additional development.					
5.1-2	The tariff will be configurable in such a way that Capital Metro may implement different fare policies for different payment methods, e.g. no capping benefits if paying with open payments.					
5.1-3	The tariff fare capping program shall offer the ability to specify the customers with eligible access to capping by offering settings limit within a product group or for all customers.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
5.2	**Fare Policy - Fare Structure**					
5.2-1	Fare policy business rules will be used to determine the fare charged to the rider on the basis of applicable passenger types, fare structures (including mode), and fare products.					
5.2-2	The System will be upgraded to support a variety of fare policies and products, including stored value wallet, transfers, reduced fares for eligible customers, daily and monthly pass products, multi-ride products, programs that require riders to pre-qualify (e.g., active-duty military, low-income program), programs by customer account type, and other Capital Metro-specific programs.					
5.2-3	The System will support stored value, which will serve as an electronic cash-equivalent, and will be accepted for payment across all modes and services. When stored value is used for payment, the System will deduct the correct fare at each boarding or entry in real-time from the account, based on the fare pricing configuration.					
5.2-4	The system will be upgraded to support fare capping. If fare capping is enabled, riders will pay per boarding up until a capping threshold; at this point, riders will no longer be charged for their boardings for the remainder of the specified time period.					
5.2-5	The system will support the setting of multiple fare cap time periods, each with their own capped price threshold. Fare cap time periods will be configurable for anywhere from 1 to 366 days. The capping time periods will be calendar-based, not rolling.					
5.2-6	The system will be capable of issuing time-based passes as the base fare. These passes will be configurable by Capital Metro to be valid for anywhere between 60 and 180 minutes.					
5.2-7	The system will support separate fare cap price thresholds for different services and different rider categories. This could include a single multiple that is applied to all base fares to establish the relevant caps.					
5.2-8	The system will support calendar products that are valid for unlimited rides during a predefined calendar period for rides on services costing at or below the face value of the pass. The system will also support rolling products that are valid for unlimited rides on services costing at or below the face value of the product for a predefined period starting at product activation, which may occur upon sale or first use. Calendar and rolling products do not need to be simultaneously supported.					
5.2-9	The System will support date-based and promotional pricing that offers discounted fares on a temporary and permanent basis, up to and including the offering of free fares. Discounted fare pricing will be able to be configured for specific fare media types, passenger types, modes, service types, and routes, and put into effect indefinitely or for a defined period.					
5.3	**Fare Policy - Fare Products**					
5.3-1	The System will continue to support fare products and pricing for business accounts, school pass programs, group fares, and other bulk fare sales.					
5.3-2	Accounts will be able to contain multiple fare products simultaneously (e.g., stored value and a pass product).					
5.3-3	The configurable service day may be longer than 24 hours, and service day hours may overlap. Pass products will be configurable to extend the validity to the end of the last service day.					
5.3-4	Unused rolling period pass products (e.g. day passes) can expire. Expiration will be configurable. Validated rolling period pass products expire at the end of the validity period.					
5.3-5	Day passes and short-term products (e.g., convention passes) will activate upon first tap, and the validity period will be configurable to accommodate specified transit days.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
5.4	**Fare Policy - Passenger Types**					
5.4-1	A passenger type must be defined for each account. The default passenger type that will be associated with a account will be the Adult full fare passenger type. Passenger types include but are not limited to: • Adult full fare • Youth K-12 • Emergency and Active-duty military • MetroAccess • Reduced fare Additional passenger types will be able to be defined by Capital Metro.					
5.4-2	An account may only have one passenger type associated with it.					
5.4-3	Adult full fare customers will have the option of associating an account with a customer account or remaining anonymous.					
5.4-4	Certain reduced fare passenger types will require association to a customer account.					
5.4-5	Passenger types will be able to be modified and configured manually, or automatically based on customer date of birth or the granting of a temporary classification with a configurable end date.					
5.5	**Fare Policy - Loading Fare**					
5.5-1	The System will be upgraded to enable customers to use stored value wallet to purchase fare products.					
5.5-2	The System will enable a customer to set up autoload to reload stored value wallet and/or fare products.					
5.5-3	Customers will be able to define threshold and calendar-based autoloads for accounts based on parameters set by Capital Metro staff.					
5.5-4	The loading of stored value will be restricted based on configurable parameters, including the minimum and maximum amount that can be loaded in a single transaction.					
5.5-5	All parameters governing threshold and calendar-based autoloads will be fully configurable by Capital Metro staff, including the enabling or disabling of an autoload, threshold value (e.g., trigger), funding source, and fare product and/or amount to be loaded. Final configuration parameters will be defined during design review.					
5.5-6	The capability to load a particular fare product to an account will be configurable based on the fare product type and passenger type associated with the account.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
6.1	**Fare Media - General Requirements**					
6.1-1	Fare media and applications will be designed for use in an account-based system, and serve as credentials for accessing closed-loop transit accounts maintained within the System back office.					
6.1-2	All System electronic fare media will be ISO/IEC-14443 compliant for secure communication with System card readers and fare validators.					
6.1-3	The System will be upgraded to accept the following closed-loop media for fare payment: - Capital Metro-issued Extended Use (EU) smart cards - Capital Metro-issued Limited Use (LU) paper smart cards - Capital Metro-approved Third party smart cards, such as employee or student ID cards - Virtual Capital Metro fare cards in a mobile wallet application - Printed paper tickets with QR code, issued by Capital Metro Ticket Vending Machines					
6.1-4	Each closed-loop fare card, virtual fare card and QR-code ticket will be associated with a unique transit account in the back office.					
6.1-5	For smart card fare media and QR-code tickets, each customer will be required to have and present their own fare card. Mobile ticketing applications on a single device may be used for more than one customer (registered user plus guest(s)), provided each customer is using a unique transit account.					
6.1-6	The System will be upgraded to accept the following open payment media, for direct payment of fares at the validator: - Contactless bank cards, including VISA, MasterCard and American Express - Virtual bank card in a smart phone mobile wallet, including Apple Pay or Google Pay					
6.1-7	Nothing in this contract shall prevent Capital Metro from procuring supplies of fare cards using competitive purchase from multiple U.S. sources. Bytemark shall provide the specifications, licenses and associated documentation necessary to enable procurement by Capital Metro of fare media from qualified smart card producers/printers.					
6.2	**Fare Media - Capital Metro-Issued Fare Cards**					
6.2-1	The transit payment application will be upgraded to be compatible with the following MIFARE formats: the latest version of DESFire for EU cards, and the latest version of Ultralight-C for LU fare media. All smart card fare media will be supplied by Capital Metro, including a supply for testing.					
6.2-2	All Capital Metro-issued EU fare cards will be reloadable at designated retailers participating in the retail sale/reload network. This may require magnetic stripe and/or bar code graphics on the card for processing of card sale and reload transactions, as determined by the retail reload network provider.					
6.2-3	The System will support the printing of personalized and customized EU fare cards using the CST plus Capital Metro or Bytemark-supplied peripherals, such as printer/encoder.					
6.2-4	Capital Metro-issued EU fare cards will be printed with a unique non-sequential 16-digit serial number that is distinct from the card's Unique Identification Number (UID). Each card will also be printed with a randomized three-digit security code. Capital Metro will provide an electronic file that lists each card with its UID, serial number and security code.					
6.2-5	EU fare cards will be worthless until activated at time of sale.					
6.2-6	LU fare cards will be worthless until distributed by Capital Metro to social services agencies for issue to qualified users.					
6.2-7	EU fare cards will have the ability to be managed within the mobile app and customer web app.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
7.1	**Operations and Maintenance Services - Operations and Maintenance Model**					
7.1-1	The System will be operated as follows: Capital Metro will be responsible for: field equipment maintenance; in-person sales; phone sales; financial settlement; card inventory management and distribution; branding and user interface. Bytemark will be responsible for the following outsourced functions: maintenance and administration of the hosted central system and the hosted website; retail sales/reload network management; vendor management; merchant accounts; financial settlement; incident and change management; disaster recovery; the information security management system; and software maintenance and system updates. Outsourced functions for which Bytemark will NOT be responsible include: maintenance of field equipment supplied by others.					
7.1-2	Working with Capital Metro, Bytemark will execute updates to amend the existing Warranty, Maintenance and Services Agreement (WMA), including at minimum updates to: Scope of Work, App. A - Supported Systems, App. B - Bytemark Contacts, App C - Client Contacts, App E - Performance Management Disincentives and App H - Performance Deficiencies Credits.					
7.1-3	Bytemark will update as necessary and execute the Software Licensing Agreement					
7.2	**Operations and Maintenance Services - Performance Measurement**					
7.2-1	Update the Warranty and Maintenance Agreement with the following components: Back office availability will be calculated based on the total out of service time for the associated system: Back office application availability = 1 - (out of service time / total operating time) Total Operating Time is defined as the number of minutes in a day (1440) multiplied by the number of days in the month of measurement, while Out of Service Time is defined as all time during which the System is not in a fully operational state, and includes all time necessary to respond and repair to issues. Scheduled maintenance time is excluded from the calculation. The availability requirement for each System back office application is as follows: Application availability must meet or exceed 99.99% each calendar month					
7.2-2	Back office accuracy shall be based on the number of incidents where a device or back office generated transaction is recorded incorrectly within the associated system. Performance will only be measured for those applications for which Bytemark is responsible. The accuracy requirements for the System back office applications are as follows: Financial Management application: No more than 2 incidents of inaccurate reporting per calendar month.					

