



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

Regular Meeting of the Board of Directors

9:00 a.m.

Wednesday, October 25, 2023

Lowell H. Lebermann, Jr., Board Room
3300 N. IH-35, Suite 300
Austin, Texas 78705

*A live video stream of this meeting may be viewed on the internet at
www.mobilityauthority.com*

Persons with disabilities. If you plan to attend this meeting and may need auxiliary aids or services, such as an interpreter for those who are deaf or hearing impaired, or if you are a reader of large print or Braille, please contact Laura Bohl at (512) 996-9778 at least two days before the meeting so that appropriate arrangements can be made.

Español. Si desea recibir asistencia gratuita para traducir esta información, llame al (512) 996-9778.

AGENDA

No action on the following:

1. Welcome and opportunity for public comment – See **Notes** at the end of this agenda.

Convene the Audit Committee Meeting

2. Audit Committee Meeting
 - A. Audit Committee meeting called to order by Committee Chairman Singleton.
 - B. Introduction of external auditors from RSM US LLP.
 - C. Discuss, consider, and take appropriate action to accept the Fiscal Year 2023 Audit Reports.
 - D. Adjourn Audit Committee.

Consent Agenda

See **Notes** at the end of this agenda.

3. Approve the minutes from the September 27, 2023 Regular Board Meeting.
4. Prohibit the operation of certain vehicles on Mobility Authority toll facilities pursuant to the Habitual Violator Program.

Regular Items

Items to discuss, consider, and take appropriate action.

5. Accept the unaudited financial statements for August and September 2023.
6. Discuss and consider amending the Mobility Authority Policy Code § 301.002 to modify the minimum toll rates for the Mopac Express Lanes and adding a new Mobility Authority Policy Code § 301.0075 regarding Prepaid License Plate Billing.
7. Discuss and consider modifying the annual toll rate escalation becoming effective January 1, 2024 and possible action if necessary.
8. Discuss and consider adopting the five-year capital plan.
9. Discuss and consider approving an interlocal agreement with the Cameron County Regional Mobility Authority for transaction processing services.
10. Discuss and consider approving a contract with Kapsch TrafficCom USA, Inc. to provide intelligent transportation system performance-based maintenance services for the Mobility Authority's toll system.
11. Discuss and consider approving a contract with Deloitte Consulting, LLP for enhancement development of the Mobility Authority's Data Platform System.

Briefings and Reports

Items for briefing and discussion only. No action will be taken by the Board.

12. Quarterly Updates.
 - A. 183A Phase III Project
 - B. 183 North Mobility Project
 - C. Barton Skyway Ramp Relief Project

13. Executive Director Report.
 - A. IBTTA Annual Meeting.
 - B. Agency performance metrics.
 - i. Roadway Performance
 - ii. Call-Center Performance

Executive Session

Under Chapter 551 of the Texas Government Code, the Board may recess into a closed meeting (an executive session) to deliberate any item on this agenda if the Chairman announces the item will be deliberated in executive session and identifies the section or sections of Chapter 551 that authorize meeting in executive session. A final action, decision, or vote on a matter deliberated in executive session will be made only after the Board reconvenes in an open meeting.

The Board may deliberate the following items in executive session if announced by the Chairman:

14. Discuss the exchange or purchase of one or more parcels or interests in real property owned by the Mobility Authority and related legal issues as authorized by §551.071 (Consultation with Attorney) and §551.072 (Deliberation Regarding Real Property).
15. Discuss legal issues related to claims by or against the Mobility Authority; pending or contemplated litigation and any related settlement offers; or other matters as authorized by §551.071 (Consultation with Attorney).
16. Discuss legal issues relating to procurement and financing of Mobility Authority transportation projects and toll system improvements, as authorized by §551.071 (Consultation with Attorney).
17. Discuss personnel matters as authorized by §551.074 (Personnel Matters).

Reconvene in Open Session.

Regular Items

Items to discuss, consider, and take appropriate action.

18. Adjourn meeting.

Notes

Opportunity for Public Comment. At the beginning of the meeting, the Board provides a period of up to one hour for public comment on any matter subject to the Mobility Authority's jurisdiction. Each speaker is allowed a maximum of three minutes. A person who wishes to address the Board must register in advance and provide the speaker's name, address, phone number and email, as well as the agenda item number and whether you wish to speak during the public comment period or during the agenda item. If a speaker's topic is not listed on this agenda, the Board may not deliberate the speaker's topic or question the speaker during the open comment period but may direct staff to investigate the matter or propose that an item be placed on a subsequent agenda for deliberation and possible action by the Board. The Board may not deliberate or act on an item that is not listed on this agenda.

Consent Agenda. The Consent Agenda includes routine or recurring items for Board action with a single vote. The Chairman or any Board Member may defer action on a Consent Agenda item for discussion and consideration by the Board with the other Regular Items.

Public Comment on Agenda Items. A member of the public may offer comments on a specific agenda item in open session if he or she signs the speaker registration sheet for that item before the Board takes up consideration of the item. The Chairman may limit the amount of time allowed for each speaker. Public comment unrelated to a specific agenda item must be offered during the open comment period.

Meeting Procedures. The order and numbering of agenda items is for ease of reference only. After the meeting is convened, the Chairman may rearrange the order in which agenda items are considered, and the Board may consider items on the agenda in any order or at any time during the meeting.

Participation by Telephone Conference Call. One or more members of the Board of Directors may participate in this meeting through a telephone conference call, as authorized by Sec. 370.262, Texas Transportation Code (*see below*). Under that law, each part of the telephone conference call meeting that by law must be open to the public, shall be audible to the public at the meeting location, and will be tape-recorded or documented by written minutes. On conclusion of the meeting, the tape recording or the written minutes of the meeting will be made available to the public.

TEXAS TRANSPORTATION CODE Sec. 370.262. MEETINGS BY TELEPHONE CONFERENCE CALL.

(a) Chapter 551, Government Code, does not prohibit any open or closed meeting of the board, a committee of the board, or the staff, or any combination of the board or staff, from being held by telephone conference call. The board may hold an open or closed meeting by telephone conference call subject to the requirements of Sections 551.125(c)-(f), Government Code, but is not subject to the requirements of Subsection (b) of that section.

(b) A telephone conference call meeting is subject to the notice requirements applicable to other meetings.

(c) Notice of a telephone conference call meeting that by law must be open to the public must specify the location of the meeting. The location must be a conference room of the authority or other facility in a county of the authority that is accessible to the public.

(d) Each part of the telephone conference call meeting that by law must be open to the public shall be audible to the public at the location specified in the notice and shall be tape-recorded or documented by written minutes. On conclusion of the meeting, the tape recording or the written minutes of the meeting shall be made available to the public.

TEXAS GOVERNMENT CODE Sec. 551.125. OTHER GOVERNMENTAL BODY. (a) Except as otherwise provided by this subchapter, this chapter does not prohibit a governmental body from holding an open or closed meeting by telephone conference call.

~~(b) A meeting held by telephone conference call may be held only if:~~

- ~~(1) an emergency or public necessity exists within the meaning of Section 551.045 of this chapter; and~~
- ~~(2) the convening at one location of a quorum of the governmental body is difficult or impossible; or~~
- ~~(3) the meeting is held by an advisory board.~~

(c) The telephone conference call meeting is subject to the notice requirements applicable to other meetings.

(d) The notice of the telephone conference call meeting must specify as the location of the meeting the location where meetings of the governmental body are usually held.

(e) Each part of the telephone conference call meeting that is required to be open to the public shall be audible to the public at the location specified in the notice of the meeting as the location of the meeting and shall be tape-recorded. The tape recording shall be made available to the public.

Mobility Authority Board Meeting Agenda
Wednesday, October 25, 2023

(f) The location designated in the notice as the location of the meeting shall provide two-way communication during the entire telephone conference call meeting and the identification of each party to the telephone conference shall be clearly stated prior to speaking.



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #1

Welcome and opportunity for public
comment

Welcome and opportunity for public comment.
No Board action required.



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #2

Accept the Independent Audit Reports
from RSM US LLP for the Fiscal Year
Ending June 30, 2023

Strategic Plan Relevance: Stewardship
Department: Finance
Contact: José Hernández, Chief Financial Officer
Associated Costs: N/A
Action Requested: Consider and act on the draft resolution

Background: Each year the Mobility Authority engages an independent CPA firm to conduct the Authority's required annual audit and single audit. RSM US LLP has completed the annual audit for FY 2023 and will present those reports to the Audit Committee. The draft Resolution accepts the annual audits for FY 2023.

Audit Committee - Agenda:

- A. Audit Committee meeting called to order by Committee Chairman Singleton.
- B. Introduction of external auditors from RSM US LLP.
- C. Discuss, consider, and take appropriate action to accept the Fiscal Year 2023 Audit Reports.
- D. Adjourn Audit Committee.

Action requested/Staff Recommendation: Staff recommends the Board accept the annual audits for FY 2023.

Backup provided: FY 2023 Audit Reports to be provided at the Board Meeting

**MEETING OF THE AUDIT COMMITTEE
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**

RESOLUTION NO. 23-0XX

**ACCEPTING THE INDEPENDENT AUDIT REPORTS FROM RSM US LLP
FOR THE FISCAL YEAR ENDING JUNE 30, 2023**

WHEREAS, by Resolution No. 09-50 enacted July 31, 2009, the Board of Directors established the Audit Committee as a standing committee of the Board of Directors, consisting of all of the members of the Board of Directors; and

WHEREAS, under Resolution No. 09-50 and Section 101.036 of the Mobility Authority Policy Code, the Audit Committee is authorized to exercise all powers and authority of the Board of Directors with respect to Mobility Authority finances, and accordingly acts as, and on behalf of, the Board of Directors with respect to the matters addressed by this resolution; and

WHEREAS, the firm of RSM US LLP, has been engaged to provide an independent audit of the finances of the Central Texas Regional Mobility Authority for the fiscal year ending on June 30, 2023, and has presented that audit to the Audit Committee; and

WHEREAS, the Audit Committee has reviewed the “Report to the Board of Directors” and the “Basic Financial Statements” prepared by RSM US LLP, attached respectively as Exhibits A and B to this resolution, and has heard and considered the presentation on the audit by RSM US LLP.

NOW THEREFORE, BE IT RESOLVED, that the Audit Committee accepts the independent audit reports of the Central Texas Regional Mobility Authority prepared by RSM US LLP for the fiscal year ending on June 30, 2023; and

BE IT FURTHER RESOLVED that this resolution constitutes approval by the Audit Committee of the investment reports required by 43 *Texas Administrative Code* Rule §26.61(b).

Adopted by the Audit Committee of the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

David Singleton
Chairman, Audit Committee

Exhibit A

Report to the Board of Directors

(To be provided at the Board Meeting)

Exhibit B

Basic Financial Statements

(To be provided at the Board Meeting)



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #3

Approve the minutes from the
September 27, 2023 Regular Board
Meeting

Strategic Plan Relevance: Service
Department: Legal
Contact: Geoff Petrov, General Counsel
Associated Costs: N/A
Funding Source: N/A
Action Requested: Consider and act on motion to approve minutes

Description/Background: Approve the attached draft minutes for the September 27, 2023, Regular Board Meeting.

Backup provided: Draft minutes September 27, 2023, Regular Board Meeting

MINUTES
Regular Meeting of the Board of Directors of the
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY

Wednesday, September 27, 2023
9:00 a.m.

This was an in-person meeting. Notice of the meeting was posted September 22, 2023, online on the website of the Mobility Authority and in the Mobility Authority's office lobby at 3300 N. Interstate 35, #300, Austin, Texas 78705-1849. Chairman Jenkins, Board Members David Armbrust, Mike Doss, Heather Gaddes, and Ben Thompson were present and Vice Chair Nikelle Meade and David Singleton joined remotely over audio.

**An archived copy of the live-streamed audio of this
meeting is available at:**

<https://mobilityauthority.new.swagit.com/videos/272676>

After noting that a quorum of the Board was present, Chairman Jenkins called the meeting to order at 9:06 a.m. and had each Board Member state their name for the record.

1. Welcome and opportunity for public comment.

Bobby Levinski, Save Our Springs, provided public comment following the Executive Director Report.

Consent Agenda

2. Approve the minutes from the August 16, 2023 Regular Board Meeting and the September 20, 2023 Board Workshop.
3. Prohibit the operation of certain vehicles on Mobility Authority toll facilities pursuant to the Habitual Violator Program.

ADOPTED AS: RESOLUTION NO. 23-032

4. Approve a contract with Dan Williams Company for metal beam guard fence replacement on the 183A Toll facility.

ADOPTED AS: RESOLUTION NO. 23-033

MOTION: Approve Item Nos. 2 thru 4.

RESULT: Approved (Unanimous); 7-0

MOTION: Mike Doss
SECONDED BY: Heather Gaddes
AYE: Armbrust, Doss, Gaddes, Jenkins, Meade, Singleton,
Thompson
NAY: None.

Regular Items

5. Accept the unaudited financial statements for July 2023.

Presentation by Jose Hernandez, Chief Financial Officer.

MOTION: Accept the unaudited financial statements for July 2023.
RESULT: Approved (Unanimous); 7-0
MOTION: David Singleton
SECONDED BY: Ben Thompson
AYE: Armbrust, Doss, Gaddes, Jenkins, Meade, Singleton,
Thompson
NAY: None.

ADOPTED AS: RESOLUTION NO. 23-034

6. Discuss and take appropriate action regarding a cost-of-living adjustment for Mobility Authority retirees.

Presentation by Jose Hernandez, Chief Financial Officer.

MOTION: Adopt the 100% CPI-U COLA to be effective January 1,
2024.
RESULT: Approved (Unanimous); 7-0
MOTION: Mike Doss
SECONDED BY: Ben Thompson
AYE: Armbrust, Doss, Gaddes, Jenkins, Meade, Singleton,
Thompson
NAY: None.

ADOPTED AS: RESOLUTION NO. 23-035

7. Discuss and consider approving a contract with Deloitte Consulting, LLP for toll operations and maintenance services related to the Mobility Authority's Data Platform System.

Presentation by Greg Mack, Director of Information Technology.

MOTION: Approve a contract with Deloitte Consulting, LLP for toll operations and maintenance services related to the Mobility Authority's Data Platform System.

RESULT: Approved (Unanimous); 7-0

MOTION: Heather Gaddes

SECONDED BY: David Armbrust

AYE: Armbrust, Doss, Gaddes, Jenkins, Meade, Singleton, Thompson

NAY: None.

ADOPTED AS: RESOLUTION NO. 23-036

8. Approve the annual cybersecurity training compliance report for submittal to the Texas Department of Information Resources as required by Texas Government Code §2054.5191.

Presentation by Greg Mack, Director of Information Technology.

MOTION: Approve the annual cybersecurity training compliance report for submittal to the Texas Department of Information Resources as required by Texas Government Code §2054.5191.

RESULT: Approved (Unanimous); 7-0

MOTION: Mike Doss

SECONDED BY: Ben Thompson

AYE: Armbrust, Doss, Gaddes, Jenkins, Meade, Singleton, Thompson

NAY: None.

ADOPTED AS: RESOLUTION NO. 23-037

9. Approve a contract with Dan Williams Company for construction of the County Line Road Project funded by Travis County.

Presentation by Mike Sexton, Acting Director of Engineering.

MOTION: Approve a contract with Dan Williams Company for construction of the County Line Road Project funded by Travis County.

RESULT: Approved (Unanimous); 7-0

MOTION: David Armbrust

SECONDED BY: Heather Gaddes

AYE: Armbrust, Doss, Gaddes, Jenkins, Meade, Singleton,
Thompson
NAY: None.

ADOPTED AS: RESOLUTION NO. 23-038

Briefings & Reports

10. Executive Director Report.

Presentation by James Bass, Executive Director.

- A. Agency performance metrics.
 - i. Roadway Performance
 - ii. Call-Center Performance

Executive Session

Chairman Jenkins announced there would be no Executive Session.

- 11. Discuss the sale, transfer or exchange of one or more parcels or interests in real property owned by the Mobility Authority and related legal issues as authorized by §551.071 (Consultation with Attorney) and §551.072 (Deliberation Regarding Real Property; Closed Meeting).
- 12. Discuss legal issues related to claims by or against the Mobility Authority; pending or contemplated litigation and any related settlement offers; or other matters as authorized by §551.071 (Consultation with Attorney).
- 13. Discuss legal issues relating to procurement and financing of Mobility Authority transportation projects, as authorized by §551.071 (Consultation with Attorney).
- 14. Discuss personnel matters as authorized by §551.074 (Personnel Matters).

Regular Items

After confirming that no member of the public wished to address the Board, Chairman Jenkins declared the meeting adjourned at 10:16 a.m.

15. Adjourn.



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #4

Prohibit the operation of certain
vehicles on Mobility Authority toll
facilities pursuant to the Habitual
Violator Program

Strategic Plan Relevance:	Stewardship & Service
Department:	Operations
Contact:	Tracie Brown, Director of Operations
Associated Costs:	N/A
Funding Source:	N/A
Action Requested:	Consider and act on draft resolution

Project Description/Background: The Mobility Authority's habitual violator process prescribes two notices before habitual violator remedies go into effect. A pre-determination letter is sent 60 days before any remedies are enforced advising the customer again of their outstanding balance and providing an opportunity for resolution. Assuming no resolution, a *Notice of Determination* is mailed notifying the customer they've been determined to be a habitual violator and advising of the consequences. The customer is also informed of their right to appeal the decision and the process by which to do so.

If the customer does not contact the Authority to appeal the habitual violator determination or resolve their outstanding balance, a block is placed on the related vehicle's registration preventing renewal. The block remains in effect until all tolls and fees have been paid, a payment plan has been arranged with the Mobility Authority or the customer is determined to no longer be a habitual violator.

Previous Actions & Brief History of the Program/Project: State law provides that persons deemed to be habitual violators may also be prohibited from use of the Mobility Authority's toll facilities by order of the Board of Directors. Habitual violator customers operating a vehicle in violation of a ban are subject to a Class C misdemeanor with a fine up to \$500. A second or subsequent occurrence may result in impoundment of the vehicle. Similar to registration blocks, vehicle bans remain in effect until all

outstanding amounts owed to the Authority have been resolved or the customer is no longer deemed a habitual violator.

Financing: Not applicable.

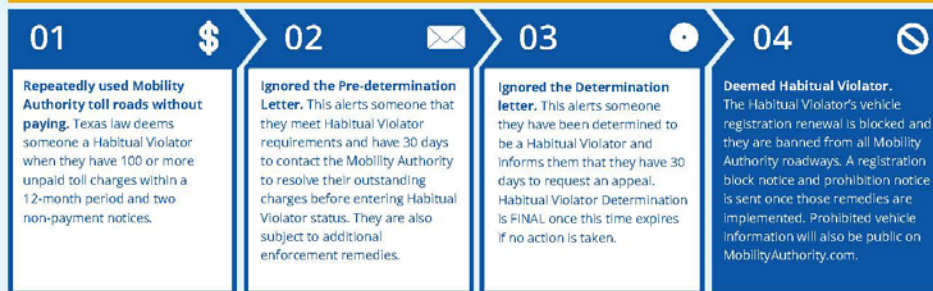
Action requested/Staff Recommendation: Staff affirms that all required steps have been followed and proper notice previously provided to customers determined to be habitual violators. To date, these customers have not appealed this determination or resolved their outstanding balances.

Therefore, staff recommends that the Board of Directors approve the order prohibiting certain vehicles from use of the Authority's toll facilities. Following the Board's approval of this order, a Notice of Prohibition will be mailed by first class mail advising of the ban, consequences if the ban is violated and how the customer may resolve their outstanding balance.

Backup provided: Habitual Violator Vehicle Ban FAQs
Draft Resolution



Habitual Violator Process



Who is a Habitual Violator?

A Habitual Violator is defined in Section 372.106(a) of the Texas Transportation Code as (A) one who was issued at least two written notices of nonpayment that contained in aggregate 100 or more events of nonpayment within a period of one year and, (B) was issued a warning that failure to pay the amounts specified in the notices may result in the toll project entity's exercise of Habitual Violator remedies.

What enforcement remedies is the Mobility Authority implementing for Habitual Violators?

To encourage equitable payment by all customers, legislation allows for enforcement remedies up to and including vehicle registration renewal blocks, prohibiting Habitual Violator's vehicles on Mobility Authority roadways, on-road enforcement of the vehicle ban, as well as posting names to the agency website of those Habitual Violators with banned vehicles. The Mobility Authority will be implementing these remedies beginning November 2019.

How will I know I'm a Habitual Violator subject to enforcement remedies?

Habitual Violators are provided due process protections prior to any enforcement action.

- A registered vehicle owner who the Mobility Authority determines meets the Habitual Violator status is sent a letter advising them that Habitual Violator remedies may be implemented if the customer's outstanding balance is not resolved. This letter is not required by law but is sent as a courtesy to reflect the Mobility Authority's commitment to the customer.
- A registered vehicle owner who the Mobility Authority determines to be a Habitual Violator receives written notice of that determination and an opportunity for a justice of the peace hearing to challenge their Habitual Violator status.
- Habitual Violator Determination is FINAL if no action is taken, prompt in the Mobility Authority to send a Vehicle Registration Block Notice and/or a Vehicle Ban Notice. These notices urge the Habitual Violator yet again to resolve their toll debt with the Mobility Authority.
- Sufficient time is provided to respond to all notifications.

Learn more about the Habitual Violator Enforcement Program at MobilityAuthority.com



How can I resolve my Habitual Violator status and settle my toll bill balance?

You can pay outstanding tolls and administrative fees with cash, money order or credit card (a payment plan may be available) by: calling the Mobility Authority Customer Service Center at 512-410-0562, online at www.paymobilitybill.com, or in person at our walk-up center.

Why is the Mobility Authority pursuing enforcement remedies?

The vehicle registration block and other toll enforcement actions are intended to encourage tollway drivers to pay for services rendered to ensure fairness to the overwhelming majority of drivers who pay for the service, maintenance and safety of the toll roads.

How will a person be notified that he or she is subject to enforcement remedies?

A notification letter announcing that a person has met the criteria of Habitual Violator is sent to the address in the Texas Department of Motor Vehicles (TTC 372.106) database, allowing 30 days to contact to dispute their determination as a Habitual Violator or address the account balance before remedies are applied. If the Habitual Violator does not make arrangements with the Mobility Authority during this period, they will be subject to all enforcement remedies. Additionally, notification of a registration renewal block is mailed.

Can someone dispute a toll bill?

Yes. You may contact the Mobility Authority to review all outstanding tolls and fees, correct any errors and arrange for payment to clear your status as a Habitual Violator and the block on your registration. Habitual Violators are also given an opportunity to request an administrative hearing with a justice of the peace.

How will I know or be notified that I am subject to a vehicle ban?

Habitual violators subject to vehicle ban will receive notification that they have been banned, including when the ban will take effect and instructions for how to remove their status as a Habitual Violator.

Can I dispute my toll bill that subjects me to the vehicle ban?

Yes. You may contact the Mobility Authority to review all outstanding tolls and administrative fees, correct any errors and arrange for payment to clear your status as a Habitual Violator and remove the vehicle ban.