#	Compliance Term	Comply	Release	Bytemark Comments	Capital Metro Response	Test #
7.3	**Operations and Maintenance Services - Credit Assessment**					
7.3-1	Bytemark and Capital Metro shall revise as necessary and execute the Software Licensing Agreement.					
7.3-2	Credits will be determined as a percentage of the operations payments made to Bytemark. The credit percentage and operations payment associated with each KPI will be determined during negotiations.					
7.3-3	The credit will be assessed if a KPI fails to meet the specified performance requirement (or threshold) for three consecutive monthly reporting periods.					
7.3-4	Bytemark shall be responsible for reporting on credits in the System performance reports and will deduct credits directly from any invoices submitted to Capital Metro.					
8.1	**Marketing Strategy, Campaign, & Customer Outreach**					
8.1-1	Bytemark shall subcontract with a marketing firm approved by Capital Metro to develop and coordinate the functional digital marketing materials including in-app, customer account web portal, and Capital website web tutorials.					

EPPM Phase Tasks and Deliverables. Bytemark shall perform the following phase tasks and provide the associated deliverables required to deploy all hardware, software, updates and configurations resulting in a fully functional and tested system. Bytemark shall obtain CMTA review of all deliverables and make changes and updates to deliverables per CMTA review as needed. CMTA acceptance of all deliverables for each phase as evidenced by a signed phase acceptance certificate is required prior to invoicing. Each phase is closed by Bytemark's Phase Completion Notification with Proof of Deliverables, CMTA's Acceptance Certificate Signoff, and Bytemark's Invoice upon Receipt of CMTA Authorization to Invoice.	
1.0	**Plan. Meet with CMTA project manager and business area stakeholders for project planning, including review of proposed schedule, roles and responsibilities, as well as conduct a complete review of functionality to be delivered, and other project activities. Plan Deliverables from Bytemark:** 1. Project organization chart 2. Project schedule - draft detailed schedule following Capital Metro's EPPM phased tasks and deliverables (draft) 3. Action Items and Issues log (AIL) 4. Project Management Plan (PMP-draft) 5. Infrastructure and Integration Audit 6. Initiate Risk Register 7. System Implementation Plan (draft) 8. Compliance Matrix Review and Update 9. Kick-off meeting with stakeholders to review and clarify requirements including confirmation of any required updates to CMTA's environment
2.0	**Design. Bytemark's technical requirements gathering and detailed design, beginning with on-site assessment and discussion with affected CMTA departments. This phase will determine how the system will be installed, product wireframe presentation to the customer, and how it will be managed in the back end. Bytemark will work with CMTA to develop materials that will provide a basis to help instruct CMTA stakeholders in the easiest and most efficient way to use the system to their utmost advantage. Design Deliverables:** 1. On-Site Assessment & Design Workshop; Documentation of Findings 2. Configuration Management Document ("CMD" - Draft) 3. Wireframe diagrams (Draft) 4. System Implementation Plan (Final) 5. Disaster Recovery Plan (Draft) 6. Quality Assurance Plan (Draft) CMTA only confirms QA/QC; Plan shall clearly delineate that Bytemark performs QA/QC process 7. Risk Management Plan (Final) 8. Data dictionary and Entity Relationship Diagram (ERD) 9. Project Schedule (Baseline) with Resource Loading 10. Network architecture diagram (Draft) 11. Communication connection designs (Draft) 12. Installation Plan (Draft): equipment installation design (if applicable), procedures, schedule, CMTA support required; detailed so CMTA can perform installation 13. Perform Preliminary Design Review (PDR) Design and System Implementation Plan with Stakeholders 14. Create Final Design based on review and perform Final Design Review (FDR) 15. Review and Acceptance of Final Design and Project Management Plan 16. Compliance Matrix Review and Update
3.0	**Develop. Development, configuration and installation of the solution and integration as well as installation within a development and a test environment so configuration and testing of the required functionality can be started. This task will include setting the initial configuration values by Bytemark so they can be tested and changed if needed. During this phase, the rollout of the system must be worked on to include training all IT and Operational staff who will use or have on-going support roles. Develop Deliverables:** 1. Quality Assurance Plan Including QA/QC Checklist (Final) 2. Test Environment Installation that provides CMTA full access throughout the project and the life of the system 3. Supporting Infrastructure Implemented 4. Application and Functionality Development 5. Test Procedure/Plan including test Scripts, use cases, acceptance test criteria demonstrating each Compliance Matrix term is developed and meets requirement (Draft) 6. Update Compliance Matrix with Test Number(s) 7. CMD Values Test and Update 8. High-level Training of CMTA Staff to Prepare for Test Phase 9. Bytemark Warranty and Maintenance Plan Review 10. Review and Feedback of CMTA Support Responsibility Matrix 11. Role-based, On-site Training Plan for all User Types (Draft): •Training schedule and course outlines for review a minimum of three weeks prior to the scheduled classes •Separate training sessions for revenue, maintenance and system administrator roles •Provide all materials necessary to train participants (CMTA will provide space and laptops) •Schedule the training staff to be on site timely to ensure equipment, materials, student accounts and classroom are fully ready for when class begins •Arrange for an instructor(s) with thorough knowledge of the material covered in the course(s) and the ability to effectively lead the knowledge transfer •Provide customized training manuals specific to CMTA's environment in Microsoft Word and PDF. Bytemark shall provide the agreed-to number of hard copies

4.0	**Test. Bytemark shall develop and implement a comprehensive program to test all components and applications that comprise the integrated Bytemark AFPS solution. Testing is to be performed in five distinct and separate phases:** **1. Functional Unit Test (FUT)** **2. System Integration Test (SIT)** **3. Field Integration Test (FIT)** **4. Pilot Test** **5. System Acceptance Test** **The testing phase shall not be deemed completed until all functional requirements have been fully tested and approved by Capital Metro. Bytemark shall develop an AFPS Test Plan that includes the number and range of tests, detailed schedule indicating the sequence of each test, and when and where each test will take place. Bytemark shall not perform any test until the corresponding test plan and procedures have been approved by Capital Metro. Bytemark shall develop Test Procedure documents with test scripts, all anticipated use cases and acceptance criteria for review and approval by Capital Metro for each phase of testing. Test deliverables:** 1. Test Plan 2. Test Procedures 3. Pilot Test Plan (subset used to determine public launch) 4. System Acceptance Test Plan 5. Final System Acceptance (subset used to determine the start of warranty) 6. Security Penetration Test (performed as part of SAT) 7. Disaster Recovery Test - End-to-End (performed as part of FIT) 8. Volume and Stress Tests 9. Regression Testing of the entire Test Plan for any Class 1 and Class 2 Failures 10 Test Results and Reports (including results for failed tests) 11. Agency Test Facility 12. Procedures for changing environments (dev, test, stage, prod) 13. Installation Plan (Final) 14. Test Failure Log & Remediation Plan. Bytemark shall lead testing of the solution including integrations and resolve all Severe (Class 1) and Significant (Class 2) Test Failure Results (TFRs). Bytemark shall endeavor to resolve Minor (Class 3) TFRs during this phase; however, the requirement for Class 3 resolution is during the Closeout phase. Definition for each class are as follows: •Severe - A Class 1 test failure is a severe defect that prevents, inhibits, or significantly impairs further testing or operation of the system. •Significant - A Class 2 test failure is a significant defect that does not prevent further testing or has a minimal effect on normal operations of the system. •Minor – A Class 3 test failure is a minor or isolated defect that does not impact or invalidate the testing or normal operations of the system. 15. Compliance Matrix Review and Update 16. Training Plan (Final) 17. User, Admin, Maint., Installation, and Training Manuals
5.0	**Deploy/Go Live: Deploy: once all the test failures have been corrected, the Bytemark shall install and configure the software and incorporate it into the live environment. Go Live: the system shall go live and be monitored for the first 30 days of operation. If Severe (Class 1) or Significant (Class 2) issues arise, the Go-Live period may be cancelled, extended or restarted. The Bytemark shall be required to participate in the monitoring of the system and respond to issues so they are quickly resolved. Deploy/Go Live Deliverables:** 1. Conduct Training for all User Types 2. Document Procedures and Migrate Environment from Test to Production 3. QA/QC checklist Sign off 4. Delivery and Inventory of Spares (if applicable) 5. Update to Disaster Recovery Plan 6. Delivery of all Documentation including User, System Admin, Maintenance, Installation and Training Manuals, (Revise Draft) 7. Deployment, Implementation, Configuration and Integration of the Bytemark solution with all environments 8. System Acceptance Test (SAT) 9. Resolution of SAT TFRs 10. Go Live Schedule and Transition Plan 11. System Go Live 12. Technical Lead On-site During First Week of Go Live, or Longer if System Issues are Experienced 13. Review and coordinate with CMTA to update CMTA Business Process Flowcharts for Fare System Solution Effectiveness 14. Revised (final) Copies of all Required Documentation including User and Training Manuals 15. Compliance Matrix Review and Update
6.0	**Close. Obtain acceptance by CMTA to formally close the project. Apply appropriate updates to project documents. Close out all procurement activities ensuring termination of all relevant agreements. Close Deliverables:** 1. Follow-up training on areas identified during Go Live and Training Documentation (Final) 2. Data dictionary and Entity Relationship Diagram (Final) 3. Network architecture diagram (Final) 4. Communication connection designs (Final) 5. All AIL items closed 6. Resolution of all Minor (Class 3) TFRs 7. Wireframe Diagrams (final) 8. Final Documentation for Environment Refresh (Develop-Test-Stage-Production) 9. Disaster Recovery Plan (Final) 10. Configuration Management Documents (CMD – Final) 11. APIs and all documentation related to all integrations (Final) 12. Warranty and Maintenance Procedure Review and Forms 13. As-builts: updates to any documentation including design document changes 14. Participation in Lessons Learned

Project Management. Bytemark shall manage the project continuously beginning with the Notice to Proceed through Close, and shall lead the project and is expected to drive and manage all aspects of the project including the management of any subBytemarks. CMTA shall manage and coordinate all its resources. A full-time Project manager or technical lead is required to be onsite at least two weeks per month during each phase of the project. A PMP is preferred and shall be approved by CMTA. Project Management Deliverables:		
7.0	1. Active Partnership with CMTA in assuring Project Success 2. Onsite as needed (May Be Performed by Technical Lead Depending Upon Scheduled Activities By Agreement with CMTA); Technical Lead will be onsite during pilot testing and resolution of any TFRs 3. Separate Lead Project Manager and Technical Lead for All Communication Regarding Work Under This Contract 4. Task Coordination with The Designated CMTA project manager 5. Regular Communication with The Project Manager and any other staff designated to discuss progress, critical risk factors, schedule, or unique issues that may surface. 6. Specification of CMTA's staff resources needed for project success with at least two weeks notice in advance within the project schedule. 7. Support Responsibility Matrix Review and Updates as Needed	8. Weekly Status Meetings with Updated Schedule and AIL 9. Review and Feedback of Change Requests as Needed 10. Monthly Risk Registry Updates 11. Monthly Management Review Meetings 12. Monthly Project Status Report 13. Quarterly attendance and Status Presentation at Steering Committee Meetings 14. Responsible for ensuring all project documentation, including meeting minutes, AIL updates, project schedule and plans are kept updated in the CMTA SharePoint site
Payment Milestones. Payment for each of the above described project phases (1.0-6.0) shall be paid in the following percentages of total Contract cost by release.		
8.0	1.0 Plan: 5% 2.0 Design: 10% 3.0 Develop: 15% 4.0 Test: 15% 5.0 Deploy/Go Live: 45% 6.0 Closeout: 10%	Payment will be governed based on: 1. Notification of Plan Phase Completion with Proof of Deliverables 2. Sign off on Phase Acceptance Certificate 3. Phase Invoice upon Receipt of Capital Metro Authorization to Invoice

EXHIBIT F - SCOPE OF SERVICES AND COMPLIANCE MATRIX - Appendix B1:
QUESTIONS

1.00	**Hosted Environment -** Answer the following questions in the "Answer" column:	**Answer**
1.01	Is this application hosted via a public cloud such as Amazon, an infrastructure as a service (IaaS), or is it self-hosted?	
1.02	Does the Contractor manage this or does a hosting provider manage it?	
1.03	Data security - Where and how is the data secured? Is it encrypted? Who 'owns' the data?	
1.04	Network security - firewalls, intrusion detection systems:	
1.05	•Do you have IDS/IPS? Who manages these devices?	
1.06	•Are these shared resources between the vendor and other hosted customers?	
1.07	•Are they shared between all of this vendor's customers or are they specific to an individual customer?	
1.08	Audit and logging trails, and system logging:	
1.09	•What information is logged?	
1.10	•Are logs reviewed and if so, by whom? Can we access these logs if necessary?	
1.11	Data segregation - How do you ensure data security and prevent unauthorized access to data of one tenant by other tenant users?	
1.12	•Who has access to our data and servers? How is it controlled?	
1.13	Availability - How do you mitigate the effect of potential DDoS attacks?	
1.14	•What is the bandwidth and what is the percentage of use? What is the percent of peak time use?	
1.15	•Performance management system - uptime, availability, response, delay, etc. Do you provide scheduled reports to their customers?	
1.16	•Backups - What is the backup and restoration plan? Is there an SLAs for recovery?	
1.17	•Identity management and sign-on process - How is identity management handled?	
1.18	•Do you support '2 factor authentication'?	
1.19	•Does the system provide limits on the number of invalid access attempts allowed?	
1.20	•If so, is the user locked out of the system indefinitely or for a specified timeframe?	
1.21	•Vulnerability patching - Server OS updates - What is their process, patching schedule, etc.? Will we incur downtime during patching? What is their notification process?	
1.22	•Disaster Recovery - How often do they test? Is the customer notified?	
1.23	•IT security - Can the vendor provide an overview of its' IT security program?	
1.24	•Is there a dedicated IT security team?	
1.25	•Do they have a formal security incident response plan?	
1.26	•If there is a breach, how quickly do you respond to remedy the problem? Is there a documented customer notification plan? Are there SLAs for notification?	
1.27	•Do you perform vulnerability scans, security assessments, or penetration testing? If so, how often?	
1.28	•Is the application designed and reviewed for the OWASP Top Ten security risks?	
1.29	Can you provide a data flow diagram? If so, please attach.	
1.30	Can you provide a detailed description of secure connection? If so, please attach.	
1.31	What daily steps are taken to ensure the system is up and all features available?	
2.00	**Network -** Answer the following questions in the "Answer" column:	**Answer**
2.01	What protocols are used? (Please be very detailed and specific, to include port numbers)	
2.02	How much bandwidth is required per client?	
2.03	What is the frequency for security patches and anti-virus updates? (Contractor or Capital Metro?)	
3.00	**Help Desk / Desktop -** Answer the following questions in the "Answer" column:	**Answer**
3.01	Are there special printer/printing requirements?	
3.02	What Client side software or services are needed (assume workstation has nothing on it)?	
3.03	Is there a specific drive mapping(s) required?	
3.04	Can the workstation use a DNS name to reference the server or devices?	
3.05	Can the workstation use a UNC name to reference the server or devices?	

4.00	**Manuals - The manuals shall be customized specific to Capital Metro's environment, provided in Microsoft Word and PDF, and be updated when new releases are provided. include but are not limited to the list below. In the "Answer" column, indicate the manual to be provided and what it covers**	**Answer**
4.01	Design and Requirements Documentation	
4.02	Acceptance Test Criteria	
4.03	Systems Administration Manual	
4.04	Security User's Manual	
4.05	User's Manual	
4.06	Database Dictionary	
4.07	Database Entity Relationship Diagram	
4.08	Architecture Diagram	
4.09	Integration Manual	
4.10	Process Flows	
4.11	Systems Configuration Documentation	
4.12	Maintenance Procedures Manual	
4.13	Reporting Manual	
4.14	Software License Agreements	
4.15	System, Hardware, and Software Maintenance Agreement	
5.00	**Reliability.** The solution shall have a proven, low-maintenance reliability record on multiple existing similar transit systems for at least two (2) years; using the below criteria, specify in the "Answers" column the reliability rates of your solution:	**Answer**
5.01	Uptime of hosted backend solution	
6.00	**Accessibility** - Answer the following questions in the "Answer" column:	
6.01	Is solution compliant with current WCAG (Web Content Accessibility Guideline) 2.0 AA and Title II Web Accessibility standards?	
6.02	Describe methodology for ensuring that all customer- and staff- facing screens are compatible with screen reader technology using text-to-speech and/or a refreshable Braille display. Are compatibility tests 100% automated or are power users (with disabilities, familiar with text-to-speech/refreshable Braille displays) brought in to consult and if so, at what stage(s)? How do you ensure that screens make proper use of forms mode, contextual labels, image field descriptions, and curbed read back of meta data?	
6.03	Can all screens be altered by high contrast settings either native to the solution or using those built into current windows operating systems?	
6.04	Can font size of all customer- and staff-facing screens be adjusted for visibility?	
6.05	If applicable, do all CAPTCHA (or similar) anti-bot checks include an alternative audio challenge?	
6.06	Are all customer-facing screens presented in English and Spanish?	