What happens if I am banned, but get caught driving on a Mobility Authority toll road?

A person commits an offense when operating a vehicle in violation of the ban and is subject to a Class C misdemeanor with a fine up to \$500. A second or subsequent occurrence of driving on the tollway in violation of a ban may result in impoundment of the vehicle.

How will the Mobility Authority know if I'm still driving (after being banned)?

Mobility Authority roads are equipped with technology that recognizes vehicle and license plates on our prohibited list. Individuals operating a prohibited vehicle on Mobility Authority roads will be reported to nearby law enforcement patrolling Mobility Authority roads.

**GENERAL MEETING OF THE BOARD OF DIRECTORS
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**

RESOLUTION NO. 23-0XX

**PROHIBITING THE OPERATION OF CERTAIN MOTOR VEHICLES
ON MOBILITY AUTHORITY TOLL FACILITIES PURSUANT TO
THE HABITUAL VIOLATOR PROGRAM**

WHEREAS, Transportation Code, Chapter 372, Subchapter C, authorizes toll project entities, including the Central Texas Regional Mobility Authority (Mobility Authority), to exercise various remedies against certain motorists with unpaid toll violations; and

WHEREAS, Transportation Code §372.106 provides that a “habitual violator” is a registered owner of a vehicle who a toll project entity determines:

(1) was issued at least two written notices of nonpayment that contained:

(A) in the aggregate, 100 or more events of nonpayment within a period of one year, not including events of nonpayment for which: (i) the registered owner has provided to the toll project entity information establishing that the vehicle was subject to a lease at the time of nonpayment, as provided by applicable toll project entity law; or (ii) a defense of theft at the time of the nonpayment has been established as provided by applicable toll project entity law; and

(B) a warning that the failure to pay the amounts specified in the notices may result in the toll project entity’s exercise of habitual violator remedies; and

(2) has not paid in full the total amount due for tolls and administrative fees under those notices; and

WHEREAS, the Mobility Authority previously determined that the individuals listed in Exhibit A are habitual violators, and these determinations are now considered final in accordance with Transportation Code, Chapter 372, Subchapter C; and

WHEREAS, Transportation Code §372.109 provides that a final determination that a person is a habitual violator remains in effect until (1) the total amount due for the person’s tolls and administrative fees is paid; or (2) the toll project entity, in its sole discretion, determines that the amount has been otherwise addressed; and

WHEREAS, Transportation Code §372.110 provides that a toll project entity, by order of its governing body, may prohibit the operation of a motor vehicle on a toll project of the entity if:

(1) the registered owner of the vehicle has been finally determined to be a habitual violator; and

(2) the toll project entity has provided notice of the prohibition order to the registered owner; and

WHEREAS, the Executive Director recommends that the Board prohibit the operation of the motor vehicles listed in Exhibit A on the Mobility Authority's toll roads, including (1) 183A Toll; (2) 290 Toll; (3) 71 Toll; (4) MoPac Express Lanes; (5) 45SW Toll; and (6) 183 Toll.

NOW THEREFORE, BE IT RESOLVED that the motor vehicles listed in Exhibit A are prohibited from operation on the Mobility Authority's toll roads, effective October 25, 2023; and

BE IT FURTHER RESOLVED that the Mobility Authority shall provide notice of this resolution to the individuals listed in Exhibit A, as required by Transportation Code §372.110; and

BE IT IS FURTHER RESOLVED that the prohibition shall remain in effect for the motor vehicles listed in Exhibit A until the respective habitual violator determinations are terminated, as provided by Transportation Code §372.110.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

Robert W. Jenkins, Jr.
Chairman, Board of Directors

Exhibit A

LIST OF PROHIBITED VEHICLES

(To be provided at the Board Meeting)



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #5

Accept the unaudited financial
statements for August 2023 and
September 2023

Strategic Plan Relevance: Stewardship
Department: Finance
Contact: José Hernández, Chief Financial Officer
Associated Costs: N/A
Funding Source: N/A
Action Requested: Consider and act on draft resolution

Project Description/Background: Presentation and acceptance of the unaudited financial statements for August 2023 and September 2023.

Previous Actions & Brief History of the Program/Project: N/A

Financing: N/A

Action requested/Staff Recommendation: Accept the financial statements for August 2023 and September 2023.

Backup provided: Draft Resolution
Draft financial statements for August 2023
and September 2023

**MEETING OF THE BOARD OF DIRECTORS
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**

RESOLUTION NO. 23-0XX

**ACCEPT THE UNAUDITED FINANCIAL STATEMENTS FOR AUGUST 2023
AND SEPTEMBER 2023**

WHEREAS, the Central Texas Regional Mobility Authority (Mobility Authority) is empowered to procure such goods and services as it deems necessary to assist with its operations and to study and develop potential transportation projects, and is responsible to insure accurate financial records are maintained using sound and acceptable financial practices; and

WHEREAS, close scrutiny of the Mobility Authority's expenditures for goods and services, including those related to project development, as well as close scrutiny of the Mobility Authority's financial condition and records is the responsibility of the Board and its designees through procedures the Board may implement from time to time; and

WHEREAS, the Board has adopted policies and procedures intended to provide strong fiscal oversight and which authorize the Executive Director, working with the Mobility Authority's Chief Financial Officer, to review invoices, approve disbursements, and prepare and maintain accurate financial records and reports; and

WHEREAS, the Executive Director, working with the Chief Financial Officer, has reviewed and authorized the disbursements necessary for the month of August 2023 and has caused financial statements to be prepared and attached to this resolution as Exhibit A; and

WHEREAS, the Executive Director, working with the Chief Financial Officer, has reviewed and authorized the disbursements necessary for the month of September 2023 and has caused financial statements to be prepared and attached to this resolution as Exhibit B.

NOW THEREFORE, BE IT RESOLVED, that the Board of Directors accepts the unaudited financial statements for August 2023 and unaudited financial statements for September 2023, attached hereto as Exhibit A and Exhibit B, respectively.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

Robert W. Jenkins, Jr.
Chairman, Board of Directors

Exhibit A

Financial Statements for August 2023

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending August 31, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
REVENUE				
Operating Revenue				
Toll Revenue	153,792,700	25,745,239	16.74%	20,261,274
Video Tolls	64,352,000	8,447,113	13.13%	8,636,463
Fee Revenue	12,962,900	2,022,288	15.60%	1,503,924
Total Operating Revenue	231,107,600	36,214,639	15.67%	30,401,661
Other Revenue				
Transfer In - Cash	62,770,349	62,770,349	100.00%	-
Interest Income	24,905,700	7,703,971	30.93%	1,944,424
Grant Revenue	945,500	-	-	-
Misc Revenue	230,000	5,051	2.20%	9,434
Total Other Revenue	88,851,549	70,479,370	79.32%	1,953,857
TOTAL REVENUE	319,959,149	106,694,010	33.35%	32,355,519
EXPENSES				
Salaries and Benefits				
Salary Expense-Regular	4,871,464	553,196	11.36%	490,469
Salary Reserve	80,000	-	-	-
TCDRS	1,591,401	103,773	6.52%	97,357
FICA	249,197	29,387	11.79%	24,971
FICA MED	70,635	7,948	11.25%	7,072
Health Insurance Expense	584,446	75,297	12.88%	56,735
Life Insurance Expense	3,817	458	11.99%	678
Auto Allowance Expense	10,200	1,445	14.17%	1,063
Other Benefits	166,290	11,159	6.71%	12,229
Unemployment Taxes	5,760	-	-	18
Total Salaries and Benefits	7,633,210	782,663	10.25%	690,592
Administrative				
Administrative and Office Expenses				
Accounting	9,500	1,265	13.31%	1,222
Auditing	245,000	-	-	-
Financial Advisors	162,000	36,000	22.22%	36,000
Human Resources	37,500	168	0.45%	479
Legal	70,000	4,750	6.79%	1,770
IT Services	365,000	24,503	6.71%	24,654
Internet	150	-	-	-
Software Licenses	1,167,000	685,645	58.75%	29,668
Cell Phones	27,800	3,326	11.96%	1,747
Local Telephone Service	2,000	17,386	869.31%	16,047
Overnight Delivery Services	250	-	-	40
Copy Machine	10,000	2,544	25.44%	2,544
Repair & Maintenance-General	10,000	-	-	-
Meeting Facilities	2,000	-	-	-
Meeting Expense	13,750	489	3.55%	2,891
Toll Tag Expense	3,000	100	3.33%	100

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending August 31, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Parking / Local Ride Share	3,550	27	0.76%	30
Mileage Reimbursement	4,350	85	1.95%	123
Insurance Expense	651,000	98,062	15.06%	85,376
Rent Expense	562,540	11,939	2.12%	124,013
Building Parking	3,500	70	2.01%	333
Total Legal Services	488,000	18,793	3.85%	340
Total Administrative and Office Expenses	3,837,890	905,150	23.58%	327,376
Office Supplies				
Books & Publications	5,090	639	12.56%	308
Office Supplies	8,250	88	1.06%	1,112
Misc Office Equipment	4,500	-	-	-
Computer Supplies	202,100	7,515	3.72%	52,142
Copy Supplies	1,000	-	-	-
Other Reports-Printing	1,500	-	-	-
Office Supplies-Printed	2,000	102	5.10%	85
Postage Expense	550	329	59.73%	122
Total Office Supplies	224,990	8,672	3.85%	53,769
Communications and Public Relations				
Graphic Design Services	75,000	-	-	-
Website Maintenance	464,000	76,740	16.54%	15,136
Research Services	150,000	-	-	-
Communications and Marketing	400,000	11,940	2.99%	-
Advertising Expense	500,000	164,199	32.84%	42,670
Direct Mail	40,000	-	-	-
Video Production	160,000	-	-	28,359
Photography	25,000	295	1.18%	450
Radio	50,000	-	-	-
Other Public Relations	22,500	-	-	-
Promotional Items	20,000	1,166	5.83%	-
Annual Report printing	1,300	-	-	-
Direct Mail Printing	17,500	-	-	-
Other Communication Expenses	15,000	-	-	7,188
Total Communications and Public Relations	1,940,300	254,340	13.11%	93,803
Employee Development				
Subscriptions	750	139	18.53%	264
Agency Memberships	88,440	25	0.03%	-
Continuing Education	14,800	-	-	-
Professional Development	20,150	-	-	-
Other Licenses	2,500	-	-	375
Seminars and Conferences	104,100	1,445	1.39%	30,700
Travel	110,500	12,892	11.67%	-
Total Employee Development	341,240	14,501	4.25%	31,339

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending August 31, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Financing and Banking Fees				
Trustee Fees	62,000	15,000	24.19%	15,000
Bank Fee Expense	3,240	947	29.24%	185
Continuing Disclosure	7,000	-	-	-
Arbitrage Rebate Calculation	16,300	-	-	16,300
Rating Agency Expense	45,000	32,500	72.22%	31,000
Total Financing and Banking Fees	133,540	48,447	36.28%	62,485
Total Administrative	6,477,960	1,231,111	19.00%	568,772
Operations and Maintenance				
Operations and Maintenance Consulting				
GEC-Trust Indenture Support	1,131,395	251,825	22.26%	210,571
GEC-Financial Planning Support	275,000	50,386	18.32%	46,465
GEC-Toll Ops Support	1,584,000	152,814	9.65%	101,815
GEC-Roadway Ops Support	1,605,500	108,083	6.73%	81,961
GEC-Technology Support	679,526	167,549	24.66%	131,166
GEC-Public Information Support	200,000	23,711	11.86%	20,696
GEC-General Support	1,631,820	162,027	9.93%	106,464
General System Consultant	1,381,000	27,875	2.02%	84,877
Traffic Modeling	125,000	-	-	-
Traffic and Revenue Consultant	1,010,000	34,518	3.42%	82,508
Total Operations and Maintenance Consulting	9,623,241	978,788	10.17%	866,523
Roadway Operations and Maintenance				
Roadway Maintenance	3,431,819	503,586	14.67%	695,433
Landscape Maintenance	2,789,256	461,740	16.55%	912,025
Signal & Illumination Maint	25,000	-	-	-
Maintenance Supplies-Roadway	400,000	-	-	-
Tools & Equipment Expense	-	-	-	444
Gasoline	30,000	3,729	12.43%	3,450
Repair & Maintenance - Vehicles	10,000	360	3.60%	396
Natural Gas	2,500	1,025	40.98%	771
Electricity - Roadways	250,000	40,653	16.26%	42,810
Total Roadway Operations and Maintenance	6,938,575	1,011,093	14.57%	1,655,328
Toll Processing and Collection Expense				
Image Processing	3,000,000	236,147	7.87%	334,192
Tag Collection Fees	11,500,000	1,793,431	15.60%	1,508,831
Court Enforcement Costs	10,000	-	-	-
ETC Incentive	500,000	-	-	-
Total Processing and Collection Expense	15,010,000	2,029,578	13.52%	1,843,023
Toll Operations Expense				
Generator Fuel	3,000	-	-	-
Fire and Burglar Alarm	500	82	16.45%	82
Refuse	2,360	300	12.73%	324

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending August 31, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Telecommunications	60,000	-	-	-
Water - Irrigation	7,500	1,409	18.78%	2,334
Electricity	750	178	23.71%	111
ETC spare parts expense	100,000	-	-	-
Repair & Maintenance Toll Equip	50,000	-	-	31,491
Law Enforcement	600,000	81,143	13.52%	66,950
ETC Maintenance Contract	6,450,000	499,698	7.75%	334,139
Transaction Processing Maintenance Contract	2,000,000	-	-	-
ETC Toll Management Center System Operation	2,885,054	112,851	3.91%	76,630
ETC Development	650,000	29,106	4.48%	-
ETC Testing	225,000	-	-	-
Total Toll Operations Expense	13,034,164	724,766	5.56%	512,061
Total Operations and Maintenance	44,605,980	4,744,225	10.64%	4,876,935
Other Expenses				
Special Projects and Contingencies				
HERO	200,000	24,638	12.32%	24,638
Special Projects	100,000	-	-	-
71 Express Net Revenue Payment	5,000,000	1,075,128	21.50%	-
Customer Relations	10,000	-	-	-
Technology Initiatives	185,000	-	-	-
Other Contractual Svcs	390,000	40,500	10.38%	49,500
Contingency	200,000	-	-	-
Total Special Projects and Contingencies	6,085,000	1,140,267	18.74%	74,138
Non Cash Expenses				
Amortization Expense				
Amortization Expense - Software	1,228,015	4,233	0.34%	213,382
Amortization Expense - Right to Use Asset - Subscr	355,208	63,615	17.91%	-
Amortization Expense - Refundings	1,907,487	1,024,236	53.70%	886,852
Subtotal Amortization Expense	3,490,710	1,092,085	31.29%	1,100,234
Depreciation Expense				
Dep Exp - Furniture & Fixtures	2,178	-	-	436
Dep Expense - Equipment	476,653	103,784	21.77%	-
Dep Expense - Autos & Trucks	45,399	5,068	11.16%	8,892
Dep Expense - Buildng & Toll Fac	187,058	29,458	15.75%	29,458
Dep Expense - Highways & Bridges	48,608,788	8,472,925	17.43%	8,436,924
Dep Expense - Toll Equipment	3,917,914	506,497	12.93%	698,975
Dep Expense - Signs	1,641,174	201,492	12.28%	169,428
Dep Expense - Land Improvements	884,934	117,969	13.33%	147,489
Depreciation Expense - Computers	98,507	-	-	31,514
Subtotal Depreciation Expense	55,862,606	9,437,194	16.89%	9,523,115
Total Non Cash Expenses	59,353,316	10,529,279	17.74%	10,623,349
Total Other Expenses	65,438,316	11,669,545	17.83%	10,697,487

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending August 31, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Non Operating Expenses				
Bond Issuance Expense	1,250,000	-	-	88,049
Loan Fee Expense	40,000	-	-	-
Interest Expense - Debt Obligations	95,964,098	13,329,994	13.89%	13,003,297
Interest Expense - Right to Use Assets	26,164	-	-	-
Transfer Out - Cash	62,770,349	62,770,349	100.00%	-
CAMPO RIF Payment	6,000,000	-	-	-
Community Initiatives	645,000	-	-	-
Total Non Operating Expenses	166,695,611	76,100,343	45.65%	13,091,346
TOTAL EXPENSES	290,851,076	94,527,886	32.50%	29,925,131
Net Income	29,108,072	12,166,123		2,430,387

Central Texas Regional Mobility Authority
Balance Sheet
as of August 31, 2023

as of 08/31/2023 as of 08/31/2022

ASSETS

Current Assets

Cash

Regions Operating Account	\$ 119,587	\$ 2,795,467
Cash in TexStar	304,100	42,849
Regions Payroll Account	107,719	96,550

Restricted Cash

Goldman Sachs FSGF 465	582,135,790	982,744,133
Restricted Cash - TexSTAR	8,682,213	10,388,374
Overpayments account	-	291,128

Total Cash and Cash Equivalents	591,349,409	996,358,500
--	--------------------	--------------------

Accounts Receivables

Accounts Receivable - Net	4,979,871	2,770,089
Due From Other Agencies	226,563	69,732
Due From TTA	668,161	604,373
Due From NTTA	1,517,325	1,110,520
Due From HCTRA	3,771,136	1,842,768
Due From TxDOT	7,565,900	4,153,555
Interest Receivable	693,342	708,479

Total Receivables	19,422,298	11,259,516
--------------------------	-------------------	-------------------

Short Term Investments

Treasuries	118,543,252	-
Agencies	339,758,036	112,436,936

Total Short Term Investments	458,301,288	112,436,936
-------------------------------------	--------------------	--------------------

Total Current Assets	1,069,072,995	1,120,054,953
-----------------------------	----------------------	----------------------

Construction in Progress

412,418,308	274,331,968
--------------------	--------------------

Capital Assets (Net of Depreciation and Amortization)

Depreciable Assets

Computers	-	66,993
Furniture and Fixtures	-	1,742
Equipment	1,297,304	9,624
Autos and Trucks	41,813	84,991
Buildings and Toll Facilities	4,200,503	4,387,561
Highways and Bridges	1,664,294,215	1,708,238,358
Toll Equipment	15,152,659	19,306,149
Signs	11,171,404	12,989,618
Land Improvements	5,196,366	6,051,780

Central Texas Regional Mobility Authority
Balance Sheet
as of August 31, 2023

	as of 08/31/2023	as of 08/31/2022
Right of way	88,149,606	88,149,606
Leasehold Improvements	4,233	37,021
Intangible Assets		
Computer Software	-	1,573,709
Right to Use Assets		
Leases	1,286,881	-
Subscription Based IT Arrangements	503,471	-
Total Fixed Assets	1,791,298,454	1,840,897,153
Other Assets		
Intangible Assets-Net	172,360,460	174,405,333
2005 Bond Insurance Costs	-	3,345,875
Prepaid Insurance	49,031	42,688
Deferred Outflows (pension related)	2,661,405	675,913
Pension Asset	1,046,634	2,549,818
Total Other Assets	176,117,530	181,019,627
Total Assets	\$ 3,448,907,287	\$ 3,416,303,701

LIABILITIES

Current Liabilities		
Accounts Payable	4,878,930	19,954,847
Construction Payable	4,182,841	5,356,306
Overpayments	1,570	294,629
Interest Payable	13,590,075	13,632,683
TCDRS Payable	82,304	71,893
Due to other Agencies	3,779	3,073
Due to TTA	652,223	606,448
Due to HCTRA	161,897	132,638
Due to Other Entities	1,883,620	55,983
71E TxDOT Obligation - ST	3,761,703	1,818,107
Total Current Liabilities	29,198,941	41,926,606
Long Term Liabilities		
Compensated Absences	240,954	268,014
Right to Use Obligations - Lease	1,286,881	-
Right to Use Obligations - SBITA	579,894	-
Deferred Inflows (pension related)	1,340,710	1,481,361
Long Term Payables	3,448,440	1,749,375

Central Texas Regional Mobility Authority
Balance Sheet
as of August 31, 2023

as of 08/31/2023 as of 08/31/2022

Bonds Payable

Senior Lien Revenue Bonds:

Senior Lien Revenue Bonds 2010	95,580,925	88,711,545
Senior Lien Revenue Bonds 2011	16,373,850	19,037,840
Senior Refunding Bonds 2013	-	3,475,000
Senior Lien Revenue Bonds 2015	10,000,000	10,000,000
Senior Lien Refunding Revenue Bonds 2016	59,340,000	70,790,000
Senior Lien Revenue Bonds 2018	44,345,000	44,345,000
Senior Lien Revenue Bonds 2020A	50,265,000	50,265,000
Senior Lien Refunding Bonds 2020B	54,970,000	55,600,000
Senior Lien Refunding Bonds 2020C	138,435,000	138,435,000
Senior Lien Revenue Bonds 2020E	167,160,000	167,160,000
Senior Lien Revenue Bonds 2021B	255,075,000	255,075,000
Senior Lien Refunding Bonds 2021D	274,150,000	274,625,000
Senior Lien Refunding Bonds 2021E	332,585,000	335,610,000
Sn Lien Rev Bnd Prem/Disc 2013	-	596,372
Senior Lien Premium 2016 Revenue Bonds	6,675,724	7,456,351
Sn Lien Revenue Bond Premium 2018	2,838,789	3,105,362
Senior Lien Revenue Bond Premium 2020A	11,130,761	11,318,006
Senior Lien Refunding Bond Premium 2020B	11,147,401	11,682,477
Senior Lien Revenue Bonds Premium 2020E	23,854,638	25,570,024
Senior Lien Revenue Bonds Premium 2021B	52,890,189	53,451,667
Senior Lien Refunding Bonds Premium 2021D	44,278,923	44,780,143
Total Senior Lien Revenue Bonds	1,651,096,201	1,671,089,788

Sub Lien Revenue Bonds:

Sub Lien Refunding Bonds 2013	-	2,725,000
Sub Lien Refunding Bonds 2016	71,435,000	72,605,000
Sub Lien Refunding Bonds 2020D	97,440,000	98,580,000
Subordinated Lien BANs 2020F	110,875,000	110,875,000
Subordinate Lien Refunding Bonds 2020G	61,570,000	61,570,000
Subordinated Lien BANs 2021C	244,185,000	244,185,000
Sub Refunding 2013 Prem/Disc	-	127,249
Sub Refunding 2016 Prem/Disc	4,862,401	5,655,571
Subordinated Lien BANs 2020F Premium	5,337,153	9,340,018
Subordinated Lien Refunding Bonds Premium 2020G	6,696,919	7,100,891
Sub Lien BANS 2021C Premium	25,372,258	32,983,935
Total Sub Lien Revenue Bonds	627,773,731	645,747,664

Central Texas Regional Mobility Authority
Balance Sheet
as of August 31, 2023

	as of 08/31/2023	as of 08/31/2022
Other Obligations		
TIFIA Note 2021	360,361,691	352,597,160
71E TxDOT Obligation - LT	51,918,220	55,077,264
Regions 2022 MoPac Loan	23,765,900	24,690,900
Total Other Obligations	436,045,811	432,365,324
Total Long Term Liabilities	2,718,364,182	2,750,952,151
Total Liabilities	2,747,563,123	2,792,878,758
NET ASSETS		
Contributed Capital	121,462,104	121,462,104
Net Assets Beginning	567,715,936	499,532,451
Current Year Operations	12,166,123	2,430,387
Total Net Assets	701,344,164	623,424,943
Total Liabilities and Net Assets	\$ 3,448,907,287	\$ 3,416,303,701