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
4	**Application & Interface Security** *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?				
5			AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?				
6			AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?				
7			AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?				
8			AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?				
9	**Application & Interface Security** *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, (removed all) identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?				
10			AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?				
11	**Application & Interface Security** *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?				
12	**Application & Interface Security** *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
13	**Audit Assurance & Compliance** *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?				
14	**Audit Assurance & Compliance** *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?				
15			AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?				
16			AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?				
17			AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?				
18			AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?				
19			AAC-02.6		Are the results of the penetration tests available to tenants at their request?				
20			AAC-02.7		Are the results of internal and external audits available to tenants at their request?				
21			AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?				
22	**Audit Assurance & Compliance** *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?				
23			AAC-03.2		Do you have capability to recover data for a specific customer in the case of a failure or data loss?				
24			AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?				
25			AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
26	**Business Continuity Management & Operational Resilience** *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Do you provide tenants with geographically resilient hosting options?				
27			BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?				
28	**Business Continuity Management & Operational Resilience** *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?				
29	**Business Continuity Management & Operational Resilience** *Power / Telecommunications*	BCR-03	BCR-03.1	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Do you provide tenants with documentation showing the transport route of their data between your systems?				
30			BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?				
31	Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system’s security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
32	**Business Continuity Management & Operational Resilience** *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?				
33	**Business Continuity Management & Operational Resilience** *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?				
34	**Business Continuity Management & Operational Resilience** *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?				
35			BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?				
36			BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?				
37			BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?				
38			BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?				
39	**Business Continuity Management & Operational Resilience** *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
40	**Business Continuity Management & Operational Resilience** *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?				
41			BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?				
42			BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?				
43	**Business Continuity Management & Operational Resilience** *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?				
44	**Business Continuity Management & Operational Resilience** *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical control capabilities to enforce tenant data retention policies?				
45			BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?				
46			BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?				
47			BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
48	**Change Control & Configuration Management** *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?				
49			CCC-01.2		Is documentation available that describes the installation, configuration and use of products/services/features?				
50	**Change Control & Configuration Management** *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?				
51			CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?				
52	**Change Control & Configuration** *Management* *Quality Testing*	CCC-03	CCC-03.1	Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services	Do you provide your tenants with documentation that describes your quality assurance process?				
53			CCC-03.2		Is documentation describing known issues with certain products/services available?				
54			CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?				
55			CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?				
56	**Change Control & Configuration Management** *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?				
57	**Change Control & Configuration Management** *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, as well as infrastructure network and systems components. Technical measures shall be implemented to provide assurance that, prior to deployment, all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer (tenant) as per agreement (SLA).	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
58	**Data Security & Information Lifecycle Management** *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?				
59			DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?				
60			DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?				
61			DSI-01.4		Can you provide the physical location/geography of storage of a tenant’s data upon request?				
62			DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?				
63			DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?				
64			DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?				
65	**Data Security & Information Lifecycle Management** *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?				
66			DSI-02.2		Can you ensure that data does not migrate beyond a defined				
67	**Data Security & Information Lifecycle Management** *eCommerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?				
68			DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?				
69	**Data Security & Information Lifecycle Management** *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?				
70			DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?				
71	**Data Security & Information Lifecycle Management** *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?				
72	**Data Security & Information Lifecycle Management** *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?				
73	**Data Security & Information Lifecycle Management** *Secure Disposal*	DSI-07	DSI-07.1	Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?				
74			DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
75	**Datacenter Security** *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership y defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?				
76			DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?				
77	**Datacenter Security** *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?				
78	**Datacenter Security** *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?				
79	**Datacenter Security** *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)				
80	**Datacenter Security** *Offsite equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?				
81	**Datacenter Security** *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?				
82			DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?				
83	**Datacenter Security** *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?				
84	**Datacenter Security** *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?				
85	**Datacenter Security** *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
86	**Encryption & Key Management** *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?				
87	**Encryption & Key Management** *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?				
88			EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?				
89			EKM-02.3		Do you maintain key management procedures?				
90			EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?				
91			EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?				
92	**Encryption & Key Management** *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?				
93			EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?				
94			EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?				
95			EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?				
96	**Encryption & Key Management** *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?				
97			EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?				
98			EKM-04.3		Do you store encryption keys in the cloud?				
99			EKM-04.4		Do you have separate key management and key usage duties?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
100	**Governance and Risk Management** *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?				
101			GRM-01.2		Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?				
102			GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?				
103	**Governance and Risk Management** *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?				
104			GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?				
105	**Governance and Risk Management** *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?				

	A	B	C	D	E	F	G	H	I
1	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
2									
3						Yes	No	Not Applicable	
106	**Governance and Risk Management** *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?				
107			GRM-04.2		Do you review your Information Security Management Program (ISMP) least once a year?				
108	**Governance and Risk Management** *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?				
109	**Governance and Risk Management** *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?				
110			GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?				
111			GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?				
112			GRM-06.4		Do you disclose which controls, standards, certifications and/or regulations you comply with?				
113	**Governance and Risk Management** *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?				
114			GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
115	**Governance and Risk Management** *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?				
116	**Governance and Risk Management** *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?				
117			GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?				
118	**Governance and Risk Management** *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?				
119			GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?				
120	**Governance and Risk Management** *Program*	GRM-11	GRM-11.1	Organizations shall develop and maintain an enterprise risk management framework to mitigate risk to an acceptable level.	Do you have a documented, organization-wide program in place to manage risk?				
121			GRM-11.2		Do you make available documentation of your organization-wide risk management program?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
122	**Human Resources** *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?				
123			HRS-01.2		Is your Privacy Policy aligned with industry standards?				
124	**Human Resources** *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?				
125	**Human Resources** *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?				
126			HRS-03.2		Do you document employee acknowledgment of training they have completed?				
127			HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?				
128			HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?				
129			HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?				
130	**Human Resources** *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?				
131			HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?				
132	**Human Resources** *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?				
133	**Human Resources** *Nondisclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?				
134	**Human Resources** *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
135	**Human Resources** *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Do you provide documentation regarding how you may or access tenant data and metadata?				
136			HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?				
137			HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?				
138	**Human Resources** *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?				
139			HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?				
140	**Human Resources** *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?				
141			HRS-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?				
142			HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?				
143	**Human Resources** *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?				
144			HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?				
145			HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
146	**Identity & Access Management** *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)				
147			IAM-01.2		Do you monitor and log privileged access (administrator level) to information security management systems?				
148	**Identity & Access Management** *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?				
149			IAM-02.2		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
150	**Identity & Access Management** *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?				
151	**Identity & Access Management** *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?				
152			IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?				
153	**Identity & Access Management** *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?				
154	**Identity & Access Management** *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?				
155			IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?				
156	**Identity & Access Management** *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?				
157			IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?				
158			IAM-07.3		Do you have more than one provider for each service you depend on?				
159			IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?				
160			IAM-07.5		Do you provide the tenant the ability to declare a disaster?				
161			IAM-07.6		Do you provided a tenant-triggered failover option?				
162			IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
163	**Identity & Access Management** *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?				
164			IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?				
165	**Identity & Access Management** *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?				
166			IAM-09.2		Do your provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?				
167	**Identity & Access Management** *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?				
168			IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?				
169			IAM-10.3		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?				

	A	B	C	D	E	F	G	H	I
1	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
2									
3						Yes	No	Not Applicable	
170	**Identity & Access Management** *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?				
171			IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?				
172	**Identity & Access Management** *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?				
173			IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?				
174			IAM-12.3		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?				
175			IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?				
176			IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?				
177			IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?				
178			IAM-12.7		Do you allow tenants to use third-party identity assurance services?				
179			IAM-12.8		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?				
180			IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?				
181			IAM-12.10		Do you support the ability to force password changes upon first logon?				
182			IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?				
183	**Identity & Access Management** *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?				
184			IAM-13.2		Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?				
185			IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
186	**Infrastructure & Virtualization Security** *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?				
187			IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?				
188			IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?				
189			IVS-01.4		Are audit logs centrally stored and retained?				
190			IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?				
191	**Infrastructure & Virtualization Security** *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?				
192			IVS-02.2		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?				
193	**Infrastructure & Virtualization Security** *Clock Synchronization*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?				
194	**Infrastructure & Virtualization Security** *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?				
195			IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?				
196			IVS-04.3		Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?				
197			IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
198	**Infrastructure & Virtualization Security** *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?				
199	**Infrastructure & Virtualization Security** *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?				
200			IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?				
201			IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?				
202			IVS-06.4		Are all firewall access control lists documented with business justification?				
203	**Infrastructure & Virtualization Security** *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
204	**Infrastructure & Virtualization Security** *Production / Nonproduction Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?				
205			IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?				
206			IVS-08.3		Do you logically and physically segregate production and non-production environments?				
207	**Infrastructure & Virtualization Security** *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?				
208			IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?				
209			IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?				
210			IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?				
211	**Infrastructure & Virtualization Security** *VM Security - vMotion Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?				
212			IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?				
213	**Infrastructure & Virtualization Security** *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
214	Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?				
215			IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)				
216			IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?				
217	Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?				
218			IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
219	**Interoperability & Portability** *APIs*	IPY-01	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?				
220	**Interoperability & Portability** *Data Request*	IPY-02	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?				
221	**Interoperability & Portability** *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?				
222			IPY-03.2		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?				
223	**Interoperability & Portability** *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?				
224			IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?				
225	**Interoperability & Portability** *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g.., OVF) to help ensure interoperability?				
226			IPY-05.2		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
227	**Mobile Security** *Anti-Malware*	MOS-01	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?				
228	**Mobile Security** *Application Stores*	MOS-02	MOS-02	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?				
229	**Mobile Security** *Approved Applications*	MOS-03	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?				
230	**Mobile Security** *Approved Software for BYOD*	MOS-04	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?				
231	**Mobile Security** *Awareness and Training*	MOS-05	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?				
232	**Mobile Security** *Cloud Based Services*	MOS-06	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?				
233	**Mobile Security** *Compatibility*	MOS-07	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system and application compatibility issues?				
234	**Mobile Security** *Device Eligibility*	MOS-08	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
235	**Mobile Security** *Device Inventory*	MOS-09	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each device in the inventory.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?				
236	**Mobile Security** *Device Management*	MOS-10	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?				
237	**Mobile Security** *Encryption*	MOS-11	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?				
238	**Mobile Security** *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?				
239			MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?				
240	**Mobile Security** *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?				
241			MOS-13.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?				
242	**Mobile Security** *Lockout Screen*	MOS-14	MOS-14	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?				
243	**Mobile Security** *Operating Systems*	MOS-15	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
244	**Mobile Security** *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?				
245			MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?				
246			MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?				
247	**Mobile Security** *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?				
248			MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?				
249			MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?				
250	**Mobile Security** *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?				
251			MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?				
252	**Mobile Security** *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?				
253			MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?				
254	**Mobile Security** *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?				
255			MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
256	**Security Incident Management, E-Discovery & Cloud Forensics** *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?				
257	**Security Incident Management, E-Discovery & Cloud Forensics** *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?				
258			SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?				
259			SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?				
260			SEF-02.4		Have you tested your security incident response plans in the last year?				
261	**Security Incident Management, E-Discovery & Cloud Forensics** *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?				
262			SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?				
263	**Security Incident Management, E-Discovery & Cloud Forensics** *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?				
264			SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?				
265			SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?				
266			SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?				
267	**Security Incident Management, E-Discovery & Cloud Forensics** *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes and impacts on all information security incidents?				
268			SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
269	**Supply Chain Management, Transparency and Accountability** *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?				
270			STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?				
271	**Supply Chain Management, Transparency and Accountability** *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?				
272	**Supply Chain Management, Transparency and Accountability** *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?				
273			STA-03.2		Do you provide tenants with capacity planning and use reports?				
274	**Supply Chain Management, Transparency and Accountability** *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
275	**Supply Chain Management, Transparency and Accountability** *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?				
276			STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?				
277			STA-05.3		Does legal counsel review all third-party agreements?				
278			STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?				
279			STA-05.5		Do you provide the client with a list and copies of all sub processing agreements and keep this updated?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
280	**Supply Chain Management, Transparency and Accountability** *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?				
281	**Supply Chain Management, Transparency and Accountability** *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?				
282			STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?				
283			STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?				
284			STA-07.4		Do you review all agreements, policies and processes at least annually?				
285	**Supply Chain Management, Transparency and Accountability** *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?				
286			STA-8.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?				
287	**Supply Chain Management, Transparency and Accountability** *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you permit tenants to perform independent vulnerability assessments?				
288			STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?				

	A	B	C	D	E	F	G	H	I
1 2	Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
3						Yes	No	Not Applicable	
289	**Threat and Vulnerability Management** *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?				
290			TVM-01.2		Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?				
291	**Threat and Vulnerability Management** *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?				
292			TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?				
293			TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?				
294			TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?				
295			TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?				
296			TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?				
297	**Threat and Vulnerability Management** *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?				
298			TVM-03.2		Is all unauthorized mobile code prevented from executing?				

Capital Metro Estimated Ridership Figures for 2025 and 2040

			2025 Peak Daily Ridership Estimate: 200,000		2040 Peak Daily Ridership Estimate: 300,000	
	Hour	Max %	Max Number of Boardings	Rate Per Minute	Max Number of Boardings	Rate Per Minute
	12 AM	0.965%	1,929	32	2,894	48
	1 AM	0.422%	844	14	1,266	21
	2 AM	0.641%	1,282	21	1,923	32
	3 AM	0.049%	98	2	147	2
	4 AM	0.046%	92	2	137	2
	5 AM	0.330%	661	11	991	17
	6 AM	1.684%	3,368	56	5,053	84
Peak Service Period	7 AM	6.969%	13,938	232	20,907	348
	8 AM	**10.230%**	**20,459**	**341**	**30,689**	**511**
	9 AM	8.156%	16,312	272	24,469	408
	10 AM	7.564%	15,129	252	22,693	378
	11 AM	5.576%	11,152	186	16,728	279
	12 PM	6.030%	12,061	201	18,091	302
	1 PM	5.906%	11,812	197	17,719	295
	2 PM	5.524%	11,047	184	16,571	276
	3 PM	7.384%	14,769	246	22,153	369
	4 PM	7.643%	15,285	255	22,928	382
	5 PM	8.150%	16,299	272	24,449	407
	6 PM	5.959%	11,917	199	17,876	298
	7 PM	3.823%	7,646	127	11,469	191
	8 PM	3.326%	6,652	111	9,978	166
	9 PM	2.119%	4,238	71	6,358	106
	10 PM	1.504%	3,009	50	4,513	75
	11 PM	0.854%	1,707	28	2,561	43

Definitions	
1.01	**Account-based architecture:** The transit fare collection system architecture that uses the back office system to apply relevant business rules, determine the fare, and settle the transaction. The terminal reads information stored on fare payment media and sends it to a back office over a network. The back office determines whether the card is valid and returns an “approve" or "deny” signal that enables the terminal to open the gate or to signal the rider and the bus operator on whether to allow passage.
1.02	**ADA:** The Americans with Disabilities Act of 1990 (and 2008 amendment).
1.03	**Boarding:** The number of times passengers board public transportation vehicles
1.04	**Bytemark Software License Agreement:** A documented agreement that gives Capital Metro a non-exclusive, non-transferable right to use the system applications.
1.05	**Bytemark Agreements:** Bytemark Warranty, Maintenance and Services Agreement (WMA), including at minimum updates to: Scope of Work, App. A - Supported Systems, App. B - Bytemark Contacts, App C - Client Contacts, App E - Performance Management Disincentives and App H - Performance Deficiencies Credits
1.06	**Capital Metropolitan Transportation Authority:** (Used interchangeably with “Capital Metro", “CapMetro”, “The Authority”) the public transportation entity for the Austin metropolitan area.
1.07	**Close Loop Payment and Fare Card:** Closed fare payment system and fare cards that only work within the fare payment system.
1.08	**Contactless Bank Card:** A credit or debit card with an embedded, integrated circuit chip that can make secure payments through a terminal via near field communication.
1.09	**Contract or Contract Documents:** The writings and drawings embodying the legally binding obligations between Capital Metro and the Service Provider for completion of the work.
1.10	**Demand Response:** Public transportation services in which a vehicle is not bound to a predefined route or time schedule.
1.11	**Destination:** The location where a passenger trip ends.
1.12	**Extended Use (EU) smart cards:** Plastic chip cards that are reloadable for extended use as a ticket medium and stored value prepaid card.
1.13	**Fare:** Payment required from each passenger for a ride on any mode of transportation provided by CapMetro.
1.14	**Fare Capping:** Trips are free after a given amount is paid within a given time period
1.15	**Field Integration Testing (FIT):** Testing that is essentially System Integration Testing (SIT) in the field in which the System is exercised in what will become the production environment upon successful completion of the test.
1.16	**Fixed Route:** Public transit service in which a vehicle is operated along predefined routes on a fixed time schedule.
1.17	**Functional Unit Testing (FUT):** Testing of individual units or modules of an application in isolation in order to confirm correct functionality, and compliance with specifications.
1.18	**ISO/IEC-14443 compliant:** International standard that defines proximity cards used for identification and the transmission protocols for communicating with it.
1.19	**Limited Use (LU) paper smart cards:** Paper card with prepaid value that is not reloadable for limited use as a ticket medium.
1.20	**MetroAccess:** Branding of the Capital Metro paratransit transportation service.
1.21	**MIFARE formats:** the latest version of DESFire for EU cards, and the latest version of Ultralight-C for LU fare media.
1.22	**Mode or Service Type:** Capital Metro service types are currently Local, Commuter, and MetroAccess. More information can be found at capmetro.org/fares.
1.23	**Near Field Communications (NFC):** NFC technology is a standards-based wireless communication technology that is built into mobile phones and that allows devices that are a few centimeters apart to exchange data.
1.24	**Open Loop Payment and Fare Card:** Open loop payments and open bank card payments are used synonymously and defined as the use of financial industry-issued credit, debit or prepaid contactless cards (e.g., American Express, Discover, MasterCard, Visa) for fare payment at points of entry/exit to modes of transportation.
1.25	**Origin:** The location where a rider boards a vehicle at the beginning of each ride.
1.26	**Paratransit services:** Pre-booked, origin-to-destination service for qualified individuals who, by way of a disability or medical condition, are functionally unable to use fixed routes some or all of the time. Service Providers operating paratransit vehicles may or may not be dedicated providers.
1.27	**Pass Product:** General term referencing all transit service passes offered by Capital Metro.
1.28	**Passenger type:** A data point mainly differentiating between the ADA-eligible customer, their companions, attendants, children, service animals, etc.
1.29	**Passenger:** Any person being transported. Used interchangeably with “rider” in this document.
1.30	**Payment Card Industry (PCI) standards:** Technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data.
1.31	**Personally Identifiable Information (PII):** Any data that could potentially be used to identify a particular person such as a full name, social security number, driver's license number, bank account number, etc.
1.32	**Quick Read (QR)-Code Ticket:** Transit pass with printed QR code.
1.33	**Reduced Fare:** Eligible passengers who purchase half price fares and are any of the following: Seniors 65 and older; Medicare card holders; Active-duty military personnel; Riders with disabilities.
1.34	**Revenue Vehicle:** A vehicle which transports CapMetro customers. Used interchangeably with "in-service vehicle."
1.35	**Scope of Work:** A section of the Contract consisting of written descriptions of work to be performed or the technical requirements to be fulfilled. Commonly referred to as “Exhibit F” throughout this document.
1.36	**Self-Healing:** A solution which monitors itself for errors and backend efficiency improvements.
1.37	**Shall:** This term will be used throughout this Scope of Services interchangeably to mean “has a duty to”, or “is required to” perform a particular function or task.
1.38	**Stored Value Wallet:** A virtual in-app or physical smart card containing one or more purses which can be loaded and reloaded with value and used to make purchases.
1.39	**System Acceptance Testing (SAT):** Testing, in which all system components must meet or exceed all performance requirements, with the intent to assess acceptability for delivery.
1.40	**System Integration Testing (SIT):** Testing to verify integration of the different system modules and that they are working correctly as a connected whole.
1.41	**Tap On Tap Off Fare:** Fare is charged based on where the passenger boards and disembarks.
1.42	**Title II:** A portion of ADA law which applies to state and local government and ensures that qualified individuals with disabilities receive no discrimination in services, programs, and activities provided by those entities. Applicable here, Capital Metro is required to provide ADA-accessible services and products to its customers and employees.
1.43	**Transfer:** When a passenger switches between routes.
1.44	**Transit Day:** Period of Capital Metro service that extends beyond a normal 24-hour period. A transit day is currently up to 26 hours from 3:00 to 2
1.45	**Vehicle Operator:** Direct-hire employees of the Service Provider with whom Capital Metro contracts service to operate vehicles transporting passengers. Used interchangeably with "driver."