Central Texas Regional Mobility Authority
Statement of Cash Flow
as of August 2023

Cash flows from operating activities:

Receipts from toll revenues	39,069,690
Receipts from Other Sources (AR)	5,051
Payments to vendors	(40,351,025)
Payments to employees	(788,101)
Net cash flows provided by (used in) operating activities	(2,064,385)

Cash flows from capital and related financing activities:

Prepaid payment on Intangible assets	(1,024,236)
Issuance Expense	(3,513,621)
Payments on bonds / loans	(444,629)
RIF Contribution	-
Acquisition of capital assets - non project	(1,417,034)
Acquisitions of construction in progress	(7,938,874)
Net cash flows provided by (used in) capital and related financing activities	(14,338,394)

Cash flows from investing activities:

Interest income	7,703,971
Purchase of investments	(234,773,911)
Proceeds from sale or maturity of investments	-
Net cash flows provided by (used in) investing activities	(227,069,941)

Net increase (decrease) in cash and cash equivalents	(283,250,904)
Cash and cash equivalents at beginning of period	894,022,611
Cash and cash equivalents at end of period	610,771,707

Reconciliation of change in net assets to net cash provided by operating activities:

Operating income	12,166,123
Adjustments to reconcile change in net assets to net cash provided by operating activities:	
Depreciation and amortization	10,529,279
Changes in assets and liabilities:	
Decrease in accounts receivable	2,855,051
Increase in prepaid expenses and other assets	98,062
Decrease in accrued expenses	(33,338,923)
Decrease in Interest expense	13,329,994
Increase in interest receivable	(7,703,971)
(Decrease) increase in Pension Asset	-
(Increase) in deferred outflows of resources	-
(Increase) in deferred inflows of resources	-
Total adjustments	(14,230,509)
Net cash flows provided by (used in) operating activities	\$ (2,064,385)

Reconciliation of cash and cash equivalents:

Unrestricted cash and cash equivalents	19,953,704
Restricted cash and cash equivalents	590,818,003
Total	610,771,707

Investments by Fund

Fund	TexSTAR	TexSTAR- Trustee	Goldman Sachs	Agencies/ Treasuries	Balance
Renewal and Replacement Fund	8.63		57.76		66.39
Grant Fund	476,656.03		10,037,836.30		10,514,492.33
Senior Debt Service Reserve Fund	1,034,492.18		6,012,790.80	104,995,814.41	112,043,097.39
2010 Senior Lien Debt Service			63,317.39		63,317.39
2011 Sr Debt Service t			4,863,815.80		4,863,815.80
2013 Sr Debt Service t			41,969.63		41,969.63
2013 Sub Debt Service			33,031.41		33,031.41
2013 Sub Debt Service Reserve Fund	818,606.47		128.71		818,735.18
2015 Sr Debt Service			4,170,351.15		4,170,351.15
2016 Sr Lien Rev Refunding Debt Service			9,451,488.10		9,451,488.10
2016 Sub Lien Rev Refunding Debt Service			2,157,284.44		2,157,284.44
2016 Sub Lien Rev Refunding DSR			603,056.33	6,671,837.25	7,274,893.58
Operating Fund	3,085,873.43	304,100.30	15,293,149.54		18,683,123.27
Revenue Fund			2,262,971.25		2,262,971.25
General Fund	1,193,741.70		75,906,289.05	104,917,207.70	182,017,238.45
71E Revenue Fund			30,467,902.42		30,467,902.42
MoPac Revenue Fund			16,060,730.22		16,060,730.22
MoPac General Fund					-
MoPac Operating Fund			1,049,817.82		1,049,817.82
MoPac Loan Repayment Fund			336,784.00		336,784.00
2015B Project	366,900.95		7,940,384.97		8,307,285.92
2015 TIFIA Project	728,906.58		9,076,502.90	30,000,000.00	39,805,409.48
2011 Sr Financial Assistance Fund	16.36		28,158.74		28,175.10
2018 Sr Lien Debt Service			380,517.40		380,517.40
2018 Sr Lien Project Cap I			743.43		743.43
2018 Sr Lien Project	977,010.57		13,162,787.93		14,139,798.50
2020A Senior Lien Debt Service			430,317.02		430,317.02
2020B Senior Lien Debt Service			903,405.04		903,405.04
2020C Senior Lien Debt Service			4,113,189.40		4,113,189.40
2020D Sub Lien Debt Service			3,209,311.03		3,209,311.03
2020D Sub Debt Service Reserve Fund			455,270.53	7,987,089.95	8,442,360.48
2020E Senior Lien Project			91,825,227.68	50,000,000.00	141,825,227.68
2020E Senior Lien Project Cap Interest			15,108,595.33		15,108,595.33
2020F Sub Lien Project			44,466.13		44,466.13
2020F Sub Lien Deb Service			951,826.56		951,826.56
2020G Sub Lien Debt Service			438,265.16		438,265.16
2020G Sub Lien Debt Service Reserve			791,657.75	2,995,158.73	3,786,816.48
2021A Sub Lien Debt Service Reserve			2,270,886.96	15,974,180.00	18,245,066.96
2021A Sub Debt Service			99.96		99.96
2021B Senior Lien Cap I Project Fund			36,082,251.50		36,082,251.50
2021B Senior Lien Project			104,787,374.96	135,000,000.00	239,787,374.96
2021C Sub Lien Cap I Project Fund			1,395.15		1,395.15
2021C Sub Lien Project			99,001,051.73		99,001,051.73
2021C Sub Lien Debt Service			2,096,384.89		2,096,384.89
2021D Senior Lien Debt Service			2,257,880.93		2,257,880.93
2021E Senior Lien Debt Service			3,712,753.07		3,712,753.07
Totals	8,682,212.90	304,100.30	577,883,478.27	458,541,288.04	1,045,411,079.51

CTRMA INVESTMENT REPORT

Month Ending 08/31/23

Balance 8/1/2023	Accrued Interest	Additions	Cash Transfers	Discount Amortization	Withdrawals	Balance 8/31/2023	Rate Aug
Amount in Trustee TexStar							
2011 Sr Lien Financial Assist Fund	16.32	0.04				16.36	5.2974%
2013 Sub Lien Debt Service Reserve General Fund	814,939.94	3,666.53				818,606.47	5.2974%
Trustee Operating Fund	1,188,394.92	5,346.78				1,193,741.70	5.2974%
Renewal and Replacement	7,567,072.53	18,800.90	(4,500,000.00)			3,085,873.43	5.2974%
TxDOT Grant Fund	8.63					8.63	5.2974%
Senior Lien Debt Service Reserve Fund	474,521.07	2,134.96				476,656.03	5.2974%
2015B Sr Ln Project	1,029,858.66	4,633.52				1,034,492.18	5.2974%
2015C TIFIA Project	365,257.60	1,643.35				366,900.95	5.2974%
2018 Sr Lien Project	725,641.79	3,264.79				728,906.58	5.2974%
	972,634.53	4,376.04				977,010.57	5.2974%
13,138,345.99	43,866.91	-	(4,500,000.00)	-	-	8,682,212.90	
Amount in TexStar Operating Fund							
340,775.52	3,324.78		4,500,000.00		4,540,000.00	304,100.30	5.2974%

Goldman Sachs

Operating Fund	11,149,618.90	53,952.92	93,160.99	4,000,000.00		3,583.27	15,293,149.54	5.2100%
2020A Senior Lien Debt Service	222,417.39	841.51		207,058.12			430,317.02	5.2100%
2020B Senior Lien Debt Service	626,923.00	2,448.43		274,033.61			903,405.04	5.2100%
2020C Senior Lien Debt Service	665,192.06	2,578.65		3,445,418.69			4,113,189.40	5.2100%
2020D Sub Lien Debt Service	2,623,055.89	10,381.86		575,873.28			3,209,311.03	5.2100%
2020D Sub Debt Service Reserve Fund	453,343.95	1,926.58					455,270.53	5.2100%
2020E Sr Lien Project	145,772,717.83	639,118.74				54,586,608.89	91,825,227.68	5.2100%
2020E Sr Ln Project Cap Interest	15,043,094.66	65,500.67					15,108,595.33	5.2100%
2020E Sr Lien Debt Service	0.00						0.00	5.2100%
2020F Sub Lien Project	48,631.93					4,165.80	44,466.13	5.2100%
2020F Sub Lien Debt Service	491,877.24	1,858.64		458,090.68			951,826.56	5.2100%
2020G Sub Lien Debt Service	226,483.12	855.81		210,926.23			438,265.16	5.2100%
2020G Sub Debt Service Reserve Fund	749,406.95	3,120.30		39,130.50			791,657.75	5.2100%
2021A Sub Debt Service Reserve Fund	1,703,129.04	6,033.15		561,724.77			2,270,886.96	5.2100%
2021A Sub Debt Service	99.53	0.43					99.96	5.2100%
2021B Senior Lien Cap I Project Fund	35,926,642.35	155,609.15					36,082,251.50	5.2100%
2021B Senior Lien Project	203,860,623.83	926,751.13				100,000,000.00	104,787,374.96	5.2100%
2021B Senior Lien Cap I Debt Service	0.00						0.00	5.2100%
2021C Sub Lien Cap I Project Fund	1,389.19	5.96					1,395.15	5.2100%
2021C Sub Lien Project	94,927,531.28	484,562.52	4,671,012.48			1,082,054.55	99,001,051.73	5.2100%
2021C Sub Lien Debt Service	1,083,348.14	4,093.50		1,008,943.25			2,096,384.89	5.2100%
2021D Senior Lien Debt Service	1,287,157.90	4,923.42	-	965,799.61			2,257,880.93	5.2100%
2021E Senior Lien Debt Service	2,650,405.00	10,378.61		1,051,969.46			3,712,753.07	5.2100%
2011 Sr Financial Assistance Fund	27,905.81	252.93					28,158.74	5.2100%
2010 Senior DSF	63,047.05	270.34					63,317.39	5.2100%
2011 Senior Lien Debt Service	4,251,794.95	16,922.64		595,098.21			4,863,815.80	5.2100%
2013 Senior Lien Debt Service	41,790.44	179.19					41,969.63	5.2100%
2013 Sub Debt Service Reserve Fund	128.16	0.55					128.71	5.2100%
2013 Subordinate Debt Service	32,890.38	141.03					33,031.41	5.2100%
2015A Sr Lien Debt Service	4,152,477.41	17,873.74					4,170,351.15	5.2100%
2015B Project	7,911,220.08	34,232.49				5,067.60	7,940,384.97	5.2100%
2015C TIFIA Project	8,992,605.47	83,897.43					9,076,502.90	5.2100%
2016 Sr Lien Rev Refunding Debt Service	8,238,560.87	32,942.06		1,179,985.17			9,451,488.10	5.2100%
2016 Sub Lien Rev Refunding Debt Service	1,687,436.72	6,659.99		463,187.73			2,157,284.44	5.2100%
2016 Sub Lien Rev Refunding DSR	600,488.79	2,567.54					603,056.33	5.2100%
2018 Sr Lien Project Cap I	740.26	3.17					743.43	5.2100%
2018 Sr Lien Debt Service	196,622.53	743.06		183,151.81			380,517.40	5.2100%
2018 Sr Lien Project	12,889,718.49	55,254.75	217,814.69				13,162,787.93	5.2100%
TxDOT Grant Fund	9,994,979.27	42,857.03					10,037,836.30	5.2100%
Renewal and Replacement	1,150.49	37.65		1,638,300.00		1,639,430.38	57.76	5.2100%
Revenue Fund	10,817,096.87	49,936.38	17,930,078.79	(26,430,305.73)		103,835.06	2,262,971.25	5.2100%
General Fund	68,324,055.89	293,541.33		8,118,985.24		830,293.41	75,906,289.05	5.2100%
Senior Lien Debt Service Reserve Fund	5,987,199.68	25,591.12					6,012,790.80	5.2100%
71E Revenue Fund	29,409,204.05	124,639.96	333,521.31	703,212.56		102,675.46	30,467,902.42	5.2100%
MoPac Revenue Fund	71,741.93	1,779.74	293,593.28	(367,114.95)			0.00	5.2100%
MoPac General Fund	15,445,424.29	64,383.41		550,922.52			16,060,730.22	5.2100%
MoPac Operating Fund	956,056.27	4,410.04	70,018.93	400,000.00		380,667.42	1,049,817.82	5.2100%
MoPac Loan Repayment Fund	170,629.18	545.58		165,609.24			336,784.00	5.2100%
709,778,054.51	3,234,605.13	23,609,200.47	-	-	-	158,738,381.84	577,883,478.27	

Amount in Fed Agencies and Treasuries

Amortized Principal	308,541,288.04		150,000,000.00		-		458,541,288.04	
---------------------	-----------------------	--	-----------------------	--	----------	--	-----------------------	--

Certificates of Deposit

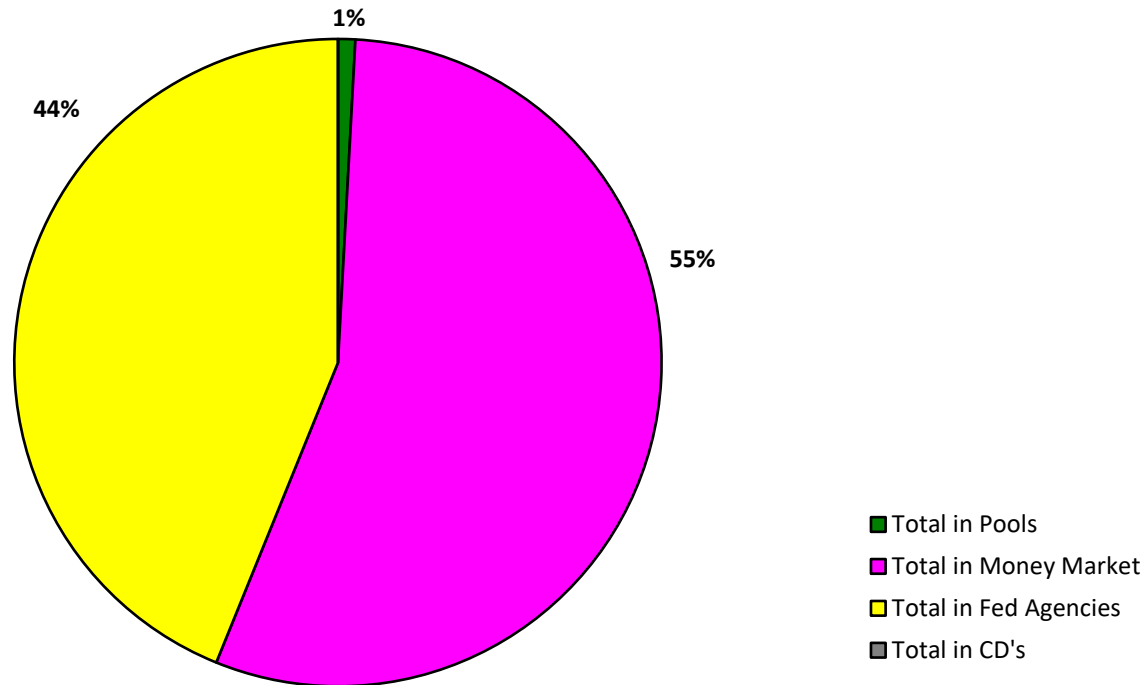
Total in Pools - TxStar	13,479,121.51	47,191.69	-	-	-	4,540,000.00	8,986,313.20	
Total in GS FSGF	709,778,054.51	3,234,605.13	23,609,200.47	-	-	158,738,381.84	577,883,478.27	
Total in Fed Agencies and Treasuries	308,541,288.04	-	150,000,000.00	-	-	-	458,541,288.04	
Total Invested	1,031,798,464.06	3,281,796.82	173,609,200.47	-	-	163,278,381.84	1,045,411,079.51	

All Investments in the portfolio are in compliance with the CTRMA's Investment policy and the relevant provisions of the Public Funds Investment Act Chapter 2256.023

José Hernández, CFO
Ann Zigmond, Controller

8/31/2023

Allocation of Funds



Goldman Sachs Escrow Funds

	Balance		Accrued		Balance
	8/1/2023	Additions	Interest	Withdrawals	8/31/2023
Travis County Escrow Fund - Elroy Road	3,001,419.85		12,903.77	3,656.12	3,010,667.50
Travis County Escrow Fund - Ross Road	164,832.18		708.46	896.35	164,644.29
Travis County Escrow Fund - Old San Antonio Road	32,649.68		139.98	1,070.12	31,719.54
Travis County Escrow Fund - Old Lockhart Road	129,939.86	25,500.00	557.02	22,838.30	133,158.58
Travis County Escrow Fund - County Line Road	228,596.20		1,033.25	10,890.95	218,738.50
Travis County Escrow Fund - South Pleasant Valley Road	311,656.41		1,347.01	9,238.96	303,764.46
Travis County Escrow Fund - Thaxton Road	120,336.48		545.05	9,589.69	111,291.84
Travis County Escrow Fund - Pearce Lane Road	283,973.42		1,259.74	6,906.27	278,326.89

						Interest Income		
Bank	FUND	COST	Cummulative Amortization	Book Value	Maturity Value	Accrued Interest	Amortization	Interest Earned
6180006366	2016SUBDSR	6,671,837.25		6,671,837.25				-
1001017484	2020D DSRF	7,987,089.95		7,987,089.95	8,200,000.00			-
1001021540	2020G DSRF	2,995,158.73		2,995,158.73	3,075,000.00			-
1001021543	2021A DSRF	15,974,180.00		15,974,180.00	16,400,000.00			-
6180000120	GENERAL	20,000,000.00		20,000,000.00	20,000,000.00			-
6180000120	GENERAL	19,973,592.19		19,973,592.19	20,500,000.00			-
6180000120	GENERAL	44,963,937.40		44,963,937.40	47,150,000.00	3,864.75		3,864.75
6180000059	SENLINDSR	20,000,000.00		20,000,000.00	20,000,000.00	22,222.22		22,222.22
6180000059	SENLINDSR	20,000,000.00		20,000,000.00	20,000,000.00			-
6180000059	SENLINDSR	45,000,000.00		45,000,000.00	45,000,000.00			-
6180000059	SENLINDSR	19,973,592.19		19,973,592.19	20,500,000.00			-
6180000120	GENERAL	9,960,128.90		9,960,128.90	10,000,000.00	27,777.78		27,777.78
6180000120	GENERAL	9,960,128.90		9,960,128.90	10,000,000.00	27,777.78		27,777.78
6180005349	2015TIFIAP	30,000,000.00		30,000,000.00	30,000,000.00			
1001021273	2021BPROJ	35,000,000.00		35,000,000.00	35,000,000.00			-
1001021533	2020E PRJ	50,000,000.00		50,000,000.00	50,000,000.00			
1001021273	2021BPROJ	50,000,000.00		50,000,000.00	50,000,000.00			-
1001021273	2021BPROJ	50,000,000.00		50,000,000.00	50,000,000.00			
		458,459,645.51	-	458,459,645.51	455,825,000.00	81,642.53	-	81,642.53



PERFORMANCE

As of August 31, 2023

Current Invested Balance	\$ 10,207,693,267.12
Weighted Average Maturity (1)	27 Days
Weighted Average Life (2)	50 Days
Net Asset Value	0.999773
Total Number of Participants	1023
Management Fee on Invested Balance	0.06%*
Interest Distributed	\$ 47,862,830.52
Management Fee Collected	\$ 536,049.82
% of Portfolio Invested Beyond 1 Year	2.58%
Standard & Poor's Current Rating	AAAm

Rates reflect historical information and are not an indication of future performance.

August Averages

Average Invested Balance	\$ 10,519,484,077.09
Average Monthly Yield, on a simple basis	5.2974%
Average Weighted Maturity (1)	26 Days
Average Weighted Life (2)	49 Days

Definition of Weighted Average Maturity (1) & (2)

(1) This weighted average maturity calculation uses the SEC Rule 2a-7 definition for stated maturity for any floating rate instrument held in the portfolio to determine the weighted average maturity for the pool. This Rule specifies that a variable rate instruction to be paid in 397 calendar days or less shall be deemed to have a maturity equal to the period remaining until the next readjustment of the interest rate.
(2) This weighted average maturity calculation uses the final maturity of any floating rate instruments held in the portfolio to calculate the weighted average maturity for the pool.

The maximum management fee authorized for the TexSTAR Cash Reserve Fund is 12 basis points. This fee may be waived in full or in part in the discretion of the TexSTAR co-administrators at any time as provided for in the TexSTAR Information Statement.

NEW PARTICIPANTS

We would like to welcome the following entities who joined the TexSTAR program in August:

* Crandall Economic Development Corporation * City of Potteet

HOLIDAY REMINDER

In observance of **Columbus Day**, **TexSTAR will be closed on Monday, October 9, 2023**. All ACH transactions initiated on Friday, October 6th will settle on Tuesday, October 10th. Standard transaction deadlines will be observed on Friday, October 6th. Please plan accordingly for your liquidity needs.

ECONOMIC COMMENTARY

Market review

For the last year and half, the Federal Reserve (Fed) has engaged in an aggressive campaign to slow the economy in order to reduce inflation to its 2% target. However, the data have left Fed officials confused, with growth proving resilient even as inflation continues to decelerate. Recession risks and probability of recession have moderated in the near term, as employment and spending data have held up well; and corporate earnings have been resilient. However, in August, despite mixed data, we saw some signs of moderation, as unemployment inched higher and consumer confidence weakened.

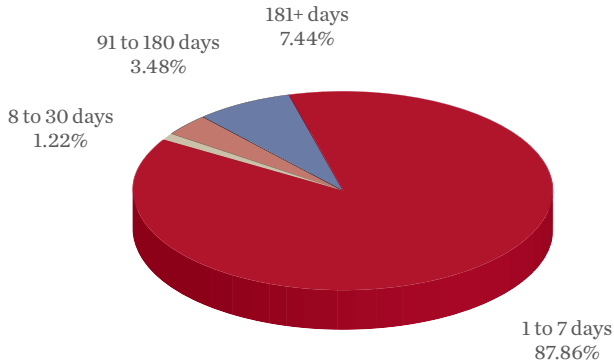
Earlier this year, markets largely anticipated that economic activity, specifically capital spending, would slow due to the lagged impact of restrictive monetary policy. Instead, record low unemployment, robust business investment, and resilient American consumers have kept the economy on an above trend growth trajectory thus far in 2023. July retail sales handily beat expectations, gaining 0.7% month-over-month (m/m) and 1.0% ex-autos. While a 1.9% m/m increase in online sales contributed the most, gains were broad-based. Elsewhere, industrial production jumped by a stronger-than-expected 1.0% m/m due to elevated auto production and sweltering temperatures driving up the demand for cooling. Manufacturing output also rose 0.5% m/m. However, excluding the sharp increase in motor vehicles and parts production, gains were a more modest 0.1%. Finally, the housing market showed continued signs of stabilization. Housing starts and permits rose by 3.9% and 0.1%, respectively, as gains in single-family more than offset declines in multi-family across both measures.

Inflation continued to come down, both at the headline and core level. The July CPI report pointed toward a continued moderation in inflation. Headline CPI rose 0.2% month-over-month (m/m) seasonally adjusted and 3.2% year-over-year (y/y) non-seasonally adjusted, a slight tick up compared to last month.

(continued page 4)

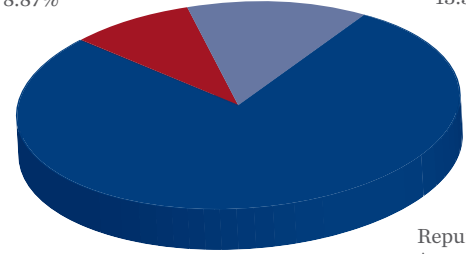
INFORMATION AT A GLANCE

PORTFOLIO BY TYPE OF INVESTMENT AS OF AUGUST 31, 2023



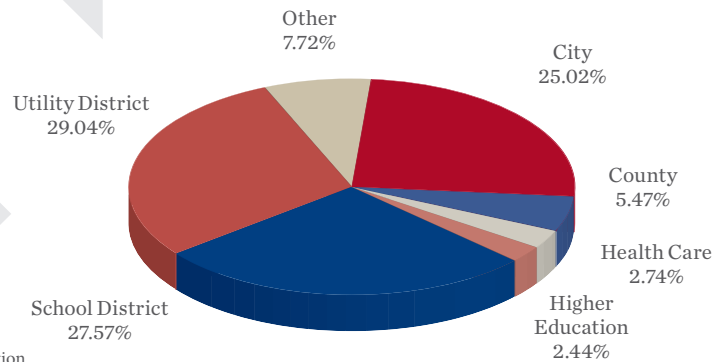
Treasuries
8.87%

Agencies
13.51%



Repurchase
Agreements
77.62%

PORTFOLIO BY MATURITY AS OF AUGUST 31, 2023 (1)



DISTRIBUTION OF PARTICIPANTS BY TYPE AS OF AUGUST 31, 2023

(1) Portfolio by Maturity is calculated using WAM (1) definition for stated maturity. See page 1 for definition

HISTORICAL PROGRAM INFORMATION

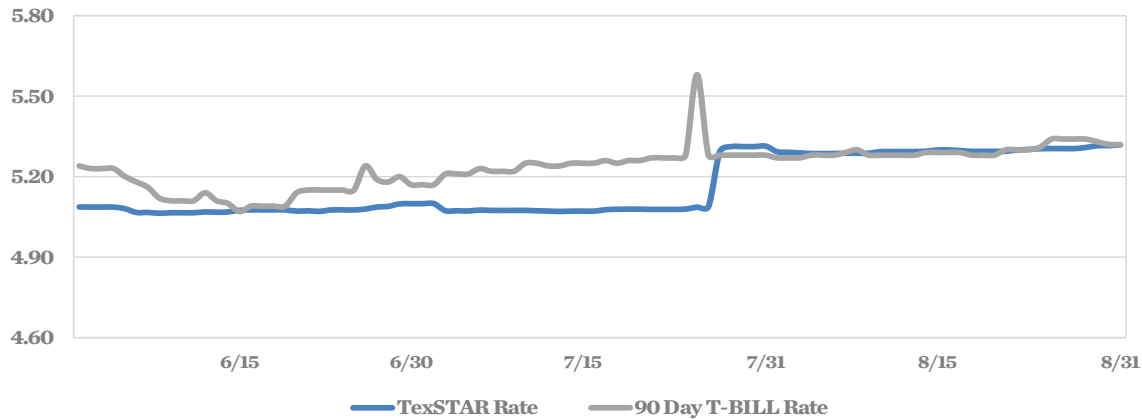
MONTH	AVERAGE RATE	BOOK VALUE	MARKET VALUE	NET ASSET VALUE	WAM (1)	WAL (2)	NUMBER OF PARTICIPANTS
Aug 23	5.2974%	\$10,207,693,267.12	\$10,205,377,223.94	0.999773	26	49	1023
Jul 23	5.1148%	10,852,471,505.08	10,849,665,890.42	0.999741	22	47	1021
Jun 23	5.0764%	10,475,876,514.08	10,473,945,855.73	0.999806	22	50	1020
May 23	5.0471%	10,704,350,596.85	10,702,720,616.60	0.999847	20	45	1019
Apr 23	4.8292%	10,940,711,794.05	10,941,057,413.24	1.000031	17	42	1017
Mar 23	4.6066%	11,042,113,205.98	11,042,864,910.32	1.000029	11	39	1012
Feb 23	4.4919%	10,962,890,240.57	10,961,778,645.78	0.999898	9	38	1008
Jan 23	4.2515%	10,451,037,339.95	10,450,044,625.54	0.999905	6	41	1003
Dec 22	3.9681%	9,016,826,910.67	9,015,709,981.89	0.999855	5	43	999
Nov 22	3.5588%	8,393,118,851.17	8,390,786,906.73	0.999722	6	47	998
Oct 22	2.8531%	8,388,414,626.87	8,384,901,873.82	0.999581	10	46	996
Sep 22	2.2941%	8,448,258,598.47	8,444,307,157.72	0.999510	16	43	994

PORTFOLIO ASSET SUMMARY AS OF AUGUST 31, 2023

	BOOK VALUE	MARKET VALUE
Uninvested Balance	\$ 557.95	\$ 557.95
Accrual of Interest Income	15,032,048.92	15,032,048.92
Interest and Management Fees Payable	(47,867,990.63)	(47,867,990.63)
Payable for Investment Purchased	0.00	0.00
Repurchase Agreement	7,948,702,999.78	7,948,702,999.78
Government Securities	2,291,825,651.10	2,289,509,607.92
TOTAL	\$ 10,207,693,267.12	\$ 10,205,377,223.94

Market value of collateral supporting the Repurchase Agreements is at least 102% of the Book Value. The portfolio is managed by J.P. Morgan Chase & Co. and the assets are safekept in a separate custodial account at the Federal Reserve Bank in the name of TexSTAR. The only source of payment to the Participants are the assets of TexSTAR. There is no secondary source of payment for the pool such as insurance or guarantee. Should you require a copy of the portfolio, please contact TexSTAR Participant Services.

TEXSTAR VERSUS 90-DAY TREASURY BILL



This material is for information purposes only. This information does not represent an offer to buy or sell a security. The above rate information is obtained from sources that are believed to be reliable; however, its accuracy or completeness may be subject to change. The TexSTAR management fee may be waived in full or in part at the discretion of the TexSTAR co-administrators and the TexSTAR rate for the period shown reflects waiver of fees. This table represents historical investment performance/return to the customer, net of fees, and is not an indication of future performance. An investment in the security is not insured or guaranteed by the Federal Deposit Insurance Corporation or any other government agency. Although the issuer seeks to preserve the value of an investment of \$1.00 per share, it is possible to lose money by investing in the security. Information about these and other program details are in the fund's Information Statement which should be read carefully before investing. The yield on the 90-Day Treasury Bill ("T-Bill Yield") is shown for comparative purposes only. When comparing the investment returns of the TexSTAR pool to the T-Bill Yield, you should know that the TexSTAR pool consists of allocations of specific diversified securities as detailed in the respective Information Statements. The T-Bill Yield is taken from Bloomberg Finance L.P. and represents the daily closing yield on the then current 90-Day T-Bill. The TexSTAR yield is calculated in accordance with regulations governing the registration of open-end management investment companies under the Investment Company Act of 1940 as promulgated from time to time by the federal Securities and Exchange Commission.

DAILY SUMMARY FOR AUGUST 2023

DATE	MNY MKT FUND EQUIV. [SEC Std.]	DAILY ALLOCATION FACTOR	INVESTED BALANCE	MARKET VALUE PER SHARE	WAM DAYS (1)	WAL DAYS (2)
8/1/2023	5.2933%	0.000145023	\$11,029,033,578.86	0.999753	24	49
8/2/2023	5.2909%	0.000144955	\$11,022,222,772.39	0.999762	24	49
8/3/2023	5.2889%	0.000144902	\$11,054,744,995.82	0.999758	24	49
8/4/2023	5.2864%	0.000144834	\$11,000,921,250.35	0.999781	24	48
8/5/2023	5.2864%	0.000144834	\$11,000,921,250.35	0.999781	24	48
8/6/2023	5.2864%	0.000144834	\$11,000,921,250.35	0.999781	24	48
8/7/2023	5.2877%	0.000144869	\$10,979,736,039.64	0.999776	24	48
8/8/2023	5.2874%	0.000144861	\$10,961,570,989.03	0.999759	25	49
8/9/2023	5.2875%	0.000144863	\$10,881,540,543.49	0.999757	25	49
8/10/2023	5.2934%	0.000145025	\$10,917,555,419.33	0.999763	25	48
8/11/2023	5.2937%	0.000145033	\$10,734,888,557.71	0.999762	25	49
8/12/2023	5.2937%	0.000145033	\$10,734,888,557.71	0.999762	25	49
8/13/2023	5.2937%	0.000145033	\$10,734,888,557.71	0.999762	25	49
8/14/2023	5.2949%	0.000145066	\$10,197,565,474.97	0.999742	27	51
8/15/2023	5.2996%	0.000145195	\$10,271,298,431.10	0.999738	26	51
8/16/2023	5.2996%	0.000145194	\$10,239,173,300.34	0.999750	27	51
8/17/2023	5.2974%	0.000145133	\$10,344,265,730.79	0.999747	27	51
8/18/2023	5.2946%	0.000145058	\$10,271,140,527.96	0.999761	26	50
8/19/2023	5.2946%	0.000145058	\$10,271,140,527.96	0.999761	26	50
8/20/2023	5.2946%	0.000145058	\$10,271,140,527.96	0.999761	26	50
8/21/2023	5.2948%	0.000145063	\$10,176,331,503.24	0.999767	27	50
8/22/2023	5.2995%	0.000145193	\$10,238,734,262.90	0.999762	26	50
8/23/2023	5.3018%	0.000145254	\$10,266,838,212.85	0.999743	26	50
8/24/2023	5.3043%	0.000145322	\$10,189,083,808.60	0.999739	26	50
8/25/2023	5.3049%	0.000145340	\$10,218,608,750.32	0.999732	26	49
8/26/2023	5.3049%	0.000145340	\$10,218,608,750.32	0.999732	26	49
8/27/2023	5.3049%	0.000145340	\$10,218,608,750.32	0.999732	26	49
8/28/2023	5.3090%	0.000145452	\$10,241,550,525.76	0.999731	27	50
8/29/2023	5.3155%	0.000145630	\$10,114,848,725.19	0.999744	27	50
8/30/2023	5.3161%	0.000145647	\$10,093,541,549.41	0.999734	27	50
8/31/2023	5.3186%	0.000145716	\$10,207,693,267.12	0.999773	27	50
Average	5.2974%	0.000145134	\$10,519,484,077.09		26	49



ECONOMIC COMMENTARY (cont.)

Core CPI maintained its 0.2% m/m pace but eased to 4.7% on a y/y basis. In the details, lower auto prices drove core goods lower while rising shelter costs, although showing signs of moderating, contributed to an increase in core services. Similarly, headline and core PCE both rose by 0.2% m/m. Overall, the disinflationary trend remained intact.

Developments in the labor market, on the other hand, were less clear. Whereas some data components reflected a potential slowing, the bigger picture suggests that employment remains stubbornly resilient.

The August Jobs report provided further evidence that the labor market is softening. Nonfarm payrolls rose by a stronger than expected 187K. However, revisions cut 110K jobs for the last two months, suggesting a slowdown in hiring. A large increase in the labor force pushed the unemployment rate higher to 3.8%, while wage growth came in below expectations, gaining 0.2% m/m and 4.3% y/y. The Job Openings and Labor Turnover Survey (JOLTS) data for July suggested a cooling in the labor market, with job openings falling 3.7% to 8.827 million, the lowest level since March 2021, but still above pre-pandemic levels. This brought down the ratio of job openings per unemployed worker to 1.5 from the peak of 2 in March 2022. Quits also fell by 6.7%, approaching 2019 levels, while layoffs ticked up. Overall, these reports still show decent momentum in the labor market. That said, a more balanced labor market and easing wage pressures should allow core inflation to move lower, reducing the need for the Fed to hike further.

After two months of solid gains, consumer confidence tumbled in August as the Conference Board Confidence Index fell 7.9 points to 106.1. Meanwhile, GDP for the second quarter was revised lower from 2.4% to 2.1% primarily due to downward revisions to inventories and net exports, while consumption increased at a modest 1.7%. Personal spending ran hot at 0.8% in July, despite personal income slowing to 0.2% in July, down from 0.3% in June.

At the Fed's Jackson Hole Economic Policy Symposium, Chair Powell's speech was relatively balanced. He noted that "inflation remains too high" and said that the Fed is "prepared to raise rates further if appropriate" but "will proceed carefully" if they do, reaffirming the 2% inflation target. Powell noted that his concern that the economy may not be cooling as expected.

Front-end Treasury yields were relatively rangebound as markets have priced in the expectation that the Fed has now reached the end of the rate hiking cycle. Three-month and six-month Treasury bill yields rose by 4 bps to 5.45% and 5.51%, respectively, while 12-month T-bill yields were unchanged at 5.39%. Longer-term Treasury yields rose more significantly, however, given increased expectations for U.S. Treasury supply and as strong economic data caused markets to price in higher yields for longer, which pushed out expectations for rate cuts.

Outlook

Until recently, U.S. economic data has been reaccelerating with upward revisions to full year GDP forecasts and the removal of most recession expectations. The U.S. consumer remains a key pillar of economic resilience and one of the primary reasons why it has become easier to contemplate a scenario in which the U.S. avoids a recession.

American consumption, which accounts for approximately 68% of GDP, has remained stalwart, despite a restrictive monetary environment, bolstering the overall health of the economy in 2023. Real consumption rose 0.6% m/m in July, suggesting consumption is off to a solid start in 3Q. However, excess savings is on track to be depleted by year-end as pandemic stimulus dissipates; so, maintaining the same standard of living is becoming increasingly difficult for the average American. While upper income consumers may continue to show resiliency, those in the lower income category may find themselves more stretched given the high cost of capital, especially with the upcoming resumption of student loan payments.

In a seemingly endless battle to reinstate price stability, the Fed continues to search for confirmation that policy is sufficiently restrictive and that job growth is declining. The key question is whether core inflation can make further progress towards 2% without significantly dampening the labor market and overall economic growth.

(continued page 5)



ECONOMIC COMMENTARY (cont.)

Core CPI increased 0.16% in each of the past two months, bringing the 3-month moving average down to 0.25% from 0.34% in the previous month. Nevertheless, two months does not make a trend.

Meanwhile, the employment report paints a picture of a job market heading in the right direction. Although year-over-year wages may be above the Fed's 3.5% target, which Chair Powell has said is consistent with 2% inflation, and the unemployment rate is still below the Fed's 4.1% year-end forecast, the labor market trajectory is still one of deceleration.

At this point, a September hike seems like a longshot. If inflation continues its downward path, the Fed will likely need to see a strong re-acceleration in the jobs data from here to hike in November. While we recognize that the Fed's decisions will be data dependent, we continue to believe that it is likely that the Fed will not hike again this year. As of the date of this writing, the market is assigning a 7% chance of a hike in September and a 35% chance of a hike in November. Additionally, the Fed would need to see employment materially deteriorate to implement rate cuts, which is unlikely to start before mid-2024. We believe that the U.S. economy will likely not enter a recession in 2023; however, recession risks remain for the middle of 2024.

This information is an excerpt from an economic report dated August 2023 provided to TexSTAR by JP Morgan Asset Management, Inc., the investment manager of the TexSTAR pool.

TEXSTAR BOARD MEMBERS

Monte Mercer	North Central TX Council of Government	Governing Board President
David Pate	Richardson ISD	Governing Board Vice President
Anita Cothran	City of Frisco	Governing Board Treasurer
David Medanich	Hilltop Securities	Governing Board Secretary
Jennifer Novak	J.P. Morgan Asset Management	Governing Board Asst. Sec./Treas
Brett Starr	City of Irving	Advisory Board
Sandra Newby	Tarrant Regional Water Dist/Non-Participant	Advisory Board
Ron Whitehead	Qualified Non-Participant	Advisory Board

The material provided to TexSTAR from J.P. Morgan Asset Management, Inc., the investment manager of the TexSTAR pool, is for informational and educational purposes only, as of the date of writing and may change at any time based on market or other conditions and may not come to pass. While we believe the information presented is reliable, we cannot guarantee its accuracy. HilltopSecurities is a wholly owned subsidiary of Hilltop Holdings, Inc. (NYSE: HTH) located at 717 N. Hardwood Street, Suite 3400, Dallas, TX 75201, (214) 859-1800. Member NYSE/FINRA/SIPC. Past performance is no guarantee of future results. Investment Management Services are offered through J.P. Morgan Asset Management Inc. and/or its affiliates. Marketing and Enrollment duties are offered through HilltopSecurities and/or its affiliates. HilltopSecurities and J.P. Morgan Asset Management Inc. are separate entities.



Exhibit B

Financial Statements for September 2023

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending September 30, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
REVENUE				
Operating Revenue				
Toll Revenue	153,792,700	38,533,687	25.06%	31,895,518
Video Tolls	64,352,000	13,408,972	20.84%	15,225,743
Fee Revenue	12,962,900	3,241,602	25.01%	2,655,696
Total Operating Revenue	231,107,600	55,184,260	23.88%	49,776,957
Other Revenue				
Transfer In - Cash	87,201,191	87,201,191	100.00%	-
Interest Income	24,905,700	10,563,041	42.41%	3,701,969
Grant Revenue	945,500	82,466	8.72%	-
Misc Revenue	230,000	5,609	2.44%	10,436
Total Other Revenue	113,282,391	97,852,307	86.38%	3,712,405
TOTAL REVENUE	344,389,991	153,036,568	44.44%	53,489,362
EXPENSES				
Salaries and Benefits				
Salary Expense-Regular	4,871,464	878,691	18.04%	783,682
Salary Reserve	80,000	-	-	-
TCDRS	1,591,401	162,515	10.21%	150,288
FICA	249,197	43,734	17.55%	37,282
FICA MED	70,635	12,624	17.87%	11,306
Health Insurance Expense	584,446	113,041	19.34%	93,100
Life Insurance Expense	3,817	726	19.03%	1,088
Auto Allowance Expense	10,200	2,295	22.50%	1,913
Other Benefits	166,290	17,210	10.35%	18,599
Unemployment Taxes	5,760	-	-	30
Total Salaries and Benefits	7,633,210	1,230,837	16.12%	1,097,287
Administrative				
Administrative and Office Expenses				
Accounting	9,500	2,176	22.91%	2,093
Auditing	245,000	62,100	25.35%	107,531
Financial Advisors	162,000	54,000	33.33%	54,000
Human Resources	37,500	494	1.32%	595
Legal	70,000	4,750	6.79%	1,770
IT Services	365,000	77,002	21.10%	48,662
Internet	150	-	-	-
Software Licenses	1,167,000	689,309	59.07%	31,051
Cell Phones	27,800	7,476	26.89%	3,027
Local Telephone Service	2,000	24,873	1243.63%	25,261
Overnight Delivery Services	250	-	-	40
Copy Machine	10,000	3,816	38.16%	3,816
Repair & Maintenance-General	10,000	8,445	84.45%	-
Meeting Facilities	2,000	-	-	-
Meeting Expense	13,750	489	3.55%	4,005
Toll Tag Expense	3,000	100	3.33%	100
Parking / Local Ride Share	3,550	27	0.76%	275

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending September 30, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Mileage Reimbursement	4,350	206	4.73%	557
Insurance Expense	651,000	147,556	22.67%	128,063
Rent Expense	562,540	25,020	4.45%	192,325
Building Parking	3,500	192	5.49%	425
Total Legal Services	488,000	18,793	3.85%	340
Total Administrative and Office Expenses	3,837,890	1,126,822	29.36%	603,936
Office Supplies				
Books & Publications	5,090	639	12.56%	615
Office Supplies	8,250	88	1.06%	1,163
Misc Office Equipment	4,500	-	-	-
Computer Supplies	202,100	23,650	11.70%	132,296
Copy Supplies	1,000	-	-	-
Other Reports-Printing	1,500	-	-	-
Office Supplies-Printed	2,000	102	5.10%	668
Postage Expense	550	329	59.73%	122
Total Office Supplies	224,990	24,807	11.03%	134,864
Communications and Public Relations				
Graphic Design Services	75,000	-	-	-
Website Maintenance	464,000	157,325	33.91%	23,692
Research Services	150,000	-	-	-
Communications and Marketing	400,000	12,420	3.11%	-
Advertising Expense	500,000	165,235	33.05%	56,551
Direct Mail	40,000	-	-	-
Video Production	160,000	-	-	28,359
Photography	25,000	295	1.18%	450
Radio	50,000	-	-	-
Other Public Relations	22,500	-	-	-
Promotional Items	20,000	1,166	5.83%	7,656
Annual Report printing	1,300	-	-	-
Direct Mail Printing	17,500	-	-	-
Other Communication Expenses	15,000	-	-	17,703
Total Communications and Public Relations	1,940,300	336,441	17.34%	134,411
Employee Development				
Subscriptions	750	139	18.53%	264
Agency Memberships	88,440	25	0.03%	1,200
Continuing Education	14,800	500	3.38%	-
Professional Development	20,150	-	-	375
Other Licenses	2,500	-	-	497
Seminars and Conferences	104,100	1,445	1.39%	35,310
Travel	110,500	12,852	11.63%	30
Total Employee Development	341,240	14,961	4.38%	37,676