1.46	**Vendor:** The individual, association, partnership, firm, company, corporation, or combination thereof, including joint ventures, contracting with Capital Metro for the delivery of the software solution described under the Contract. Used interchangeably with "Contractor" and "Provider."
1.47	**Virtual Bank Card:** A payment option on a mobile device created through a mobile app or website that creates a temporary or pseudo card number for purchases.
1.48	**Virtual Fare Card:** A ticket medium stored on a mobile device that contains a virtual QR code.
1.49	**WCAG:** The Web Content Accessibility Guidelines are part of a series of web accessibility guidelines published by the Web Accessibility Initiative (WAI) of the World Wide Web Consortium (W3C), the main international standards organization for the Internet.
1.50	**Zone Based Fare:** Fare is charged based on number of geographical “zones” traversed**.**

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

1.1 Definitions. Unless otherwise specified in this Contract (or an Exhibit hereto), the following definitions shall apply, if applicable:

1.1.1 “Acceptance” shall have the meaning set forth in Section 1.4 of this Exhibit.

1.1.2 “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, this Contract, and the parties all as in effect as of the date of this Contract and as amended during the Service Term of this Contract.

1.1.3 “Authority Data” means all data, content and information (i) submitted by or on behalf of the Authority or Customers to the Contractor and all derivative versions of such data, content and information, and any derivative versions thereof, in any form or format.

1.1.4 “Authority Electronic Property” means (i) any websites, servers, hardware, equipment, routers and other system components, software or networks owned or controlled by the Authority, (ii) any Authority mobile device apps, (iii) any interfaces 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.

1.1.5 “Confidential Information” shall have the meaning set forth in Section 2.2 of this Exhibit.

1.1.6 “Contractor’s Certification” shall have the meaning set forth in Section 1.4.3 of this Exhibit.

1.1.7 “Contractor Technology” means all software and hardware as applicable, and any technology, information, content and data, together with Intellectual Property Rights related thereto, owned, developed or used by the Contractor in the creation of the Deliverables and the performance of the Services.

1.1.8 “Deliverable(s)” means all information, data, materials, devices (including equipment and hardware), software, systems, integrations with any software and hardware, interfaces to any software and hardware, system or operating environment (including Authority Electronic Property) and other items to be delivered by the Contractor to the Authority as part of the Services, as specified in the Project Plan.

1.1.9 “Documentation” means the documentation provided to the Authority including, but not limited to, user manuals, system administration manuals, maintenance manuals, diagrams and operator instructions related to the Services furnished by the Contractor to the Authority in any format, including paper and electronic.

1.1.10 “Intellectual Property Rights” means any and all intellectual property rights, including without limitation, invention, patents, patent and patent applications (including all reissues, divisions, renewals, continuations, continuations-in-part, extensions, provisionals and reexaminations) and all rights therein provided by international treaties or conventions and all improvements to the inventions disclosed in each such registration, patent or application, trademarks, service marks, trade dress, logos, slogans, configurations, trade names, corporate names, and business names, whether or not registered, including all common law rights, and registrations and applications for registration thereof, and all rights therein provided by international treaties or conventions, works of authorship and copyrights (registered or otherwise) and registrations and applications for registration thereof, and all rights therein provided by international treaties or conventions, all internet uniform resource locators, and domain names, including any domain name application or registration, all industrial designs and any registration or application thereof anywhere in the world, data and database rights, trade secrets, proprietary know-how and show-how, whether or not reduced, all rights to obtain and rights to apply for patents, and to register trademarks and copyrights, and any similar or equivalent rights to any of the foregoing anywhere in the world.

1.1.11 "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.

1.1.12 "Project" means the project from pre-production launch to pre-final notice related to any Deliverables and Services as described in more detail in this Exhibit.

1.1.13 "Project Plan" means the project plan for the delivery, implementation, customization, configuration and/or installation of any software, hardware and any Deliverables and Services required for the Project, as provided or approved by the Authority.

1.1.14 "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.

1.1.15 "Security Incident(s)" means: (i) the loss or misuse of Authority Data; (ii) the inadvertent, unauthorized, or unlawful processing, alteration, corruption, sale, rental, or destruction of 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 (viii).

1.1.16 "Security Requirements" means 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 from unauthorized access, processing, destruction, modification, distribution and use, as approved in writing by the Authority.

1.1.17 "Service Term" means the term of the contract as set forth in Exhibit A to the Contract.

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

1.1.19 "Technical Specifications" means the technical specifications, functional specifications, descriptions, designs, standards, instructions, and business requirements of the Authority related to the S, as may be further described in this Contract. Unless otherwise agreed upon in writing by the Authority, the Technical Specifications shall be outlined in detail in Exhibit H to this Contract.

1.1.20 "Updates" means all bug fixes, error corrections, patches, updates, upgrades or new releases or version of any software created or acquired by the Contractor and used in provision of the Services during the Service Term.

1.2 Contractor Requirements.

1.2.1 Unless specified in the applicable Project Plan, the Contractor will shall furnish, at its own expense, all resources, personnel, equipment, tools, and supplies necessary for 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 this 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.

1.2.2 The parties agree that the Contractor will not be tasked or responsible for establishing and managing Security Requirements necessary to protect Authority Data integrity in performance of the Services. The Authority agrees that it will be solely responsible for and ensure that all desired Security Requirements necessary to protect Authority Data integrity are established, implemented and managed internally. If requested, however, by the Authority, the Contractor will reasonably cooperate with and assist the Authority and the Authority's other Product contractors to implement security protocols (e.g., firewalls, SSI, McAfee anti-virus, configuring the system for Cisco ICE, configuring the system for the NetScaler application firewall, monthly Microsoft security patches, etc.) and take appropriate actions with respect to any software, hardware and all Authority Data and Authority Electronic Property disclosed or provided to the Contractor so as to enable the Contractor to satisfy its obligations under this Contract and to help prevent the loss, alteration or unauthorized use of the Authority Data and the Authority Electronic Property, to the extent within the Contractor's access, possession or control. 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's, at all times while on-site at the Authority's facilities or remotely accessing the Authority's systems or facilities. In event that the Contractor utilizes computers, laptops or other devices comprising development software, applications or tools in its performance of the Services, Contractor is required to consult in advance of use thereof with Authority and review security measures installed on such computers or devices and sign-off that it will ensure its computers and devices are consistently maintained during the term of this Agreement per Authority with all patches and upgrades at all times to minimize potential induced security issues from such Contractor devices.

1.2.3 The Contractor will perform formal classroom training and provide necessary related documentation, equipment, tools, training aids and other materials, required or requested for the operation and use of the Deliverables and any software and/or hardware, upon initial deployment and during the Service Term, as reasonably requested by the Authority. Such training will be performed on the operating environment at the Authority's facilities (unless otherwise agreed upon by the parties in the Project Plan).

1.2.4 The Contractor and/or its designated third-party auditor(s) will perform all audits necessary to ensure data integrity and adherence to the 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's or its Project contractors.

1.2.5 The Contractor will use commercially reasonable efforts to reasonably assist the Authority, if requested, to adopt and implement all facility and network security, disaster recovery plans and back-up plans as to protect against theft and unauthorized access, disclosure and use of the Authority Data, the Authority Electronic Property and the Authority's Confidential Information, to the extent within the Contractor's access, possession or control, and to ensure the integrity and continuity of the performance of Services and the Project under this Contract and consult and cooperate with the Authority and any contactors it designates, in its performance of these obligations.

1.2.6 The Contractor, as well as its agents, representatives, and employees, shall comply with all of the Authority rules, regulations, and guidelines then in effect when on-site at the Authority and all Applicable Laws.

1.2.7 The Contractor will promptly notify the Authority upon discovering or otherwise learning of any Security Incident involving Authority Data. Following any Security Incident the Contractor will consult in good faith with the Authority regarding Remediation Efforts that may be necessary and reasonable.

1.2.8 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 obligation 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 such Customers and employees to those required by the legal obligation or as pre-approved by the Authority. The Contractor will reasonably cooperate in connection with 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.

1.3 Project Plan and Milestone Deadlines.

1.3.1 The Contractor shall provide Services necessary to assess and evaluate the Authority's business requirements and information technology systems in order to create, deploy, configure, customize, migrate, deliver and/or implement the Services and any software and/or hardware and, if required by the Authority, any Authority Data to be migrated, interfaced to or used in conjunction with the Deliverables. Unless otherwise provided or specified by the Authority, the Contractor will prepare for the Authority's review and approval a Project Plan setting forth in detail (i) the scope of the Project and the Services required to complete the Project, (ii) the milestones and schedule for completing all tasks and requirements for the Project (including the creation, deployment, configuration, customization, migration, delivery and/or implementation of any software, hardware, systems and any Authority Data), (iii) all Authority Electronic Property required for the Contractor to perform the Services, if any, (iv) all Deliverables, and (v) all acceptance criteria, testing and post-implementation tasks. No Project Plan will be effective until approved in writing by the Authority's designated project manager.

1.3.2 This is a fast track Project with completion deadlines that cannot reasonably be extended. For this reason, it is the desire of the Authority to recognize any likely budget overruns as soon as possible, and by this Contract it is employing the Contractor to perform design monitoring, estimating, value analysis and other functions to help the Authority meet the Project budget. At any time that the Contractor develops concerns about the integrity of the budget for the Project, the Contractor shall promptly advise the Authority of the concerns through a variance report, which shall, at a minimum, state: (i) the Contractor's concern; (ii) the apparent cause of the concern, delay, or budgetary issue; (iii) in the event of a concern about a delay, specifically demonstrate the negative impact of the delay to the critical path for the Project Plan; (iv) define any cost impacts to the Project; and (v) provide the Contractor's proposed resolution to the concern. If any estimate submitted to the Authority exceeds previously approved estimates or the Authority's budget, the Contractor shall make appropriate recommendations to the Authority.