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending September 30, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Financing and Banking Fees				
Trustee Fees	62,000	32,500	52.42%	36,000
Bank Fee Expense	3,240	1,505	46.44%	273
Continuing Disclosure	7,000	-	-	-
Arbitrage Rebate Calculation	16,300	-	-	16,300
Rating Agency Expense	45,000	32,500	72.22%	31,000
Total Financing and Banking Fees	133,540	66,505	49.80%	83,573
Total Administrative	6,477,960	1,569,536	24.23%	994,459
Operations and Maintenance				
Operations and Maintenance Consulting				
GEC-Trust Indenture Support	1,131,395	485,164	42.88%	279,930
GEC-Financial Planning Support	275,000	100,754	36.64%	66,422
GEC-Toll Ops Support	1,584,000	278,543	17.58%	154,812
GEC-Roadway Ops Support	1,605,500	259,921	16.19%	115,749
GEC-Technology Support	679,526	328,107	48.28%	160,803
GEC-Public Information Support	200,000	56,106	28.05%	48,451
GEC-General Support	1,631,820	365,306	22.39%	198,994
General System Consultant	1,381,000	36,186	2.62%	307,054
Traffic Modeling	125,000	-	-	-
Traffic and Revenue Consultant	1,010,000	60,761	6.02%	162,641
Total Operations and Maintenance Consulting	9,623,241	1,970,849	20.48%	1,494,855
Roadway Operations and Maintenance				
Roadway Maintenance	3,431,819	256,969	7.49%	1,065,486
Landscape Maintenance	2,789,256	391,010	14.02%	1,315,369
Signal & Illumination Maint	25,000	-	-	-
Maintenance Supplies-Roadway	400,000	-	-	-
Tools & Equipment Expense	-	-	-	444
Gasoline	30,000	3,729	12.43%	5,112
Repair & Maintenance - Vehicles	10,000	360	3.60%	674
Natural Gas	2,500	7,220	288.80%	1,285
Electricity - Roadways	250,000	65,136	26.05%	63,807
Total Roadway Operations and Maintenance	6,938,575	724,424	10.44%	2,452,178
Toll Processing and Collection Expense				
Image Processing	3,000,000	514,785	17.16%	1,023,675
Tag Collection Fees	11,500,000	2,682,471	23.33%	2,361,248
Court Enforcement Costs	10,000	-	-	-
ETC Incentive	500,000	-	-	-
Total Processing and Collection Expense	15,010,000	3,197,257	21.30%	3,384,923
Toll Operations Expense				
Generator Fuel	3,000	-	-	-
Fire and Burglar Alarm	500	123	24.67%	123
Refuse	2,360	474	20.08%	640

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending September 30, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Telecommunications	60,000	-	-	-
Water - Irrigation	7,500	2,252	30.03%	3,082
Electricity	750	249	33.14%	111
ETC spare parts expense	100,000	16,453	16.45%	-
Repair & Maintenance Toll Equip	50,000	-	-	31,491
Law Enforcement	600,000	118,445	19.74%	106,434
ETC Maintenance Contract	6,450,000	531,208	8.24%	666,601
Transaction Processing Maintenance Contract	2,000,000	-	-	-
ETC Toll Management Center System Operation	2,885,054	134,101	4.65%	134,510
ETC Development	650,000	65,823	10.13%	2,759
ETC Testing	225,000	-	-	-
Total Toll Operations Expense	13,034,164	869,127	6.67%	945,752
Total Operations and Maintenance	44,605,980	6,761,657	15.16%	8,277,707
Other Expenses				
Special Projects and Contingencies				
HERO	200,000	41,838	20.92%	36,957
Special Projects	100,000	-	-	-
71 Express Net Revenue Payment	5,000,000	1,621,070	32.42%	1,324,641
Customer Relations	10,000	-	-	-
Technology Initiatives	185,000	-	-	-
Other Contractual Svcs	390,000	48,000	12.31%	75,500
Contingency	200,000	-	-	-
Total Special Projects and Contingencies	6,085,000	1,710,909	28.12%	1,437,098
Non Cash Expenses				
Amortization Expense				
Amortization Expense - Software	1,228,015	6,349	0.52%	320,073
Amortization Expense - Right to Use Asset - Subscr	355,208	55,696	15.68%	-
Amortization Expense - Refundings	1,907,487	1,536,354	80.54%	1,330,277
Subtotal Amortization Expense	3,490,710	1,598,400	45.79%	1,650,351
Depreciation Expense				
Dep Exp - Furniture & Fixtures	2,178	-	-	653
Dep Expense - Equipment	476,653	155,676	32.66%	-
Dep Expense - Autos & Trucks	45,399	7,602	16.75%	13,338
Dep Expense - Buildng & Toll Fac	187,058	44,187	23.62%	44,187
Dep Expense - Highways & Bridges	48,608,788	12,709,388	26.15%	12,655,386
Dep Expense - Toll Equipment	3,917,914	759,562	19.39%	1,035,778
Dep Expense - Signs	1,641,174	302,239	18.42%	254,143
Dep Expense - Land Improvements	884,934	163,163	18.44%	221,234
Depreciation Expense - Computers	98,507	-	-	47,270
Subtotal Depreciation Expense	55,862,606	14,141,817	25.32%	14,271,988
Total Non Cash Expenses	59,353,316	15,740,216	26.52%	15,922,338
Total Other Expenses	65,438,316	17,451,125	26.67%	17,359,437

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending September 30, 2023

	Budget Amount FY 2023	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Non Operating Expenses				
Bond Issuance Expense	1,250,000	-	-	132,074
Loan Fee Expense	40,000	-	-	-
Interest Expense - Debt Obligations	95,964,098	19,698,810	20.53%	19,504,907
Interest Expense - Right to Use Assets	-	-	-	-
Transfer Out - Cash	87,201,191	87,201,191	100.00%	-
CAMPO RIF Payment	6,000,000	6,000,000	100.00%	5,000,000
Community Initiatives	645,000	-	-	-
Total Non Operating Expenses	191,100,289	112,900,002	59.08%	24,636,981
TOTAL EXPENSES	315,255,755	139,913,156	44.38%	52,365,871
Net Income	29,134,236	13,123,412		1,123,491

Central Texas Regional Mobility Authority
Balance Sheet
as of September 30, 2023

as of 09/30/2023 as of 09/30/2022

ASSETS

Current Assets

Cash

Regions Operating Account	\$ 92,051	\$ 3,518,183
Cash in TexStar	158,162	42,930
Regions Payroll Account	107,534	99,387

Restricted Cash

Goldman Sachs FSGF 465	592,768,575	1,103,383,771
Restricted Cash - TexSTAR	6,210,647	10,409,892
Overpayments account	-	291,108

Total Cash and Cash Equivalents	599,336,969	1,117,745,271
--	--------------------	----------------------

Accounts Receivables

Accounts Receivable - Net	4,979,871	2,770,089
Due From Other Agencies	346,552	65,805
Due From TTA	988,433	548,177
Due From NTTA	1,477,295	1,062,984
Due From HCTRA	3,652,916	2,065,183
Due From TxDOT	6,073,328	164,602
Interest Receivable	693,342	693,342

Total Receivables	18,211,737	7,370,183
--------------------------	-------------------	------------------

Short Term Investments

Treasuries	118,543,252	-
Agencies	339,758,036	-

Total Short Term Investments	458,301,288	-
-------------------------------------	--------------------	----------

Total Current Assets	1,075,849,994	1,125,115,454
-----------------------------	----------------------	----------------------

Construction in Progress

423,204,754	282,434,317
--------------------	--------------------

Capital Assets (Net of Depreciation and Amortization)

Depreciable Assets

Computers	-	51,237
Furniture and Fixtures	-	1,525
Equipment	1,245,411	9,624
Autos and Trucks	39,279	80,545
Buildings and Toll Facilities	4,185,774	4,372,832
Highways and Bridges	1,659,604,479	1,704,435,035
Toll Equipment	14,916,806	19,014,496
Signs	11,094,662	12,917,392
Land Improvements	5,151,172	5,978,035

Central Texas Regional Mobility Authority
Balance Sheet
as of September 30, 2023

	as of 09/30/2023	as of 09/30/2022
Right of way	88,149,606	88,149,606
Leasehold Improvements	2,116	33,176
Intangible Assets		
Computer Software	-	1,470,864
Right to Use Assets		
Leases	1,286,881	-
Subscription Based IT Arrangements	167,087	-
Total Fixed Assets	1,785,843,273	1,836,514,366
Other Assets		
Intangible Assets-Net	171,848,342	173,961,907
2005 Bond Insurance Costs	-	3,301,851
Deferred Outflows (pension related)	2,661,405	675,913
Pension Asset	1,046,634	2,549,818
Total Other Assets	175,556,381	180,489,489
Total Assets	\$ 3,460,454,402	\$ 3,424,553,625

LIABILITIES

Current Liabilities		
Accounts Payable	3,324,075	21,780,077
Construction Payable	9,796,249	5,224,110
Overpayments	1,570	294,629
Interest Payable	19,966,690	20,449,024
TCDRS Payable	82,369	74,574
Due to other Agencies	3,569	2,849
Due to TTA	625,830	624,134
Due to HCTRA	154,452	148,238
Due to Other Entities	1,878,422	57,776
71E TxDOT Obligation - ST	4,307,645	3,142,749
Total Current Liabilities	40,140,870	51,798,159
Long Term Liabilities		
Compensated Absences	240,954	268,014
Right to Use Obligations - Lease	1,286,881	-
Right to Use Obligations - SBITA	233,657	-
Deferred Inflows (pension related)	1,340,710	1,481,361
Long Term Payables	3,102,203	1,749,375

Central Texas Regional Mobility Authority
Balance Sheet
as of September 30, 2023

as of 09/30/2023 as of 09/30/2022

Bonds Payable

Senior Lien Revenue Bonds:

Senior Lien Revenue Bonds 2010	96,178,695	89,266,291
Senior Lien Revenue Bonds 2011	16,459,605	19,136,793
Senior Refunding Bonds 2013	-	3,475,000
Senior Lien Revenue Bonds 2015	10,000,000	10,000,000
Senior Lien Refunding Revenue Bonds 2016	59,340,000	70,790,000
Senior Lien Revenue Bonds 2018	44,345,000	44,345,000
Senior Lien Revenue Bonds 2020A	50,265,000	50,265,000
Senior Lien Refunding Bonds 2020B	54,970,000	55,600,000
Senior Lien Refunding Bonds 2020C	138,435,000	138,435,000
Senior Lien Revenue Bonds 2020E	167,160,000	167,160,000
Senior Lien Revenue Bonds 2021B	255,075,000	255,075,000
Senior Lien Refunding Bonds 2021D	274,150,000	274,625,000
Senior Lien Refunding Bonds 2021E	332,585,000	335,610,000
Sn Lien Rev Bnd Prem/Disc 2013	-	447,279
Senior Lien Premium 2016 Revenue Bonds	6,736,845	7,383,436
Sn Lien Revenue Bond Premium 2018	2,816,574	3,083,148
Senior Lien Revenue Bond Premium 2020A	11,112,493	11,304,305
Senior Lien Refunding Bond Premium 2020B	11,102,812	11,637,887
Senior Lien Revenue Bonds Premium 2020E	23,711,689	25,427,076
Senior Lien Revenue Bonds Premium 2021B	52,830,298	53,414,235
Senior Lien Refunding Bonds Premium 2021D	44,221,847	44,749,354
Total Senior Lien Revenue Bonds	1,651,495,859	1,671,229,804

Sub Lien Revenue Bonds:

Sub Lien Refunding Bonds 2013	-	2,725,000
Sub Lien Refunding Bonds 2016	71,435,000	72,605,000
Sub Lien Refunding Bonds 2020D	97,440,000	98,580,000
Subordinated Lien BANs 2020F	110,875,000	110,875,000
Subordinate Lien Refunding Bonds 2020G	61,570,000	61,570,000
Subordinated Lien BANs 2021C	244,185,000	244,185,000
Sub Refunding 2013 Prem/Disc	-	95,437
Sub Refunding 2016 Prem/Disc	4,797,315	5,587,450
Subordinated Lien BANs 2020F Premium	5,003,581	9,006,445
Subordinated Lien Refunding Bonds Premium 2020G	6,663,255	7,067,227
Sub Lien BANS 2021C Premium	24,737,951	32,349,629
Total Sub Lien Revenue Bonds	626,707,102	644,646,188

Central Texas Regional Mobility Authority
Balance Sheet
as of September 30, 2023

as of 09/30/2023 as of 09/30/2022

Other Obligations

TIFIA Note 2021	361,020,863	353,243,889
71E TxDOT Obligation - LT	51,918,220	55,077,264
Regions 2022 MoPac Loan	23,765,900	24,690,900
Total Other Obligations	436,704,983	433,012,053
Total Long Term Liabilities	2,718,010,147	2,750,637,420
Total Liabilities	2,758,151,017	2,802,435,579

NET ASSETS

Contributed Capital	121,462,104	121,462,104
Net Assets Beginning	567,717,870	499,532,451
Current Year Operations	13,123,412	1,123,491
Total Net Assets	702,303,386	622,118,046

Total Liabilities and Net Assets	\$ 3,460,454,402	\$ 3,424,553,625
---	-------------------------	-------------------------

Central Texas Regional Mobility Authority
Statement of Cash Flow
as of September 2023

Cash flows from operating activities:

Receipts from toll revenues	59,249,872
Receipts from Other Sources (AR)	88,075
Payments to vendors	(45,009,416)
Payments to employees	(1,236,275)
Net cash flows provided by (used in) operating activities	13,092,256

Cash flows from capital and related financing activities:

Prepaid payment on Intangible assets	(1,536,354)
Issuance Expense	(3,513,621)
Payments on bonds / loans	(452,428)
RIF Contribution	(6,000,000)
Acquisition of capital assets - non project	(528,249)
Acquisitions of construction in progress	(12,725,320)
Net cash flows provided by (used in) capital and related financing activities	(24,755,971)

Cash flows from investing activities:

Interest income	10,563,041
Purchase of investments	(235,602,845)
Proceeds from sale or maturity of investments	-
Net cash flows provided by (used in) investing activities	(225,039,804)

Net increase (decrease) in cash and cash equivalents	(276,473,905)
Cash and cash equivalents at beginning of period	894,022,611
Cash and cash equivalents at end of period	617,548,706

Reconciliation of change in net assets to net cash provided by operating activities:

Operating income	13,123,412
Adjustments to reconcile change in net assets to net cash provided by operating activities:	
Depreciation and amortization	15,740,216
Changes in assets and liabilities:	
Decrease in accounts receivable	4,065,612
Increase in prepaid expenses and other assets	147,093
Decrease in accrued expenses	(29,119,846)
Decrease in Interest expense	19,698,810
Increase in interest receivable	(10,563,041)
(Decrease) increase in Pension Asset	-
(Increase) in deferred outflows of resources	-
(Increase) in deferred inflows of resources	-
Total adjustments	(31,156)
Net cash flows provided by (used in) operating activities	\$ 13,092,256

Reconciliation of cash and cash equivalents:

Unrestricted cash and cash equivalents	18,569,484
Restricted cash and cash equivalents	598,979,222
Total	617,548,706

Investments by Fund

Fund	TexSTAR	TexSTAR- Trustee	Goldman Sachs	Agencies/ Treasuries	Balance
Renewal and Replacement Fund	8.64		708.95		717.59
Grant Fund	478,736.54		10,082,282.02		10,561,018.56
Senior Debt Service Reserve Fund	1,039,007.51		6,039,414.35	104,995,814.41	112,074,236.27
2010 Senior Lien Debt Service			63,597.75		63,597.75
2011 Sr Debt Service t			5,485,481.65		5,485,481.65
2013 Sr Debt Service t			42,155.46		42,155.46
2013 Sub Debt Service			33,177.67		33,177.67
2013 Sub Debt Service Reserve Fund	822,179.51		129.28		822,308.79
2015 Sr Debt Service			4,230,483.38		4,230,483.38
2016 Sr Lien Rev Refunding Debt Service			11,835,342.08		11,835,342.08
2016 Sub Lien Rev Refunding Debt Service			2,633,004.50		2,633,004.50
2016 Sub Lien Rev Refunding DSR			605,726.55	6,671,837.25	7,277,563.80
Operating Fund	589,881.22	158,161.73	19,472,636.84		20,220,679.79
Revenue Fund			7,707,473.77		7,707,473.77
General Fund	1,198,952.10		70,213,927.80	104,917,207.70	176,330,087.60
71E Revenue Fund			31,595,004.11		31,595,004.11
MoPac Revenue Fund			10,688,312.32		10,688,312.32
MoPac General Fund					-
MoPac Operating Fund			1,297,663.04		1,297,663.04
MoPac Loan Repayment Fund			508,218.52		508,218.52
2015B Project	368,502.39		7,947,938.30		8,316,440.69
2015 TIFIA Project	732,088.08		9,116,692.01	30,000,000.00	39,848,780.09
2011 Sr Financial Assistance Fund	16.40		28,283.42		28,299.82
2018 Sr Lien Debt Service			566,371.74		566,371.74
2018 Sr Lien Project Cap I			746.72		746.72
2018 Sr Lien Project	981,274.99		13,220,888.14		14,202,163.13
2020A Senior Lien Debt Service			640,980.04		640,980.04
2020B Senior Lien Debt Service			1,183,613.54		1,183,613.54
2020C Senior Lien Debt Service			4,870,435.65		4,870,435.65
2020D Sub Lien Debt Service			3,801,732.10		3,801,732.10
2020D Sub Debt Service Reserve Fund			457,286.11	7,987,089.95	8,444,376.06
2020E Senior Lien Project			91,783,608.01	50,000,000.00	141,783,608.01
2020E Senior Lien Project Cap Interest			15,175,484.12		15,175,484.12
2020F Sub Lien Project			0.00		-
2020F Sub Lien Deb Service			1,416,516.17		1,416,516.17
2020G Sub Lien Debt Service			652,229.84		652,229.84
2020G Sub Lien Debt Service Reserve			1,156,903.01	2,995,158.73	4,152,061.74
2021A Sub Lien Debt Service Reserve			4,360,440.34	15,974,180.00	20,334,620.34
2021A Sub Debt Service			100.40		100.40
2021B Senior Lien Cap I Project Fund			36,241,995.01		36,241,995.01
2021B Senior Lien Project			105,450,897.67	135,000,000.00	240,450,897.67
2021C Sub Lien Cap I Project Fund			1,401.33		1,401.33
2021C Sub Lien Project			90,421,822.05		90,421,822.05
2021C Sub Lien Debt Service			3,119,792.09		3,119,792.09
2021D Senior Lien Debt Service			3,239,207.21		3,239,207.21
2021E Senior Lien Debt Service			4,790,165.35		4,790,165.35
Totals	6,210,647.38	158,161.73	582,180,270.41	458,541,288.04	1,047,090,367.56

CTRMA INVESTMENT REPORT

Month Ending September 30, 2023

	Balance 9/1/2023	Accrued Interest	Additions	Cash Transfers	Withdrawals	Balance 9/30/2023	Rate Sept
Amount in Trustee TexStar							
2011 Sr Lien Financial Assist Fund	16.36	0.04				16.40	5.3105%
2013 Sub Lien Debt Service Reserve	818,606.47	3,573.04				822,179.51	5.3105%
General Fund	1,193,741.70	5,210.40				1,198,952.10	5.3105%
Trustee Operating Fund	3,085,873.43	4,007.79		(2,500,000.00)		589,881.22	5.3105%
Renewal and Replacement	8.63	0.01				8.64	5.3105%
TxDOT Grant Fund	476,656.03	2,080.51				478,736.54	5.3105%
Senior Lien Debt Service Reserve Fund	1,034,492.18	4,515.33				1,039,007.51	5.3105%
2015B Sr Ln Project	366,900.95	1,601.44				368,502.39	5.3105%
2015C TIFIA Project	728,906.58	3,181.50				732,088.08	5.3105%
2018 Sr Lien Project	977,010.57	4,264.42				981,274.99	5.3105%
	8,682,212.90	28,434.48	-	(2,500,000.00)	-	6,210,647.38	

Amount in TexStar Operating Fund	304,100.30	4,061.43		2,500,000.00	2,650,000.00	158,161.73	5.3105%
---	-------------------	-----------------	--	---------------------	---------------------	-------------------	----------------

Goldman Sachs

Operating Fund	15,293,149.54	54,380.84	128,885.23	4,000,000.00	3,778.77	19,472,636.84	5.2100%
2020A Senior Lien Debt Service	430,317.02	1,225.52		209,437.50		640,980.04	5.2100%
2020B Senior Lien Debt Service	903,405.04	3,100.17		277,108.33		1,183,613.54	5.2100%
2020C Senior Lien Debt Service	4,113,189.40	6,901.56		750,344.69		4,870,435.65	5.2100%
2020D Sub Lien Debt Service	3,209,311.03	12,318.31		580,102.76		3,801,732.10	5.2100%
2020D Sub Debt Service Reserve Fund	455,270.53	2,015.58				457,286.11	5.2100%
2020E Sr Lien Project	91,825,227.68	518,839.36			560,459.03	91,783,608.01	5.2100%
2020E Sr Ln Project Cap Interest	15,108,595.33	66,888.79				15,175,484.12	5.2100%
2020E Sr Lien Debt Service	0.00					0.00	5.2100%
2020F Sub Lien Project	44,466.13				44,466.13	0.00	5.2100%
2020F Sub Lien Debt Service	951,826.56	2,710.44		461,979.17		1,416,516.17	5.2100%
2020G Sub Lien Debt Service	438,265.16	1,248.01		212,716.67		652,229.84	5.2100%
2020G Sub Debt Service Reserve Fund	791,657.75	3,376.42		361,868.84		1,156,903.01	5.2100%
2021A Sub Debt Service Reserve Fund	2,270,886.96	8,210.20		2,081,343.18		4,360,440.34	5.2100%
2021A TIFIA Sub Lien Debt Service Acct	99.96	0.44				100.40	5.2100%
2021A TIFIA Sub Lien Debt Service Acct	0.00			585,082.17		585,082.17	5.2100%
2021B Senior Lien Cap I Project Fund	36,082,251.50	159,743.51				36,241,995.01	5.2100%
2021B Senior Lien Project	104,787,374.96	663,522.71				105,450,897.67	5.2100%
2021B Senior Lien Cap I Debt Service	0.00					0.00	5.2100%
2021C Sub Lien Cap I Project Fund	1,395.15	6.18				1,401.33	5.2100%
2021C Sub Lien Project	99,001,051.73	420,434.55			8,999,664.23	90,421,822.05	5.2100%
2021C Sub Lien Debt Service	2,096,384.89	5,969.70		1,017,437.50		3,119,792.09	5.2100%
2021D Senior Lien Debt Service	2,257,880.93	6,826.28		974,500.00		3,239,207.21	5.2100%
2021E Senior Lien Debt Service	3,712,753.07	12,984.54		1,064,427.74		4,790,165.35	5.2100%
2011 Sr Financial Assistance Fund	28,158.74	124.68				28,283.42	5.2100%
2010 Senior DSF	63,317.39	280.36				63,597.75	5.2100%
2011 Senior Lien Debt Service	4,863,815.80	19,582.52		602,083.33		5,485,481.65	5.2100%
2013 Senior Lien Debt Service	41,969.63	185.83				42,155.46	5.2100%
2013 Sub Debt Service Reserve Fund	128.71	0.57				129.28	5.2100%
2013 Subordinate Debt Service	33,031.41	146.26				33,177.67	5.2100%
2015A Sr Lien Debt Service	4,170,351.15	18,465.56		41,666.67		4,230,483.38	5.2100%
2015B Project	7,940,384.97	35,175.95			27,622.62	7,947,938.30	5.2100%
2015C TIFIA Project	9,076,502.90	40,189.11				9,116,692.01	5.2100%
2016 Sr Lien Rev Refunding Debt Service	9,451,488.10	37,975.85		2,345,878.13		11,835,342.08	5.2100%
2016 Sub Lien Rev Refunding Debt Service	2,157,284.44	8,031.52		467,688.54		2,633,004.50	5.2100%
2016 Sub Lien Rev Refunding DSR	603,056.33	2,670.22				605,726.55	5.2100%
2018 Sr Lien Project Cap I	743.43	3.29				746.72	5.2100%
2018 Sr Lien Debt Service	380,517.40	1,083.51		184,770.83		566,371.74	5.2100%
2018 Sr Lien Project	13,162,787.93	58,100.21				13,220,888.14	5.2100%
TxDOT Grant Fund	10,037,836.30	44,445.72				10,082,282.02	5.2100%
Renewal and Replacement	57.76	1.46		53,830.00	53,180.27	708.95	5.2100%
Revenue Fund	2,262,971.25	51,972.96	17,989,142.42	(12,491,528.62)	105,084.24	7,707,473.77	5.2100%
General Fund	75,906,289.05	306,362.92	82,465.90	(5,409,434.53)	671,755.54	70,213,927.80	5.2100%
Senior Lien Debt Service Reserve Fund	6,012,790.80	26,623.55				6,039,414.35	5.2100%
71E Revenue Fund	30,467,902.42	131,592.94	383,268.69	729,572.01	117,331.95	31,595,004.11	5.2100%
MoPac Revenue Fund	0.00	840.44	347,599.02	(275,150.04)		73,289.42	5.2100%
MoPac General Fund	16,060,730.22	68,823.41		603,645.95	6,044,887.26	10,688,312.32	5.2100%
MoPac Operating Fund	1,049,817.82	3,557.27	125,990.00	400,000.00	281,702.05	1,297,663.04	5.2100%
MoPac Loan Repayment Fund	336,784.00	805.34		170,629.18		508,218.52	5.2100%
	577,883,478.27	2,807,744.56	19,057,351.26	-	16,909,932.09	582,838,642.00	

Amount in Fed Agencies and Treasuries

Amortized Principal	458,541,288.04					458,541,288.04	
---------------------	----------------	--	--	--	--	----------------	--

Certificates of Deposit

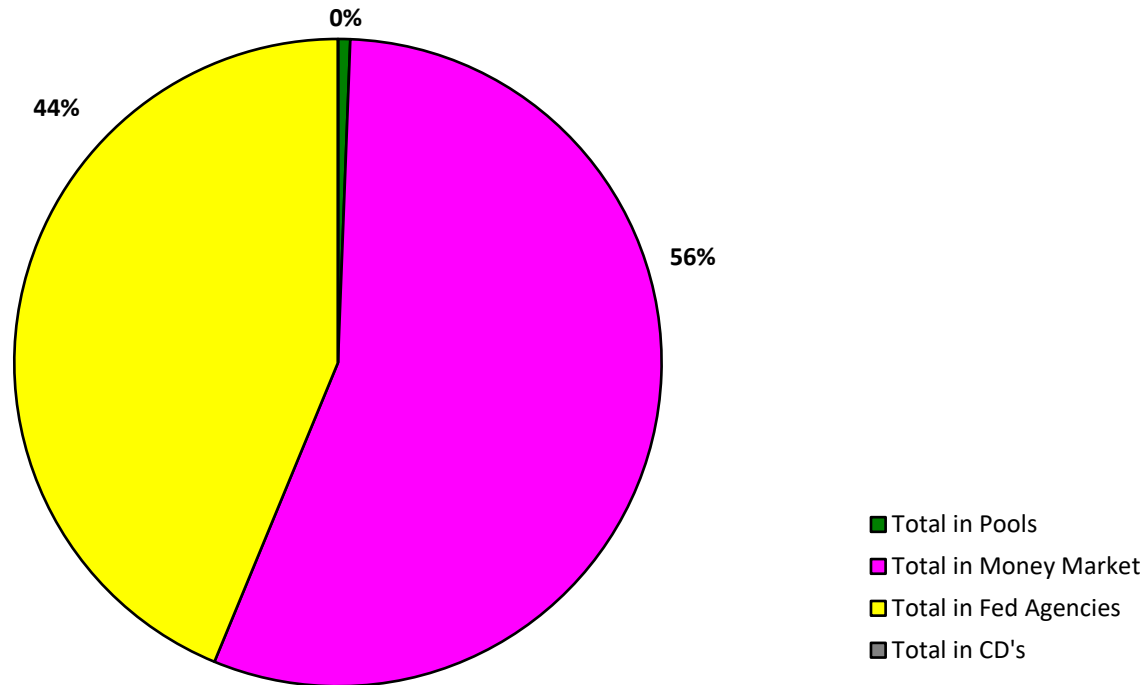
Total in Pools - TxStar	8,986,313.20	32,495.91	-	-	2,650,000.00	6,368,809.11	
Total in GS FSGF	577,883,478.27	2,807,744.56	19,057,351.26	-	16,909,932.09	582,838,642.00	
Total in Fed Agencies and Treasuries	458,541,288.04	-	-	-	-	458,541,288.04	
Total Invested	1,045,411,079.51	2,840,240.47	19,057,351.26	-	19,559,932.09	1,047,748,739.15	

All Investments in the portfolio are in compliance with the CTRMA's Investment policy and the relevant provisions of the Public Funds Investment Act Chapter 2256.02:

José Hernández, CFO
Ann Zigmund, Controller

9/30/2023

Allocation of Funds



Goldman Sachs Escrow Funds

	Balance		Accrued		Balance
	9/1/2023	Additions	Interest	Withdrawals	9/30/2023
Travis County Escrow Fund - Elroy Road	3,010,667.50		13,331.05		3,023,998.55
Travis County Escrow Fund - Ross Road	164,644.29		728.99		165,373.28
Travis County Escrow Fund - Old San Antonio Road	31,719.54		140.46		31,860.00
Travis County Escrow Fund - Old Lockhart Road	133,158.58		586.48		133,745.06
Travis County Escrow Fund - County Line Road	218,738.50	5,659,349.84	969.09	558.23	5,878,499.20
Travis County Escrow Fund - South Pleasant Valley Road	303,764.46	1,346.45			305,110.91
Travis County Escrow Fund - Thaxton Road	111,291.84	494.50			111,786.34
Travis County Escrow Fund - Pearce Lane Road	278,326.89	1,232.73			279,559.62
	4,252,311.60	5,662,423.52	15,756.07	558.23	9,929,932.96

	Amount of In							
Bank	FUND	COST	Cummulative Amortization	Book Value	Maturity Value	Interest Income		
						Accrued Interest	Amortization	Interest Earned
6180006366	2016SUBDSR	6,671,837.25		6,671,837.25				-
1001017484	2020D DSRF	7,987,089.95		7,987,089.95	8,200,000.00			-
1001021540	2020G DSRF	2,995,158.73		2,995,158.73	3,075,000.00			-
1001021543	2021A DSRF	15,974,180.00		15,974,180.00	16,400,000.00			-
6180000120	GENERAL	20,000,000.00		20,000,000.00	20,000,000.00			-
6180000120	GENERAL	19,973,592.19		19,973,592.19	20,500,000.00			-
6180000120	GENERAL	44,963,937.40		44,963,937.40	47,150,000.00	3,864.75		3,864.75
6180000059	SENLINDSR	20,000,000.00		20,000,000.00	20,000,000.00	22,222.22		22,222.22
6180000059	SENLINDSR	20,000,000.00		20,000,000.00	20,000,000.00			-
6180000059	SENLINDSR	45,000,000.00		45,000,000.00	45,000,000.00			-
6180000059	SENLINDSR	19,973,592.19		19,973,592.19	20,500,000.00			-
6180000120	GENERAL	9,960,128.90		9,960,128.90	10,000,000.00	27,777.78		27,777.78
6180000120	GENERAL	9,960,128.90		9,960,128.90	10,000,000.00	27,777.78		27,777.78
6180005349	2015TIFIAP	30,000,000.00		30,000,000.00	30,000,000.00			-
1001021273	2021BPROJ	35,000,000.00		35,000,000.00	35,000,000.00			-
1001021533	2020E PRJ	50,000,000.00		50,000,000.00	50,000,000.00			-
1001021273	2021BPROJ	50,000,000.00		50,000,000.00	50,000,000.00			-
1001021273	2021BPROJ	50,000,000.00		50,000,000.00	50,000,000.00			-
		458,459,645.51	-	458,459,645.51	455,825,000.00	81,642.53	-	81,642.53

TexSTAR
MONTHLY NEWSLETTER
SEPTEMBER
2023



PERFORMANCE

As of September 30, 2023

Current Invested Balance	\$ 9,992,445,950.80
Weighted Average Maturity (1)	30 Days
Weighted Average Life (2)	57 Days
Net Asset Value	0.999816
Total Number of Participants	1028
Management Fee on Invested Balance	0.06%*
Interest Distributed	\$ 44,553,431.86
Management Fee Collected	\$ 496,951.28
% of Portfolio Invested Beyond 1 Year	3.63%
Standard & Poor's Current Rating	AAAm

Rates reflect historical information and are not an indication of future performance.

September Averages

Average Invested Balance	\$ 10,093,864,488.70
Average Monthly Yield, on a simple basis	5.3105%
Average Weighted Maturity (1)	29 Days
Average Weighted Life (2)	56 Days

Definition of Weighted Average Maturity (1) & (2)

(1) This weighted average maturity calculation uses the SEC Rule 2a-7 definition for stated maturity for any floating rate instrument held in the portfolio to determine the weighted average maturity for the pool. This Rule specifies that a variable rate instruction to be paid in 397 calendar days or less shall be deemed to have a maturity equal to the period remaining until the next readjustment of the interest rate.
 (2) This weighted average maturity calculation uses the final maturity of any floating rate instruments held in the portfolio to calculate the weighted average maturity for the pool.

The maximum management fee authorized for the TexSTAR Cash Reserve Fund is 12 basis points. This fee may be waived in full or in part in the discretion of the TexSTAR co-administrators at any time as provided for in the TexSTAR Information Statement.

NEW PARTICIPANTS

We would like to welcome the following entities who joined the TexSTAR program in September:

- * City of Blue Mound * Galveston County Municipal Utility District No. 79 * Jacksboro Independent School District
- * Montgomery County Municipal Utility District No. 211 * Pantego Economic Development Corporation

HOLIDAY REMINDER

In observance of **Columbus Day, TexSTAR will be closed on Monday, October 9, 2023**. All ACH transactions initiated on Friday, October 6th will settle on Tuesday, October 10th. Standard transaction deadlines will be observed on Friday, October 6th. Please plan accordingly for your liquidity needs.

ECONOMIC COMMENTARY

Market review

In the third quarter, easing inflation and stronger economic growth helped fuel optimism for a soft landing of the U.S. economy. However, monthly data suggest economic momentum is slowing, and we may not be out of the woods just yet. The quarter was less exciting for financial markets, which struggled as investors re-positioned for higher rates for longer. In fact, one of the few asset classes that saw positive gains short term fixed income portfolios and funds.

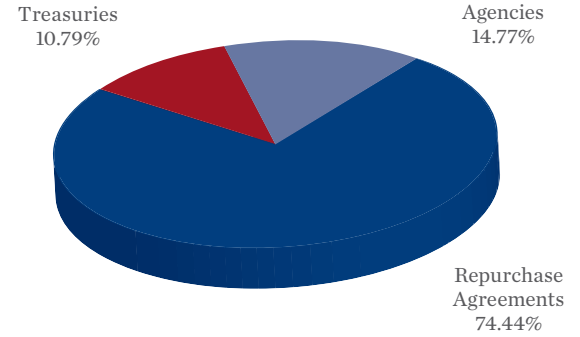
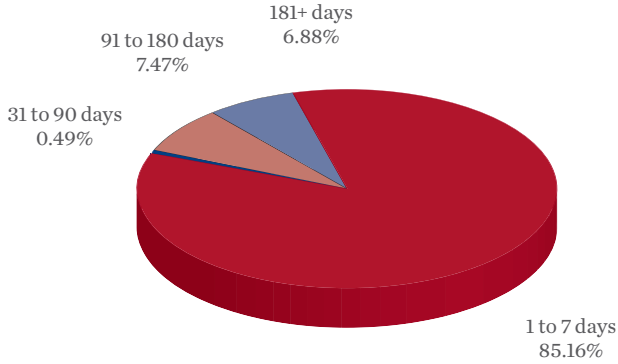
After nearly two years of hot inflation, a sustained inflation downtrend is now underway. The August CPI report showed continued progress on core inflation while energy contributed to a bounce in headline inflation. Headline CPI rose 0.6% month-over-month (m/m) seasonally adjusted and 3.7% year-over-year (y/y) non-seasonally adjusted, an acceleration compared to last month. This increase was largely anticipated and primarily driven by a 5.6% surge in energy prices, as consumer prices rose a more modest 0.3% excluding energy. Core CPI rose 0.3% m/m and eased to 4.3% on a y/y basis. In the details, shelter inflation continued to moderate while transportation services saw strong gains. However, moderating new and used vehicle prices in the months ahead should help ease core inflationary pressures. Similarly, headline PCE inflation accelerated to 3.5% y/y while core PCE eased to 3.9%. Moving forward, we expect that the impact of oil price spikes will be limited.

Labor market strength is gradually easing. The pace of job gains, while still robust, has been trending lower since last year. Improved labor force participation has so far supported job growth, with the participation rate for adults aged 25-54 having fully recovered to pre-pandemic levels. Wage inflation remains sticky but has been moderating. Wage growth has now come down to 4.3% y/y in August from a peak of 5.9% in March 2022. Weekly initial jobless claims for unemployment averaged 232K in the third quarter.

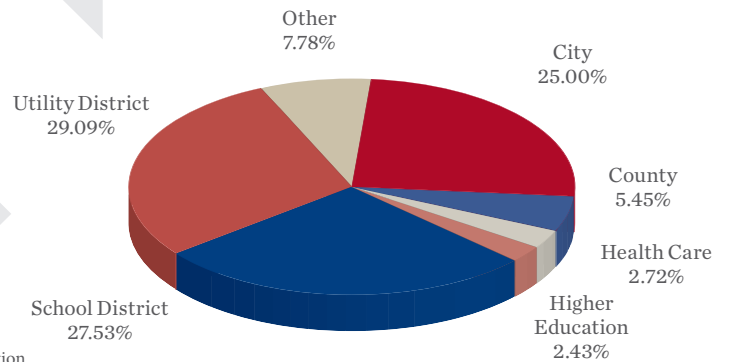
(continued page 4)

INFORMATION AT A GLANCE

PORTFOLIO BY TYPE OF INVESTMENT AS OF SEPTEMBER 30, 2023



PORTFOLIO BY MATURITY AS OF SEPTEMBER 30, 2023 (1)



DISTRIBUTION OF PARTICIPANTS BY TYPE AS OF SEPTEMBER 30, 2023

(1) Portfolio by Maturity is calculated using WAM (1) definition for stated maturity. See page 1 for definition

HISTORICAL PROGRAM INFORMATION

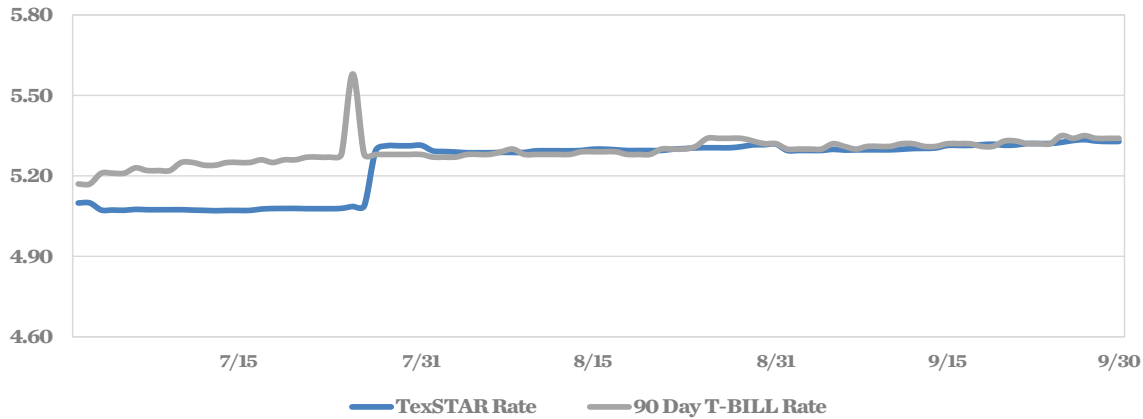
MONTH	AVERAGE RATE	BOOK VALUE	MARKET VALUE	NET ASSET VALUE	WAM (1)	WAL (2)	NUMBER OF PARTICIPANTS
Sep 23	5.3105 %	\$9,992,445,950.80	\$9,990,730,955.61	0.999816	29	56	1028
Aug 23	5.2974%	10,207,693,267.12	10,205,377,223.94	0.999773	26	49	1023
Jul 23	5.1148%	10,852,471,505.08	10,849,665,890.42	0.999741	22	47	1021
Jun 23	5.0764%	10,475,876,514.08	10,473,945,855.73	0.999806	22	50	1020
May 23	5.0471%	10,704,350,596.85	10,702,720,616.60	0.999847	20	45	1019
Apr 23	4.8292%	10,940,711,794.05	10,941,057,413.24	1.000031	17	42	1017
Mar 23	4.6066%	11,042,113,205.98	11,042,864,910.32	1.000029	11	39	1012
Feb 23	4.4919%	10,962,890,240.57	10,961,778,645.78	0.999898	9	38	1008
Jan 23	4.2515%	10,451,037,339.95	10,450,044,625.54	0.999905	6	41	1003
Dec 22	3.9681%	9,016,826,910.67	9,015,709,981.89	0.999855	5	43	999
Nov 22	3.5588%	8,393,118,851.17	8,390,786,906.73	0.999722	6	47	998
Oct 22	2.8531%	8,388,414,626.87	8,384,901,873.82	0.999581	10	46	996

PORTFOLIO ASSET SUMMARY AS OF SEPTEMBER 30, 2023

	BOOK VALUE	MARKET VALUE
Uninvested Balance	\$ 688.21	\$ 688.21
Accrual of Interest Income	22,688,328.56	22,688,328.56
Interest and Management Fees Payable	(44,540,141.00)	(44,540,141.00)
Payable for Investment Purchased	0.00	0.00
Repurchase Agreement	7,454,316,999.79	7,454,316,999.79
Government Securities	2,559,980,075.24	2,558,265,080.05
TOTAL	\$ 9,992,445,950.80	\$ 9,990,730,955.61

Market value of collateral supporting the Repurchase Agreements is at least 102% of the Book Value. The portfolio is managed by J.P. Morgan Chase & Co. and the assets are safekept in a separate custodial account at the Federal Reserve Bank in the name of TexSTAR. The only source of payment to the Participants are the assets of TexSTAR. There is no secondary source of payment for the pool such as insurance or guarantee. Should you require a copy of the portfolio, please contact TexSTAR Participant Services.

TEXSTAR VERSUS 90-DAY TREASURY BILL



This material is for information purposes only. This information does not represent an offer to buy or sell a security. The above rate information is obtained from sources that are believed to be reliable; however, its accuracy or completeness may be subject to change. The TexSTAR management fee may be waived in full or in part at the discretion of the TexSTAR co-administrators and the TexSTAR rate for the period shown reflects waiver of fees. This table represents historical investment performance/return to the customer, net of fees, and is not an indication of future performance. An investment in the security is not insured or guaranteed by the Federal Deposit Insurance Corporation or any other government agency. Although the issuer seeks to preserve the value of an investment of \$1.00 per share, it is possible to lose money by investing in the security. Information about these and other program details are in the fund's Information Statement which should be read carefully before investing. The yield on the 90-Day Treasury Bill ("T-Bill Yield") is shown for comparative purposes only. When comparing the investment returns of the TexSTAR pool to the T-Bill Yield, you should know that the TexSTAR pool consists of allocations of specific diversified securities as detailed in the respective Information Statements. The T-Bill Yield is taken from Bloomberg Finance L.P. and represents the daily closing yield on the then current 90-Day T-Bill. The TexSTAR yield is calculated in accordance with regulations governing the registration of open-end management investment companies under the Investment Company Act of 1940 as promulgated from time to time by the federal Securities and Exchange Commission.

DAILY SUMMARY FOR SEPTEMBER 2023

DATE	MNY MKT FUND EQUIV. [SEC Std.]	DAILY ALLOCATION FACTOR	INVESTED BALANCE	MARKET VALUE PER SHARE	WAM DAYS (1)	WAL DAYS (2)
9/1/2023	5.2947%	0.000145060	\$10,150,289,718.88	0.999804	27	50
9/2/2023	5.2947%	0.000145060	\$10,150,289,718.88	0.999804	27	50
9/3/2023	5.2947%	0.000145060	\$10,150,289,718.88	0.999804	27	50
9/4/2023	5.2947%	0.000145060	\$10,150,289,718.88	0.999804	27	50
9/5/2023	5.2989%	0.000145174	\$10,187,547,284.60	0.999777	27	53
9/6/2023	5.2962%	0.000145100	\$10,163,186,946.99	0.999779	27	53
9/7/2023	5.2968%	0.000145119	\$10,122,935,905.70	0.999773	27	53
9/8/2023	5.2971%	0.000145126	\$10,155,877,098.53	0.999786	27	52
9/9/2023	5.2971%	0.000145126	\$10,155,877,098.53	0.999786	27	52
9/10/2023	5.2971%	0.000145126	\$10,155,877,098.53	0.999786	27	52
9/11/2023	5.2992%	0.000145183	\$10,200,180,265.84	0.999778	28	53
9/12/2023	5.3018%	0.000145256	\$10,278,685,601.56	0.999790	28	56
9/13/2023	5.3025%	0.000145275	\$10,337,867,157.92	0.999810	28	56
9/14/2023	5.3041%	0.000145317	\$10,211,821,190.92	0.999808	28	56
9/15/2023	5.3135%	0.000145575	\$10,166,408,096.27	0.999811	29	57
9/16/2023	5.3135%	0.000145575	\$10,166,408,096.27	0.999811	29	57
9/17/2023	5.3135%	0.000145575	\$10,166,408,096.27	0.999811	29	57
9/18/2023	5.3163%	0.000145652	\$10,069,542,232.34	0.999801	30	58
9/19/2023	5.3181%	0.000145702	\$10,087,639,347.86	0.999807	31	59
9/20/2023	5.3140%	0.000145589	\$10,063,497,654.15	0.999803	31	59
9/21/2023	5.3153%	0.000145624	\$9,929,491,072.90	0.999799	32	60
9/22/2023	5.3207%	0.000145772	\$9,853,526,609.39	0.999801	32	60
9/23/2023	5.3207%	0.000145772	\$9,853,526,609.39	0.999801	32	60
9/24/2023	5.3207%	0.000145772	\$9,853,526,609.39	0.999801	32	60
9/25/2023	5.3251%	0.000145893	\$9,952,707,704.94	0.999797	31	59
9/26/2023	5.3318%	0.000146077	\$10,063,656,735.35	0.999792	31	58
9/27/2023	5.3349%	0.000146163	\$10,087,419,330.05	0.999788	30	57
9/28/2023	5.3299%	0.000146024	\$9,946,270,040.13	0.999792	31	58
9/29/2023	5.3282%	0.000145978	\$9,992,445,950.80	0.999816	30	57
9/30/2023	5.3282%	0.000145978	\$9,992,445,950.80	0.999816	30	57
Average	5.3105%	0.000145492	\$10,093,864,488.70		29	56



ECONOMIC COMMENTARY (cont.)