1.3.3 If, using reasonable project monitoring techniques, the Contractor determines that it is unlikely or fails to meet a completion date or a cost estimate due under the Project Plan for any reason regardless of which party is at fault, in addition to any other rights and remedies that may be available to the Authority, at no additional cost to the Authority and at the Authority's option, the Contractor shall provide all necessary additional personnel at its own cost to accelerate performance as may be required or necessary to complete the activities required under the Project Plan within a re-adjusted time frame agreed to by both parties in a Change Order. The completion date shall be considered met if completed in accordance with the terms of this Contract within ten (10) working days of the originally estimated completion date. The Contractor will provide the Authority with prior written notice for any delays impacting delivery or other Services completion under the Project Plan in the form of a proposed Change Order.

1.3.4 The Contractor shall use its best efforts, after obtaining explicit consent from the Authority, to re-sequence the Services to overcome and/or mitigate, to the greatest practicable extent, the effect of any delays regardless of the cause of such delays. Without limiting the foregoing, the Contractor shall diligently prosecute its Services in order to meet the proposed start date despite a dispute with the Authority relating in any way to this Contract including, without limitation, any and all the Contractor's claims for modifications to the payments due to the Contractor. The Contractor and the Authority shall cooperate to resolve all disputes and to adjust the Project Plan accordingly by Contract modification in a timely manner (not to exceed two (2) weeks from the date of notice).

1.3.5 Should the Contractor not progress in its performance of Services at a rate commensurate with the Service Term of this Contract, or fail to meet any scheduled date under the Project Plan, the Authority may, in its sole discretion, direct the Contractor to accelerate the Services by employing additional personnel and equipment or providing overtime to existing personnel as is necessary to complete by the start date. Notwithstanding any dispute, controversy, or question that might arise in the interpretation of any provision of this Contract, the performance of any Services, the delivery of any material, the payment of any monies to the Contractor, or otherwise, the Contractor agrees that it will not directly or indirectly stop or delay any Services or part thereof on its part required to be performed, nor will it stop or delay the delivery of any materials on its part required to be furnished for the Deliverables, pending the determination of such dispute or controversy so long as the Authority pays the Contractor for undisputed amounts in accordance with the Contract.

1.4 Acceptance.

1.4.1 Unless otherwise defined or specified in an Exhibit to this Contract, the provisions set forth in this Section 1.4 shall apply to determine the Authority's Acceptance of the Services performed and associated Deliverables.

1.4.2 Implementation shall be completed in a timely manner and appropriate tests conducted by the Authority to facilitate Acceptance of each Deliverable as more fully set forth in this Exhibit and the Project Plan; provided, however, that the Authority may upon written request require that the Contractor perform testing with cooperation of the Authority.

1.4.3 Unless otherwise specified in the Project Plan, within thirty (30) days after installation and testing are completed, the Contractor shall certify in writing that any software, hardware, integration and implementation related to the Services conforms to the Technical Specifications and is capable of being put into full commercial productive use in accordance with the Technical Specifications and otherwise meets the functional and business requirements set forth in this Contract (the "Contractor's Certification"). The Contractor Certification shall not be issued by the Contractor unless the Contractor has completed all tasks required for the delivery, installation, configuration, deployment (including Authority Data migration) and operational testing of any Deliverables, as applicable, and such items are ready for final testing and launch for production use by the Authority.

1.4.4 The Deliverables shall be finally accepted by the Authority when all action items opened from the beginning of the Project through the Warranty Period are closed and each component is fully installed and operational on the Authority's facilities, network, transportation vehicles or operating environment properly configured by the Contractor, and in conformity with the requirements outlined in this Contract ("Acceptance"). The final invoice will not be issued by the Contractor until final Acceptance by the Authority. The Authority reserves the right to modify the Acceptance plan during the implementation process if it is evident that anything related to Acceptance has been missed or are not appropriate for the successful provisioning of any solution.

1.4.5 If there is any objection to Acceptance, the Authority will provide the Contractor with a written notice (the "Defect Notice") reasonably identifying any claimed discrepancies between the actual performance and the requirements set forth in this Contract within reasonable time after the issuance of the Contractor's Certification.

1.4.6 Upon receiving a Defect Notice from the Authority, the Contractor shall confer with the Authority and jointly review each asserted discrepancy to determine if the claimed discrepancy is valid. The Contractor shall promptly correct the discrepancy and resubmit for Acceptance by the Authority for review and testing on the same basis as initially submitted. If, in the reasonable professional judgment of the Contractor such discrepancy is not valid, the Contractor shall so notify the Authority in writing.

1.5 Additional Representations and Warranties. In addition to all other representations, warranties, and covenants included in this Contract, Contractor represents, warrants, and covenants, for itself, its employees, subcontractors and agents that:

1.5.1 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 this Contract or which prohibits Contractor from carrying out its responsibilities under this Contract;

1.5.2 it is fully able to furnish the Services as contemplated by this Contract;

1.5.3 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 this Contract;

1.5.4 it is experienced in the type of 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 Authority project stakeholders within which the Project will be performed;

1.5.5 any software provided or utilized in the Services will not contain any Malware;

1.5.6 the Services and all Deliverables will comply with all Applicable Laws at all times from the date of Acceptance; and

1.5.7 with respect to the Services and all Deliverables there is, and on the date of Acceptance will be, no claim, litigation or proceeding pending or threatened against the Contractor with respect such Services or Deliverables, 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.

1.6 Additional Warranty Remedies. The Authority shall not be entitled to rely on any additional warranties implied by law or regulation. For any breach of the warranties contained in this Section, the Authority's remedy shall be:

1.6.1 For the Services. The satisfactory re-performance of the Services within ten (10) days (or such other reasonable period of time approved by the parties in writing) following the Authority's notice to the Contractor that the Services were not performed satisfactorily in accordance with the Project Plan.

1.6.2 For the Deliverables. The correction of errors or otherwise in the Deliverables that cause breach of the warranty. If the Contractor is unable to provide such error corrections or otherwise make the Deliverables operate as warranted within the periods specified in this Contract, the Authority shall be entitled to terminate this Contract with respect to the affected feature and recover a prorated amount paid to the Contractor based on each feature, which prorated amount will be calculated based on a useful life of five years from the date of final Acceptance. If, however, such errors result in a complete loss of functionality of any Deliverables, then the Authority shall be entitled to terminate this Contract and recover all amounts paid to the Contractor by the Authority in respect of such Deliverable.

1.7 Intellectual Property Rights.

1.7.1 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 and Authority Electronic Property and all Deliverables (excluding the Contractor Technology included in or embodied in the Deliverables), foregoing and all Intellectual Property Rights related thereto ("Authority IP"). Except as expressly authorized in the Exhibit 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 or Authority Electronic Property. The Contractor will not use any Authority Data or Authority Electronic Property in a manner that is harmful to the Authority.

1.7.2 The Contractor grants to the Authority a non-exclusive, perpetual, royalty free, fully paid up, irrevocable, and non-transferable license, in and to any Contractor Technology embodied in the Deliverables for the Authority and service providers (on behalf of the Authority) to exercise and exploit its and their ownership rights in the Deliverables in any manner. The foregoing license does not authorize the Authority to separate any Contractor Technology from the Deliverable in which it is incorporated for creating a standalone product for marketing to others.

1.7.3 For the avoidance of doubt, it is understood that Contractor may use its own previously developed data, documentation, software, ideas, concepts, materials, or information, in whatever form, in performing its obligations hereunder (collectively "Preexisting Works"). All Contractor's Preexisting Works shall remain the sole, exclusive and unrestricted property of Contractor. It is understood that in performing its obligations, Contractor may develop new and unique work products for use in conjunction with this Agreement. For the purpose of this Agreement, "Contractors Work Product" shall mean all data, documentation, software, ideas, concepts, materials, and information, in whatever form, produced or created by Contractor which may or may not relate solely and exclusively to the performance of work or the rendition of obligations under this Agreement (hereinafter "Contractors Work Product"). All Contractors Work Product shall remain the sole, exclusive and unrestricted property of Contractor.

1.7.4 Feedback: Contractor may, at its sole discretion and without restriction, use any feedback, suggestions and ideas ("Feedback") the Authority provides in future modifications of the Contractor’s App. The Authority hereby grants to Contractor the non-exclusive right~~s~~ to use, reproduce, modify, create derivative works from, distribute and display the Feedback in any manner and for any purpose.

1.7.5 Ownership Rights: The ownership rights referenced above in this section include all rights (including title to physical objects) of whatever nature including without limitation any patent, URL website address, software, software design, domain name (whether registered or not), trade secret, trademark or service mark rights (and any goodwill appurtenant thereto), any "moral rights of authors, any rights of publicity, and any right, title and interest in any copyright and any right that may affix under any copyright law now or hereinafter in force and eff etc. This also includes, without condition, limitation or reservation, the rights to copy, add to, subtract from, arrange, rearrange, revise, modify, change and adapt (collectively "Changes"), and the ownership of the results of any of these Changes with regard to the Preexisting Works and Work Products.

1.7.6 Software License. Subject to payment by the Authority in accordance with the Contract, Contractor hereby grants to the Authority: a non-exclusive, non-transferable limited license to use the computer software program licensed under this Contract in machine readable, object code form and any modifications made by Contractor thereto ("Software"), but only in connection with the configuration of the goods and operating system for which the Software is ordered and for the end-use purpose of the operation, maintenance and repair of the Project. The Authority agrees that neither it nor any third party shall modify, reverse engineer, decompile or reproduce the Software, without Contractor’s prior written consent, except for making a single copy for backup or archival purposes in accordance with the related Contractor operating documentation, and provided that Contractor's confidential and proprietary legend is included. Except to the extent that the parties otherwise agree in writing, the Authority’s license to use the copy of such Software shall terminate upon breach of this license or the Contract by the Authority, including, without limitation, breach of payment or confidentiality obligations. All copies of the Software are the property of Contractor, and all copies for which the license is terminated shall be returned to Contractor promptly after termination.