While this is above its average of 214K in 2022, the levels are still indicative of a healthy labor market and have been trending lower more recently. The Job Openings and Labor Turnover Survey (JOLTS) data for August surprised to the upside as job openings surged 7.7% to 9.6 million, up from 8.8 million in the month prior, while quits rose a modest 0.5%. The ratio of vacancies to unemployed workers remained unchanged from July at 1.5. Job openings have been volatile around a declining trend, but the data remain well above pre-pandemic norms.

Given the strength in the labor market is not surprising that the consumer has been the primary driver of the economy so far, but consumer confidence has begun to falter. The Conference Board Consumer Confidence Index fell for the second straight month, from 106.1 in August to 103 in September, reflecting a decline in consumers' assessment of future business conditions. Personal spending in August showed a deceleration relative to July, at a 0.4% m/m change, down from 0.8%. The GDP revisions had limited impact on the headline growth profile, as second quarter GDP was unchanged at a 2.1% annualized rate. In the details of the revision, the composition shifted from consumption to business investment: consumption grew a modest 0.8% annualized rate while business fixed investment spending grew 5.2%, its best pace since IQ22. Comprehensive GDP revisions painted a picture of private sector resilience and improved household savings with softer consumption growth than previously reported.

In a widely anticipated move, the Federal Open Market Committee (FOMC) voted to leave the federal funds rate unchanged at a range of 5.25% to 5.50% at its September meeting and reiterated its commitment to a data-driven approach. The updated "dot plot" remained hawkish, with the median FOMC member now expecting only two cuts in 2024, reinforcing the "higher for longer" message. Notably, its updated economic forecasts leaned strongly into the soft-landing narrative. In the Summary of Economic Projections, real GDP growth expectations rose meaningfully for 2023 and 2024. Elsewhere, the median forecast for the unemployment rate fell to 3.8% while the core PCE forecast ticked lower.

September was a challenging month for markets and for Congress. As the month ended, in a surprise turnaround just 3 hours before the deadline, Congress averted a government shutdown, passing a short-term continuing resolution to keep the government running through November 17th. Improved prospects for growth and incoming supply, against the backdrop of 'higher for longer' policy rates pushed longer term yields to their highest levels since 2007, with two-year and 10-year Treasury yields up 18 bps and 47 bps on the month to 5.05% and 4.57% respectively. Meanwhile three-month Treasury bill yields remained unchanged at 5.45%, and six-month T-bill yields increased a modest 4 bps to 5.55%. Moreover, the potential government shutdown (which was averted in the 11th hour), United Auto Workers (UAW) labor strikes and higher oil prices have weighed on investor sentiment.

Outlook

"Resiliency" has been the buzzword of 2023, with better-than-expected economic growth and corporate profits coupled with milder drags from credit tightening and business spending contraction raising hopes for a soft landing. Economic data has underscored the strength of U.S. consumers and labor markets, aided by falling inflation.

Nevertheless, the clouds of recession have not departed, as growing drags from higher energy prices, declining pandemic excess savings and the lagged effects of monetary policy suggest it is far too soon to call an "all clear" on a U.S. recession.

Business spending has held up more strongly than expected due to higher spending on manufacturing and slowing corporate profits could still constrain growth in capital expenditures. Consumers have remained resilient in the third quarter, supported by solid job growth and rising real wages. So far in 2023, excess consumer savings and the use of credit have kept consumption as a pillar of strength in the U.S. economy.

However, consumer savings balances have shrunk as they take on more debt to maintain current spending, and delinquencies are starting to rise. By our measures, pandemic excess savings has declined to \$1.1 trillion from its peak of \$2.3 trillion, leading consumers to draw on revolving credit to finance their spending habits.

(continued page 5)



ECONOMIC COMMENTARY (cont.)

Revolving credit as a share of disposable income doesn't look too worrying yet (at 6.3% in June compared to 6.5% pre-pandemic), but delinquencies for credit cards and auto loans are starting to rise. This, along with the lagged impacts of monetary tightening, higher energy prices, and the forthcoming resumption of student loan payments, should weigh on consumer spending in the coming months.

Other risks to growth are accumulating as we enter the fall. While a U.S. government shutdown was averted, Congress merely kicked the can down the road until November. The odds of a government shutdown later this year have arguably risen but would probably be temporary if it happens (a few weeks at most) until political and market pressures force everyone to keep the government open. Historically, the economic impact has tended to be short-lived and reversed the following period. Additionally, the United Auto Workers (UAW) strike continues to escalate, as progress between the UAW and automakers has not improved yet. Should it build further, the strike could negatively impact economic activity and pressure inflation upward.

Overall, the U.S. economy should continue to grow at a moderate but slowing pace from here, and while a near-term recession is not guaranteed, a slower-moving economy will be increasingly sensitive to shocks. With risks remaining on the horizon, we see at least a 50/50 chance of a recession starting by the end of 2024, and a greater chance of a recession in 2025 if one fails to materialize earlier.

This information is an excerpt from an economic report dated September 2023 provided to TexSTAR by JP Morgan Asset Management, Inc., the investment manager of the TexSTAR pool.

TEXSTAR BOARD MEMBERS

Monte Mercer	North Central TX Council of Government	Governing Board President
David Pate	Richardson ISD	Governing Board Vice President
Anita Cothran	City of Frisco	Governing Board Treasurer
David Medanich	Hilltop Securities	Governing Board Secretary
Jennifer Novak	J.P. Morgan Asset Management	Governing Board Asst. Sec./Treas
Brett Starr	City of Irving	Advisory Board
Sandra Newby	Tarrant Regional Water Dist/Non-Participant	Advisory Board
Ron Whitehead	Qualified Non-Participant	Advisory Board

The material provided to TexSTAR from J.P. Morgan Asset Management, Inc., the investment manager of the TexSTAR pool, is for informational and educational purposes only, as of the date of writing and may change at any time based on market or other conditions and may not come to pass. While we believe the information presented is reliable, we cannot guarantee its accuracy. HilltopSecurities is a wholly owned subsidiary of Hilltop Holdings, Inc. (NYSE: HTH) located at 717 N. Hardwood Street, Suite 3400, Dallas, TX 75201, (214) 859-1800. Member NYSE/FINRA/SIPC. Past performance is no guarantee of future results. Investment Management Services are offered through J.P. Morgan Asset Management Inc. and/or its affiliates. Marketing and Enrollment duties are offered through HilltopSecurities and/or its affiliates. HilltopSecurities and J.P. Morgan Asset Management Inc. are separate entities.





CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #6

Discuss and consider amending the
Mobility Authority Policy Code §
301.002(c) to modify the minimum
toll rates for the Mopac Express Lanes
and adding a new Mobility Authority
Policy Code § 301.0075 regarding
Prepaid License Plate Billing

Strategic Plan Relevance:	Stewardship
Department:	Finance
Contact:	José Hernández, Chief Financial Officer
Associated Costs:	N/A
Funding Source:	N/A
Action Requested:	Consider and act on draft resolution

Background – MoPac Managed Lanes - Section 301.002(a) of the Policy Code states that “the authority shall establish toll rates for each tolled facility operated by the authority. For the proposed action on the MoPac managed lanes, the Policy Code has stipulated five cent annual increases to the minimum toll rate annually for each segment to reach the current minimum rate of \$0.50 per segment. Currently Section 3001.003 of the Policy Code specifies the MoPac minimum rates to increase annually each January 1st, formulaically by the unadjusted index of Consumer Prices for All Urban Consumers (CPI_U) as recorded in October of the prior year. In order for the minimum toll rates on the MoPac managed lanes to be consistent with those of the 183N upon opening, it is recommended that the MoPac minimum rates be increased incrementally annually to reach \$0.73 per segment by January 1, 2026. The proposed annual incremental increases are seven cents for calendar 2024, followed by eight cents in each of calendar 2025 and 2026.

Prepaid License Plate Billing - In addition to transponder billing offered by the Mobility Authority as a prepaid account payment option, staff is proposing an additional billing and payment option for vehicles with a prepaid account using Authority toll roads without a transponder attached to the vehicle (typically on the windshield). In order to collect from prepaid accounts for vehicles without transponders, the Authority relies

upon the review of license plate images from those vehicles to match them with the appropriate prepaid accounts. This image review process incurs additional operational costs for the Authority. Images may be reviewed electronically or manually and also results in additional costs for the data platform billing processes. Therefore, staff is recommending the addition of a Prepaid License Plate Billing account rate tier to the Policy Code which would add 10 percent to the applicable transponder billing rate for vehicles with prepaid accounts that do not have a transponder attached to the vehicle.

Previous Actions - MoPac Managed Lanes - The minimum toll rates per segment for the CTRMA MoPac Managed Lanes have increased over the past six years as shown below.

Year	2018	2019	2020	2021	2022	2023
Minimum toll rate per segment	\$0.25	\$0.25	\$0.30	\$0.35	\$0.45	\$0.50
Increase/segment		\$0.00	\$0.05	\$0.05	\$0.10	\$0.05

Future Minimum Toll Rate Increases for MoPac Express Lanes - The proposed action would amend Section 301.002(c) of the Policy Code to provide that the minimum toll rate per segment for the MoPac Express Lanes will be adjusted annually each January 1st by \$0.07 per segment for calendar 2024, \$0.08 per segment for calendar 2025, and \$0.08 per segment for calendar 2026 until the minimum toll rate is \$0.73. Thereafter, the minimum toll rate per segment would follow the CPI_U annual adjustment outlined in Section 301.003 of the Policy Code..

Addition of Prepaid License Plate Billing to the Policy Code - The proposed action would add a new section to the Policy Code, Section 301.0075 Prepaid License Plate Billing, as a new rate tier for prepaid accounts for vehicles using Authority toll roads that do not have a transponder attached to them and instead utilize license plate image review for billing and payment. The new rate tier would be 10 percent higher than the applicable electronic transponder rate and is intended to offset the additional cost associated with processing transactions for payment for vehicles that do not present a tag when using Mobility Authority toll roads.

Staff Recommendation - Staff recommends adopting seven cent increase to MoPac Express Lanes gantries, bringing the minimum toll rate per segment to \$0.57 for calendar 2024, followed by two consecutive eight cent increases annually in the subsequent two calendar years to be effective for calendar 2025 and 2026, respectively. Staff also recommends the adoption of a Prepaid License Plate account toll rate tier, which adds 10

percent to applicable transponder toll rates on prepaid electronic tag accounts for vehicles that do not present a transponder when driving on CTRMA toll roads.

Backup Provided: Toll Rate Schedule

Stantec memo on Prepaid License Plate Billing rate tier

**GENERAL MEETING OF THE BOARD OF DIRECTORS
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**

RESOLUTION NO. 23-0XX

**AMENDING THE MOBILITY AUTHORITY POLICY CODE § 301.002(c) TO MODIFY
THE MINIMUM RATES FOR THE MOPAC EXPRESS LANES AND ADDING §
301.0075 TO THE MOBILITY POLICY CODE REGARDING PREPAID LICENSE
PLATE BILLING**

WHEREAS, by Resolution No. 12-016 dated February 29, 2012, the Central Texas Regional Mobility Authority (“Mobility Authority”) Board of Directors (“Board”) adopted the Mobility Authority Policy Code (“Policy Code”); and

WHEREAS, subsequent to its initial adoption, the Board has amended the Policy Code from time to time in order to modify existing policies and incorporate new policies beneficial to the operation of the Mobility Authority; and

WHEREAS, the Executive Director recommends amending Mobility Authority Policy Code § 301.002(c), a copy of which is attached hereto as Exhibit A, to modify the minimum toll rates for the Mopac Express Lanes to adjust annually by \$0.07 per segment for calendar 2024, \$0.08 per segment for calendar 2025, and \$0.08 for calendar 2026 until the minimum toll rate is \$0.73 to coincide with the expected minimum toll rate for the 183 North managed lanes at the time it opens for tolling; and

WHEREAS, the Executive Director also recommends amending the Mobility Authority Policy Code by adding a new § 301.0075, a copy of which is attached hereto as Exhibit B, to collect payment from prepaid accounts for vehicles without transponders utilizing prepaid license plate account billing as a payment option for customers.

NOW THEREFORE, BE IT RESOLVED, that the Board hereby accepts and approves the amendments to Mobility Authority Policy Code § 301.002(c), regarding the modification of the minimum toll rates for the Mopac Express Lanes and the addition of new Mobility Authority Policy Code § 301.0075 regarding Prepaid License Plate Billing, which are attached hereto as Exhibit A and Exhibit B, respectively

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

Robert W. Jenkins, Jr.
Chairman, Board of Directors

Exhibit A

MOBILITY AUTHORITY POLICY CODE

Chapter 3: OPERATIONS

Article 9. TOLL POLICIES

Subchapter A. TOLL RATES

301.001 Priority of Bond Documents

Notwithstanding any conflicting provision in this subchapter or in a prior resolution adopting the Toll Policies, the toll rates and schedules promulgated by the authority shall always be sufficient to meet or exceed all covenants and requirements set forth in all applicable bond documents and obligations of the authority. If any conflict arises between the bond documents and this subchapter or a prior resolution adopting the Toll Policies, the covenants and requirements of the bond documents shall control to the extent of such conflict.

301.002 Toll Rates

(a) The authority shall establish toll rates for each tolled facility operated by the authority. Each toll established by this section is subject to an adjustment on January 1 of each year under the procedure set forth in Section 301.003 (Annual Toll Rate Escalation). The executive director is authorized and directed to edit a toll established by this section to update and certify any change to a toll made pursuant to Section 301.003.

(b) The toll charge for each tolled facility operated by the authority shall be published on the authority website.

(c) The toll charged for use of the MoPac Express Lanes shall be comprised of both a minimum toll, as well as a variable component that is activated during higher traffic volumes.~~in nature. The minimum toll rate will be \$0.25 per Express Lane segment, in 2016 dollars.~~ The minimum toll rate per segment will be adjusted annually by \$0.075 per segment for calendar 2024, \$0.08 per segment for calendar 2025, and \$0.08 for calendar 2026 until the minimum toll rate is \$0.7350, which will coincide with the expected minimum toll rate for the 183N managed lanes at the time it opens for tolling. Once the MoPac Express Lanes at which point the minimum toll rate reaches \$0.73 per segment it will be adjusted annually in accordance with the methodology for toll rate escalation provided in Section 301.003. There shall be no maximum toll rate. To maximize throughput and maintain free flowing conditions, the toll rate for each MoPac Express Lane segment shall change on a real-time basis based on traffic volumes. When traffic volumes increase, the minimum toll rate shall be increased as much as necessary to prevent the MoPac Express Lane(s) from becoming congested. When traffic volumes decrease, the toll rate shall be reduced to encourage use of the MoPac Express Lane(s). The primary goal of the variable toll rate is to minimize congestion on the MoPac Express Lanes and to encourage more people to ride public transit or join a registered vanpool. Changeable message signs shall be located prior to the entrance of each MoPac Express

MOBILITY AUTHORITY POLICY CODE

Lane segment to notify customers of the current toll rate. A customer shall never pay more than the toll rate information shown on the sign located near the vehicle's entry point, but may be charged less. The Mobility Authority may reduce tolls if it determines that operational issues warrant such an adjustment.

Exhibit B

MOBILITY AUTHORITY POLICY CODE

301.0075 Prepaid License Plate Account Billing

A The authority offers prepaid license plate account billing as a payment option for customers that use its toll facilities with an interoperable transponder account; however, do not present or display a transponder on the vehicle driven through toll road gantries. Instead of a transponder, the vehicle is identified through an image of its license plate and matched to the corresponding interoperable transponder account. Each transponder issuer that is interoperable with the authority's toll facilities has its own user agreement concerning requirements to open and maintain a transponder account. The authority will maintain a list of transponder programs that are interoperable with the authority's website. dd-text here....

301.008 Video Billing

(a) The authority offers video billing as a payment option for customers that use its toll facilities without a transponder account. The authority, through a third-party vendor (the "Contractor"), will use the license plate information of a vehicle that does not have a valid toll transponder but travels on the authority's toll facilities to determine the registered owner of such a vehicle via an interface with Vehicle Title & Registration database or similar institution.

(b) The Contractor will send an invoice to the registered owner of the vehicle and accept payment on behalf of the authority. The Contractor will add a processing fee for each invoice. Payment of each invoice is required by the stated due date.

301.009 Establishment of Administrative Fee for Unpaid Tolls

(a) Section 370.177, Transportation Code, authorizes the assessment and collection of an administrative fee to recover the authority's cost of collecting unpaid tolls. An administrative fee may not exceed \$100.00 per unpaid toll. The authority has determined that such fees may vary depending on how far in the collection process a delinquent account proceeds.

(b) An administrative fee shall be applied at each phase of non-payment in addition to the unpaid toll. An additional administrative fee shall be imposed upon the filing of a criminal complaint for non-payment or upon the determination of habitual violator status.

(c) The administrative fee for each billing phase and enforcement level shall be approved by the authority and published on the authority's website.

(d) The board recognizes that the amount of the administrative fee should be subject to periodic change when collection costs and associated matters are considered. Therefore, the board delegates the authority to revise the administrative fee, or any aspect thereof, to the executive director, in consultation with the director of operations, and the executive director may revise an administrative

MOBILITY AUTHORITY POLICY CODE

fee by written amendment. The executive director shall give notice to the board of any such revision at the next regularly scheduled board meeting after the revision is put into effect.



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #7

Discuss and consider modifying the annual system toll rate escalation becoming effective on January 1, 2024 and possible action if necessary

Strategic Plan Relevance: Stewardship
 Department: Finance
 Contact: José Hernández, Chief Financial Officer
 Associated Costs: N/A
 Funding Source: N/A
 Action Requested: Consider and act on draft resolution

Background - Section 301.002(a) of the Policy Code states that “the authority shall establish toll rates for each tolled facility operated by the authority. Each toll established by this section is subject to an adjustment on January 1 of each year under the procedure set forth in Section 301.003 (Annual Toll Rate Escalation). The executive director is authorized and directed to edit a toll established by this section to update and certify any change to a toll made pursuant to Section 301.003.”

Non-variable toll rates - Section 301.003 of the Policy Code provides that, each October, Mobility Authority staff must calculate a percentage increase in toll rates charged on non-variable rate Mobility Authority toll facilities using the formula established by that section. The formula is based on changes to the most recently published non-revised index of Consumer Prices for All Urban Consumers (CPI-U) before seasonal adjustment, as published by the Bureau of Labor Statistics of the U.S. Department of Labor. Each year, this Toll Rate Escalation Percentage is reported to the Board.

Previous Actions - The non-variable toll rates for the CTRMA Turnpike System have increased annually. The increases for each of the last six years are shown below.

Year	2018	2019	2020	2021	2022	2023
CPI-U	2.23%	2.27%	1.71%	5.39%	8.2%	3.7%
Increase/gantry	\$0.01- \$0.03	\$0.01- \$0.03	\$0.01- \$0.03	\$0.02- \$0.09	\$0.04- \$0.14	\$0.02- \$0.05

2023 Increase for non-variable toll rates - The Toll Rate Escalation Percentage calculated based on the September 2023 CPI-U is 3.7%. This percentage increase in toll rates will automatically become effective on January 1, 2024, unless the Board affirmatively votes to modify the percentage. If the percentage is not modified from CPI-U, this increase will result in an additional \$0.02 to \$0.05 toll charged at each gantry for a customer in a two-axle vehicle who uses a TxTAG or other transponder account.

Staff Recommendation - Staff recommends adopting the CPI-U rate for all system gantries..

Backup Provided: Traffic Consultant Certification
2023 CPI-U Toll Rate Calculation
Toll Rate Schedule



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #8

Discuss and consider adopting the
five-year capital improvement plan

Strategic Plan Relevance:	Stewardship
Department:	Finance
Contact:	José Hernández, Chief Financial Officer
Associated Costs:	N/A
Funding Source:	N/A
Action Requested:	Consider and act on draft resolution

Project Description/Background: The purpose of the capital plan is to serve as a tool to inform the Board and staff on decision making for investments in the CTRMA System roadways, facilities, and the MoPac managed lanes. The capital plan is designed to provide the Board and staff a view of future potential projects needs and enhancements, as well as prospective associated funding requirements. The plan and process will allow the Board and staff to prioritize project selection and prepare for them in current and future work plans and funding cycles should the decision be made to pursue them.

Previous Actions & Brief History of the Program/Project: An outcome goal of the Board of Directors 2022 Strategic Plan was the development of a five-year capital plan. The plan will provide insight on current and future needs to maintain the system and MoPac at a desired level of service and contemplate system enhancements and expansion, as well as potential participation in other non-tolled projects in the local community. The document is a planning toll for the Board and staff and does not commit the Board to approve nor fund any projects beyond the first year of the plan. Projects in years two to five of the plan are subject to change, deferral, reprioritization, and deletion on an annual basis. This is the initial production of the five-year capital plan. The capital planning process will be an annual practice concurrent with the annual operating budget preparation cycle.

Financing: N/A

Action requested/Staff Recommendation: Staff recommends adoption of the five-year capital plan.

Backup provided: Draft Resolution
Draft Five Year Capital Plan

**GENERAL MEETING OF THE BOARD OF DIRECTORS
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**

RESOLUTION NO. 23-0XX

ADOPT THE FIVE-YEAR CAPITAL PLAN

WHEREAS, pursuant to Texas Transportation Code Section 370.261 and CTRMA Policy Code Section 101.013(a), each even numbered year the Central Texas Regional Mobility Authority is required to prepare a Strategic Plan covering its next five fiscal years; and

WHEREAS, by Resolution No. 22-042, dated September 28, 2022, the Board adopted the 2022 Mobility Authority Strategic Plan; and

WHEREAS, one of the goals outlined in the 2022 Mobility Authority Strategic Plan is to develop a system-wide capital improvement plan to provide a view of upcoming system needs, potential future projects and system enhancements, and their associated funding requirements; and

WHEREAS, Mobility Authority staff presented a draft Five Year Capital Plan for the Board's review and comment at the Board Workshop held on September 20, 2023; and

WHEREAS, the Executive Director has incorporated the Board Member's comments into the proposed Five-Year Capital Plan, a copy of which is attached hereto as Exhibit A.

NOW THEREFORE, BE IT RESOLVED that the Board hereby approves and adopts the proposed Five-Year Capital Plan in the form attached hereto as Exhibit A.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

Robert W. Jenkins, Jr.
Chairman, Board of Directors

Exhibit A

Five Year Capital Plan

FIVE-YEAR CAPITAL PLAN



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY



OCTOBER
2023

Table of Contents

CENTRAL TEXAS ROADWAY SYSTEM MAP	2
INTRODUCTION.....	3
THE CTRMA STRATEGIC PLAN	4
OVERVIEW OF CAPITAL PLANNING PROCESS	5
DESCRIPTION OF CATEGORIES.....	5
FUNDING SOURCES	6
CAPITAL BY DEPARTMENT	7
ADMINISTRATION	12
OPERATIONS	17
INFORMATION TECHNOLOGY	29
ENGINEERING.....	46

CENTRAL TEXAS ROADWAY SYSTEM MAP



INTRODUCTION

The Central Texas Regional Mobility Authority (CTRMA or Mobility Authority) was established by Travis and Williamson Counties in 2002 as the state's first regional mobility authority. The agency operates under Chapter 370, Regional Mobility Authorities, of the Texas Transportation Code, representing the Texas Legislature's vision to allow local communities greater flexibility in meeting their transportation needs. Our mission is to develop, deliver, operate, and maintain safe, high-quality roadways and related transportation solutions.