2. Proprietary Information and Non-Disclosure.

2.1 The Contractor acknowledges and agrees that this Contract creates a relationship of confidence and trust on the part of the Contractor for the benefit of the Authority. During the Term of this Contract, the Contractor may acquire certain “Confidential Information” (as defined herein) from or regarding the Authority employees, agents and representatives or documents, or otherwise as a result of performing the Services of the Contractor hereunder.

2.2 “Confidential Information” as used herein, shall mean and include, without limitation:

2.2.1 Any information concerning the Authority or the Project, which is provided by the Authority or any Project team members to the Contractor, such as accounting and financial data, product, marketing, development, pricing and related business plans and budgets, which are not published; and

2.2.2 All Authority Data and Authority Electronic Property; and

2.2.3 All Deliverables (including without limitation all work in progress) and any Contractor Technology included or embodied therein.

2.3 The Contractor acknowledges and agrees that all such Confidential Information is and shall be deemed the sole, exclusive, confidential and proprietary property and trade secrets of the Authority at all times during the Service Term of this Contract and following any expiration or termination hereof. The Contractor agrees to hold in confidence without disclosing or otherwise using any Confidential Information, except as such disclosure or use may be required in connection with and limited to the Services of the Contractor hereunder or as otherwise permitted under this Contract.

2.4 The Contractor acknowledges and agrees that the Authority would not have entered into this Contract unless the Authority was assured that all such Confidential Information would be held in confidence by the Contractor in trust for the sole benefit of the Authority.

2.5 The Contractor shall not improperly use or disclose any proprietary information or trade secrets of any third party and will not bring on to the premises of the Authority any unpublished documents or any property belonging to any third party unless consented to in writing by the third party.

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

2.7 The Authority shall have the perpetual and unrestricted right to use, copy, and incorporate into other works all reports, materials, presentations and other work product prepared by the Contractor and delivered to the Authority.

2.8 Upon any termination or expiration of this Contract, the Contractor agrees to deliver to the Authority any and all Confidential Information except that the Contractor may keep one file copy of any Confidential Information pertinent to its rights and obligations surviving the expiration or termination of this Contract, which copy shall be held in confidence in accordance with this Section.

3. 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 the Authority Data or Authority Electronic Property for any activity unrelated to the express business purposes and interests of the Authority under this Contract, without the prior written consent of the Authority.

4. Specific Performance. The Contractor acknowledges and agrees that the remedy at law for the breach of provisions of this Contract (particularly with respect to ownership of intellectual property and Confidential Information) may be inadequate and that the Authority may be entitled to injunctive relief without bond, in addition to any other rights or remedies which the Authority may have for such breach.

5. **INDEMNIFICATION. IN ADDITION TO GENERAL INDEMNIFICATION SET FORTH ELSEWHERE IN THE CONTRACT, THE FOLLOWING INDEMNIFICATION OBLIGATIONS SHALL APPLY:**

5.1 **THE CONTRACTOR SHALL INDEMNIFY, DEFEND AND HOLD HARMLESS THE AUTHORITY AND ITS AFFILIATES AND THEIR TRUSTEES, DIRECTORS, OFFICERS, EMPLOYEES, CUSTOMERS AND AGENTS FROM AND AGAINST ANY AND ALL DAMAGES OF ANY NATURE OR KIND TO THE EXTENT ARISING OUT OF, CAUSED BY, OR RESULTING FROM: (I) ANY BODILY INJURY OR DEATH OF ANY PERSON INCURRED BY THE AUTHORITY OR ANY THIRD PARTY RESULTING FROM THE NEGLIGENCE OR WILLFUL MISCONDUCT OF THE CONTRACTOR OR ITS EMPLOYEES, CONTRACTORS OR REPRESENTATIVES; (II) ANY FAILURE OF THE SERVICES OR DELIVERABLES TO CONFORM WITH APPLICABLE LAWS OR THE TECHINCAL SPECIFICATIONS OR OTHER REQUIREMENTS SET FORHT IN THIS CONTRACT; (III) ANY SECURITY INCIDENT; AND (IV) ANY ACTUAL OR ALLEGED VIOLATION, INFRINGEMENT OR MISAPPROPRIATION OF ANY COPYRIGHT, PATENT, TRADEMARK, TRADE SECRET, PRODUCT NAME, RIGHT OF PRIVACY OR PERSONA OR OTHER INTELLECTUAL PROPERTY RIGHT AND PROPRIETARY RIGHT OF A THIRD PARTY RELATED TO THE SERVICES AND DELIVERABLES REGARDLESS OF WHETHER OR NOT SUCH CLAIM, DAMAGE, LOSS, OR EXPENSE IS CAUSED IN PART BY ANY INDEMNITEE. IN PARTICULAR, THE CONTRACTOR ACKNOWLEDGES THAT THE CONTRACTOR'S OBLIGATION TO IDEMNIFY THE AUTHORITY EXTENDS TO ANY LIABILITY ARISING OUT OF ANY ACTUAL NEGLIGENCE BY THE CONTRACTOR IN THE DELIVERY OF ANY PRODUCTS OR SERVICES UNDER THIS CONTRACT. NOTWITHSTANDING THE FOREGOING, THE CONTRACTOR SHALL NOT BE LIABLE TO AN INDEMNITEE FOR ANY LOSSES INCURRED BY SUCH INDEMNITEE TO THE EXTENT SUCH CLAIM IS ATTRIBUTABLE SOLELY TO THAT INDEMNITEE'S SOLE NEGLIGENCE.**

5.2 **IF THE DELIVERABLES ARE HELD TO INFRINGE OR IT IS BELIEVED BY THE AUTHORITY TO INFRINGE THE RIGHTS OF OTHERS, THE CONTRACTOR'S WILL, AT ITS EXPENSE AND UPON**

THE AUTHORITY'S REQUEST, TO: (I) MODIFY THE INFRINGING ITEM TO BE NON-INFRINGING SO LONG AS THE UTILITY OR PERFORMANCE OF THE DELIVERABLES ARE NOT MATERIALLY IMPAIRED AND THE DELIVERABLES CONTINUE TO CONFORM TO THE TECHNICAL SPECIFICATIONS AND THE AUTHORITY'S ORIGINAL REQUIREMENTS IN ALL RESPECTS, SUBJECT TO THE AUTHORITY'S APPROVAL; OR (II) OBTAIN FOR THE AUTHORITY A LICENSE TO CONTINUE USING THE INFRINGING ITEM.

5.3 **THE INDEMNITY OBLIGATIONS CONTAINED IN THIS SECTION SHALL SURVIVE THE TERMINATION, SUSPENSION, ABANDONMENT AND/OR COMPLETION OF THIS CONTRACT.**

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

7. Waivers. No failure by the Authority to insist upon the performance by the Contractor of any provision of this Contract, and no failure of the Authority to exercise any right or remedy consequent upon a breach or other default, and no payment by the Authority or its use of the Project during the continuance of any breach or other default, shall constitute a waiver of the Contractor's breach or default or of any provision of this Contract.

8. UCITA. Neither the Uniform Computer Information Transactions Act nor any state laws incorporating such Act apply to this Contract or the transactions contemplated hereunder.

9. Warranty Disclaimer. The parties hereto acknowledge that the Service depends upon data being transmitted over the Internet, customer's network, GPS satellites, and third-party carrier networks, and as Contractor has no control over the functioning of the Internet, the work and Services offered are offered an "as-available" basis.

10. Data Privacy. The Contractor may have access to personally identifiable information ("PII") in connection with the performance of the Agreement. PII is 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. The Contractor shall take reasonable steps maintain the confidentiality, security, safety, and integrity of all Customer PII, Notwithstanding the above, the Parties hereby expressly acknowledge and agree that Contractor shall not be responsible for any security for the transmission of data over the internet, payment processing or credit or debit card transactions or the data security or data privacy associated with the services of third-party vendors performing payment processing, hosting, or cloud vendor services. Notwithstanding the foregoing, Contractor will adhere to the following requirements concerning Customer PII:

    A. The Contractor shall take reasonable steps to maintain the confidentiality of and will not reveal or divulge to any person or entity any Customer PII that becomes known to it during the term of this Agreement.
    B. The Contractor must maintain policies and programs that prohibit unauthorized disclosure of Customer PII by its employees and sub-Contractors and promote training and awareness of information security policies and practices. The Contractor must comply, and must cause its employees, representatives, agents, and sub-Contractors to comply, with such commercially and operationally reasonable directions as the Authority may make to promote the safeguarding or confidentiality of Customer PII.
    C. The Contractor must conduct background checks for employees or sub-Contractors that have access to Customer PII or systems hosting Customer PII.
    D. The Contractor must limit access to computers and networks that host Customer PII, including without limitation through user credentials and strong passwords, data encryption both during transmission and at rest, firewall rules, and network-based intrusion detection systems.

This Section will survive termination or expiration of this Agreement.

11. Data Security. Contractor shall take reasonable steps to maintain the confidentiality, security, safety, and integrity of the Authority's data. Notwithstanding any other provision of this agreement (including the indemnity

in Section 5.1), the Parties hereby expressly acknowledge and agree that Contractor shall not be responsible for any security for the transmission of data over the internet, payment processing or credit or debit card transactions or the data security or data privacy associated with the services of third-party vendors performing payment processing, hosting, or cloud vendor services. This section will survive the termination of this Agreement.