The Central Texas Regional Mobility Authority Five-Year Capital Plan (CTRMA Capital Plan) is developed to plan for the maintenance, renewal, improvement and/or replacement of capital assets. The CTRMA System (System) facilities are the 183A Turnpike Project (Phases I, II and III); the 290E Project (Phases I, II and III); the 183 South Project; the SH 71 Express Project, the 183 North Mobility Project and the SH 45 Southwest Project. The 183A Turnpike Project (Phases I and II), the 290E Project (Phases I, II and III), the 183 South Project, the SH 71 Express Project and the SH 45 Southwest Project are all currently in operation. Both the 183A Phase III Project and the 183 North Mobility Project are under construction. The CTRMA operates and maintains the MoPac Express Lanes (MoPac) currently in operation. However, MoPac is not part of the System.

The CTRMA Capital Plan includes current year estimated expenditures approved through the annual budget process and estimates for the four subsequent years to be used as a tool for planning purposes only. The subsequent years are re-evaluated, updated and/or extended as part of the annual budget process, subject to the prevailing priorities of the Board and fiscal constraints. As a multi-year planning tool, the CTRMA Capital Plan is comprised of projects continued from previous years, projects being initiated in the current year, and those with the potential to be pursued within the next five years.

The CTRMA Capital Plan is adopted annually by the CTRMA Board of Directors as a planning tool to provide a perspective on prospective capital requirements going forward. Only the projects identified in the first year of the capital plan have been formally approved and funded by the Board action through the annual budget process. The projects in the subsequent four years of the CTRMA Capital Plan and projected expenditures are subject to future deliberation by the Board and do not constitute a commitment by the Mobility Authority to approve or fund such projects.

THE CTRMA STRATEGIC PLAN

The CTRMA Strategic Plan (see graphic below) serves as the guiding document in the operation of the CTRMA, providing a roadmap to help assure alignment with our mission to “implement innovative, multi-modal transportation solutions that reduce congestion and create transportation choices that enhance quality of life and economic vitality.”



OVERVIEW OF CAPITAL PLANNING PROCESS

As represented on the prior page, the Board's strategic values and goals are the guidance for decision making, for both operational and capital needs, to allocate limited resources to accomplish the Authority's objectives. In conjunction with the annual budgeting process, capital planning starts with an internal prioritization of needs by the departments, ranking requests in three categories:

1. Absolutely essential to maintain the integrity of the enterprise,
2. Enhancements that would facilitate operations, processes, and/or driver satisfaction, and
3. Improvements that would yield future benefits if affordable (not a critical need now).

Capital requests are then presented and discussed during annual budget deliberations between the department directors, administration, and finance department. Funding parameters are established, and recommendations formulated within those constraints and in conjunction with the workplans of the departments. Funding for the projects recommended in the first year of the capital plan is allocated in the proposed budget that is presented to the Board for their consideration. The first year recommended projects of the five-year capital plan constitute the capital budget for the upcoming fiscal year.

The five-year capital plan is considered for adoption by the Board typically at the same time as the operating budget. The capital planning process commences in the spring of each year, usually March, when project additions, deletions, reprioritization, and deferral decisions and recommendations are again deliberated upon to start the cycle.

DESCRIPTION OF CATEGORIES

Capital Additions – new projects or equipment not currently a component of the System or MoPac

Renewal and Replacement – projects that will refurbish or replace existing System or MoPac capital components

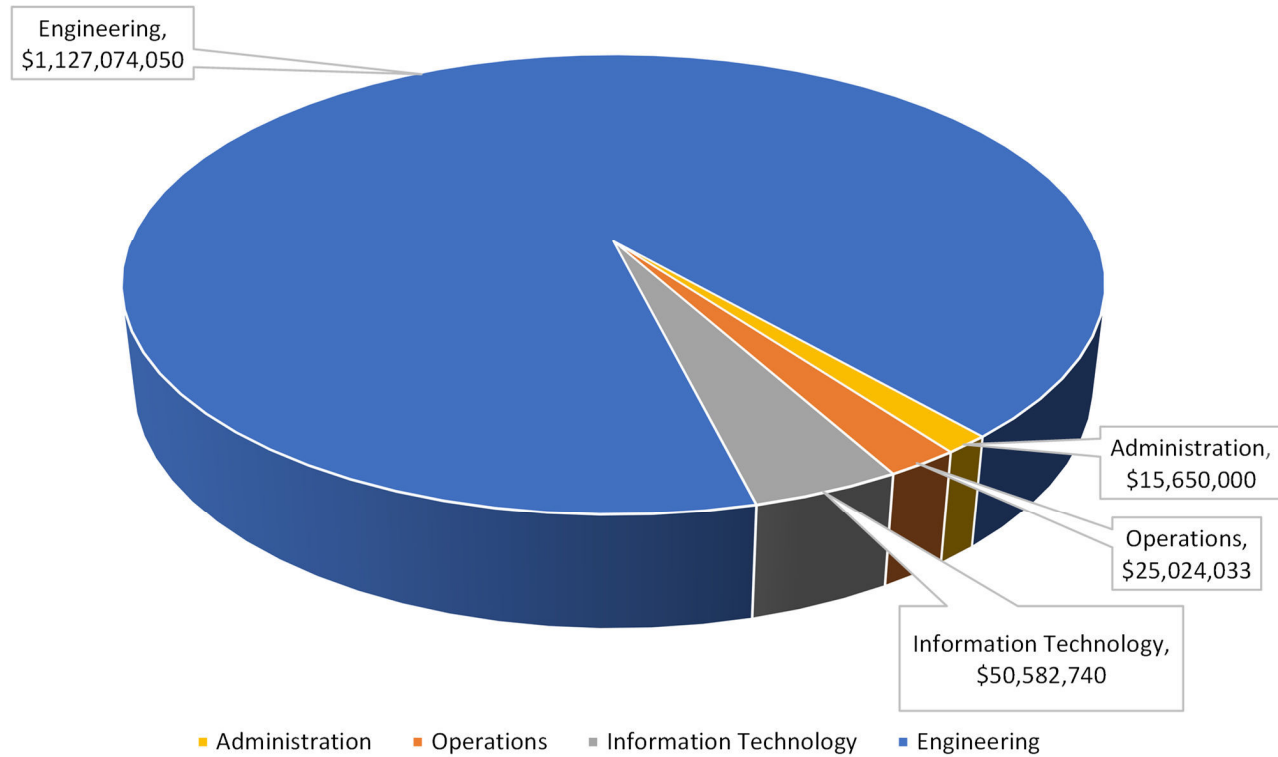
Capital Improvement Projects – major new construction of roadways

FUNDING SOURCES

The primary funding source for projects in the annual capital budget are net revenues remaining after the payment of operating and maintenance expenses, debt service payments, and any reserves required for payment of debt service. Net revenues are deposited monthly into the Authority's General Fund and capital projects are then expensed from the General Fund or the Renewal and Replacement Fund, depending on their classification.

For capital improvement projects, which are typically the major roadway construction projects, funding is typically provided through capital markets financing in the form of long-term municipal bonds and short-term notes. Once the project is complete and the short-term note proceeds have been expended, upon maturity of the notes, long-term financing for some roadways is provided through U.S. Department of Transportation (USDOT) loans via the Transportation Infrastructure Finance and Innovation Act (TIFIA) loan program. Projects in this category may also be financed by the Authority's General Fund.

FIVE-YEAR CAPITAL FORECAST BY DEPARTMENT



**Five-Year Capital Plan
Priority Rank #1**

Administration Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Purchase Property for CTRMA Office	\$ 15,000,000.00	\$ 15,000,000.00	\$ -	\$ -	\$ -	\$ -
Enterprise Resource Planning System	\$ 650,000.00	\$ 650,000.00	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 15,650,000.00	\$ 15,650,000.00	\$ -	\$ -	\$ -	\$ -

Operations Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Pay-By-Mail Implementation	\$ 2,000,000.00	\$ -	\$ 1,200,000.00	\$ 800,000.00	\$ -	\$ -
Pay-By-Mail Procurement	\$ 1,000,000.00	\$ 300,000.00	\$ 700,000.00	\$ -	\$ -	\$ -
Safety Technology - Automated Incident Detection Cameras	\$ 4,776,866.49	\$ 4,776,900.00	\$ -	\$ -	\$ -	\$ -
Toll Violation Mitigation - Automated License Plate Reader (ALPR) Technology	\$ 3,238,188.24	\$ 3,238,200.00	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 11,015,054.73	\$ 8,315,100.00	\$ 1,900,000.00	\$ 800,000.00	\$ -	\$ -

Information Technology Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Toll System Replacement	\$ 46,072,032.76	\$ 27,533,200.00	\$ 7,104,975.15	\$ 1,433,857.61	\$ -	\$ 10,000,000.00
Kapsch Central Host Upgrades	\$ 1,000,000.00	\$ 1,000,000.00	\$ -	\$ -	\$ -	\$ -
DPS Enh-Release 5	\$ 1,154,000.00	\$ 1,154,000.00	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 48,226,032.76	\$ 29,687,200.00	\$ 7,104,975.15	\$ 1,433,857.61	\$ -	\$ 10,000,000.00

Engineering Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
183A Added Capacity (Design)	\$ 27,000,000.00	\$ 8,714,000.00	\$ 8,714,000.00	\$ 8,714,000.00	\$ 858,000.00	\$ -
183A Phase II Small Sign Replacement	\$ 1,518,000.00	\$ 637,184.57	\$ -	\$ -	\$ -	\$ -
290E Maintenance Yard Expansion	\$ 85,000.00	\$ 85,000.00	\$ -	\$ -	\$ -	\$ -
290E Maintenance Yard Pond Expansion	\$ 35,000.00	\$ 35,000.00	\$ -	\$ -	\$ -	\$ -
290E PH IV (Design - Full Build - Schematic/Environmental)	\$ 50,000,000.00	\$ -	\$ 16,600,000.00	\$ 16,600,000.00	\$ 16,800,000.00	\$ -
Barton Skyway Development + Construction	\$ 10,107,058.93	\$ 5,300,000.00	\$ -	\$ -	\$ -	\$ -
CTB Delineator - 100' Spacing, 290@183, 290@130, 183@71, 71@130, 45SW@MoPac	\$ 62,700.00	\$ 62,700.00	\$ -	\$ -	\$ -	\$ -
CTB Delineator - 100' Spacing, 45SW	\$ 15,200.00	\$ 15,200.00	\$ -	\$ -	\$ -	\$ -
CTB Delineator - 100' Spacing, MoPac EL, North of FM 2222	\$ 37,150.00	\$ 37,150.00	\$ -	\$ -	\$ -	\$ -
CTB Delineator - 100' Spacing, MoPac EL, South of FM 2222	\$ 32,350.00	\$ 32,350.00	\$ -	\$ -	\$ -	\$ -
Maintenance Yard Improvement Support + Add'tl Site Investigations	\$ 800,000.00	\$ 800,000.00	\$ -	\$ -	\$ -	\$ -
MBGF Improvements - Project #2	\$ 3,000,000.00	\$ 3,000,000.00	\$ -	\$ -	\$ -	\$ -
MoPac PFC - Flexible Pavement w/Delineator Replacement	\$ 11,390,000.00	\$ -	\$ -	\$ 11,390,000.00	\$ -	\$ -
MoPac PFC Fog Seal and Surface Repair	\$ 1,800,000.00	\$ 1,800,000.00	\$ -	\$ -	\$ -	\$ -
Snow Equipment	\$ 35,000.00	\$ 35,000.00	\$ -	\$ -	\$ -	\$ -
Wall Monitoring - System Wide	\$ 300,000.00	\$ 300,000.00	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 106,217,458.93	\$ 20,853,584.57	\$ 25,314,000.00	\$ 36,704,000.00	\$ 17,658,000.00	\$ -

	Sum of Total Project Cost	2024	2025	2026	2027	2028
Total All Departments - Rank #1	\$ 181,108,546.42	\$ 74,505,884.57	\$ 34,318,975.15	\$ 38,937,857.61	\$ 17,658,000.00	\$ 10,000,000.00

Five-Year Capital Plan Priority Rank #2

Administration Department

Row Labels	Sum of Total Project Cost	2024	2025	2026	2027	2028
Grand Total						

Operations Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Roadway Traveler Communications - 183A Phase I & II Dynamic Message Signs	\$ 1,871,087.10	\$ -	\$ 1,871,087.10	\$ -	\$ -	\$ -
Roadway Traveler Communications - MoPac Single Line DMS (6 Locations)	\$ 1,660,777.65	\$ -	\$ 1,660,777.65	\$ -	\$ -	\$ -
Safety Technology - Lane Violation Detection	\$ 1,588,124.06	\$ -	\$ 1,588,124.06	\$ -	\$ -	\$ -
TIM Center Expansion and Technology	\$ 6,760,000.00	\$ 6,760,000.00	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 11,879,988.81	\$ 6,760,000.00	\$ 5,119,988.81	\$ -	\$ -	\$ -

Information Technology Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Kapsch Mopac Upgrades	\$ 300,000.00	\$ -	\$ 300,000.00	\$ -	\$ -	\$ -
Grand Total	\$ 300,000.00	\$ -	\$ 300,000.00	\$ -	\$ -	\$ -

Engineering Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
183A Added Capacity (Construction)	\$ 142,000,000.00	\$ -	\$ -	\$ -	\$ 47,249,800.00	\$ 62,999,733.33
290E Added Capacity	\$ 94,000,000.00	\$ -	\$ -	\$ 8,367,450.00	\$ 8,367,450.00	\$ 25,811,500.00
290E Large & Small Sign Replacement	\$ 3,850,000.00	\$ -	\$ 3,850,000.00	\$ -	\$ -	\$ -
Maintenance Vehicle (1)	\$ 65,000.00	\$ -	\$ 65,000.00	\$ -	\$ -	\$ -
Maintenance Yard Site Acquisition (ROW Purchase)	\$ 4,400,000.00	\$ -	\$ 4,400,000.00	\$ -	\$ -	\$ -
Slab Stabilization for 183N	\$ 300,000.00	\$ -	\$ -	\$ 150,000.00	\$ 150,000.00	\$ -
Slab Stabilization for 183S	\$ 102,532.00	\$ -	\$ 102,532.00	\$ -	\$ -	\$ -
Slab Stabilization for 290E	\$ 1,000,000.00	\$ -	\$ 500,000.00	\$ 250,000.00	\$ 250,000.00	\$ -
MoPac South (D/B Construction)	\$ 1,000,000,000.00	\$ -	\$ -	\$ 195,200,000.00	\$ 195,200,000.00	\$ 195,200,000.00
290E PH IV (Construction - Full Build)	\$ 1,500,000,000.00	\$ -	\$ -	\$ -	\$ -	\$ 250,000,000.00
Grand Total	\$ 2,745,717,532.00	\$ -	\$ 8,917,532.00	\$ 203,967,450.00	\$ 251,217,250.00	\$ 534,011,233.33

Row Labels	Sum of Total Project Cost	2024	2025	2026	2027	2028
Total All Departments - Rank #2	\$ 2,757,897,520.81	\$ 6,760,000.00	\$ 14,337,520.81	\$ 203,967,450.00	\$ 251,217,250.00	\$ 534,011,233.33

Five-Year Capital Plan Priority Rank #3

Administration Department

Row Labels	Sum of Total Project Cost	2024	2025	2026	2027	2028
Grand Total						

Operations Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Safety Technology - Wrong Way Driving MIP (6 Locations)	\$ 2,128,944.52	\$ -	\$ 2,128,944.52	\$ -	\$ -	\$ -
Grand Total	\$ 2,128,944.52	\$ -	\$ 2,128,944.52	\$ -	\$ -	\$ -

Information Technology Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Roadway Traveler Communications - roadside units 183N	\$ 439,843.55	\$ -	\$ -	\$ 439,843.55	\$ -	\$ -
Roadway Traveler Communications - roadside units 183S	\$ 733,444.18	\$ -	\$ 733,444.18	\$ -	\$ -	\$ -
Roadway Traveler Communications - roadside units 290E	\$ 627,732.01	\$ -	\$ 627,732.01	\$ -	\$ -	\$ -
Roadway Traveler Communications - roadside units 71E	\$ 20,049.90	\$ -	\$ 20,049.90	\$ -	\$ -	\$ -
Roadway Traveler Communications - Roadside Units MIP	\$ 235,638.00	\$ -	\$ 235,638.00	\$ -	\$ -	\$ -
Grand Total	\$ 2,056,707.64	\$ -	\$ 1,616,864.09	\$ 439,843.55	\$ -	\$ -

Engineering Department

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Bliss Spillar Drainage	\$ 840,000.00	\$ -	\$ 840,000.00	\$ -	\$ -	\$ -
Escarpment Turnaround	\$ 1,120,000.00	\$ -	\$ 1,120,000.00	\$ -	\$ -	\$ -
SB Windsor Exit Ramp	\$ 440,000.00	\$ -	\$ -	\$ -	\$ 440,000.00	\$ -
SH 71 TOM- Flexible Pavement	\$ 2,900,000.00	\$ -	\$ -	\$ 2,900,000.00	\$ -	\$ -
System-wide ITS SUE Investigations	\$ 2,760,000.00	\$ -	\$ 2,760,000.00	\$ -	\$ -	\$ -
Truss Bridge Aesthetics & Lighting (Montopolis Bridge)	\$ 7,166,000.00	\$ -	\$ -	\$ -	\$ -	\$ 7,166,000.00
Trails - SUP/Sidewalk	\$ 4,000,000.00	\$ -	\$ 1,000,000.00	\$ 1,000,000.00	\$ 1,000,000.00	\$ 1,000,000.00
Grand Total	\$ 19,226,000.00	\$ -	\$ 5,720,000.00	\$ 3,900,000.00	\$ 1,440,000.00	\$ 8,166,000.00

Row Labels	Sum of Total Project Cost	2024	2025	2026	2027	2028
Total All Departments - Rank #3	\$ 23,411,652.16	\$ -	\$ 9,465,808.61	\$ 4,339,843.55	\$ 1,440,000.00	\$ 8,166,000.00



ADMINISTRATION

ADMINISTRATION

The primary role of the Administration Department is to manage the agency, its departments, programs, and projects in alignment with the Strategic Plan. The Agency's mobility innovation efforts and general support for the Board of Directors is also included in this Department.

With the complexity of the Mobility Authority's roadway toll and technology systems, it is imperative that the toll and roadway systems have the capacity to effectively support both our existing and future facilities. Significant effort will be focused on the modernization of the toll and roadway technology systems and to deploy innovative mobility technologies. This is all part of an ongoing effort to maximize the safety and efficiency of our roadways using technology, to find new ways to communicate with our customers and key stakeholders, and to provide timely and relevant information needed for customers to make effective travel decisions.

Strategic Goals

- Maintain and enhance our strategic partnerships to advance the common goals we share with our regional partner agencies
- Build, operate and maintain toll and non-toll roads that reduce congestion and connect our region in innovative and safe ways
- Make targeted investments in other transportation solutions that connect to our system and enhance quality of life

Five-Year Capital Plan Administration Department

Priority Rank #1

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Purchase Property for CTRMA Office	\$ 15,000,000.00	\$ 15,000,000.00	\$ -	\$ -	\$ -	\$ -
Enterprise Resource Planning System	\$ 650,000.00	\$ 650,000.00	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 15,650,000.00	\$ 15,650,000.00	\$ -	\$ -	\$ -	\$ -

Priority Rank #2

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Grand Total						

Priority Rank #3

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Grand Total						

	Sum of Total Project Cost	2024	2025	2026	2027	2028
ADM Total All Ranks	\$ 15,650,000.00	\$ 15,650,000.00	\$ -	\$ -	\$ -	\$ -

Project Detail

Project ID:	034	Budget Fiscal Year (FY):	2024
Project Title:	Purchase Property for CTRMA Office	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 15,000,000.00
Department:	Administration		

Description: Locate and purchase site for CTRMA corporate offices with existing building or build to suit

Strategic Plan Alignment: Stewardship

Project Forecast		Forecast
Year (FY)		
2024	\$	15,000,000.00
2025	\$	-
2026	\$	-
2027	\$	-
2028	\$	-
	\$	15,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	086	Budget Fiscal Year (FY):	2024
Project Title:	Enterprise Resource Planning System	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 650,000.00
Department:	Administration		

Description: Finance to procure an Enterprise Resource Planning System

Strategic Plan Alignment: Innovation

Project Forecast Year (FY)	Forecast
2024	\$ 650,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 650,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No



OPERATIONS

OPERATIONS

The Operations Department supports the Mobility Authority's regional mobility, economic vitality, sustainability, and innovation strategic goals. The Operations Department is responsible for all aspects of revenue collection, customer service and traffic & incident management. The Operations Department serves its internal and external customers through the provision of the following core services:

- Customer Care. Ensure a quality experience for the Mobility Authority's customers. Solve complex customer service issues. Implement efficient solutions that promote self-service and increase efficiency.
- Toll Collection. Oversee the daily operation of collecting toll revenue. Monitor transaction reconciliation revenue metrics. Identify and implement opportunities for collecting revenue earlier and more often.
- Traffic & Incident Management. Coordinate the resources of partner agencies and private sector companies to detect, respond to, and clear traffic incidents as well as debris removal as quickly as possible to reduce the impacts of incidents on safety and congestion.
- Traveler Communication. Alert approaching vehicles to problem areas by updating social media and on road messaging tools to better inform drivers. Provide information regarding alternate routes for vehicles, alleviating the effects of bottlenecks or incidents.
- Violation Enforcement. Oversee the Mobility Authority's violation enforcement program to mitigate revenue leakage and protect our stakeholder's investment.

The predominant themes of the Operations Department's FY 2024 budget are to increase revenue through improved pre-paid account penetration and collections in the first 60 days of the Pay by Mail lifecycle; mitigate leakage; and improve our customer service experience. Activities this fiscal year will center around implementing new customer service features; deploying messages outlining the benefits of pre-paid account payment mechanisms; enforcing toll evasion remedies; communicating up to date and accurate travel information to stakeholders through various channels; evaluating options for our Pay by Mail program; and supporting regional and national interoperability efforts.

Strategic Goals

- Make targeted investments in other transportation solutions that connect to our system and enhance quality of life
- Implement financial strategy and policies that prioritize long-term system health and growth, a decreased reliance on debt, and good financial stewardship
- Maintain and enhance our strategic partnerships to advance the common goals we share with our regional partner agencies

Five-Year Capital Plan Operations Department

Priority Rank #1							
Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028	
Pay-By-Mail Implementation	\$ 2,000,000.00	\$ -	\$ 1,200,000.00	\$ 800,000.00	\$ -	\$ -	\$ -
Pay-By-Mail Procurement	\$ 1,000,000.00	\$ 300,000.00	\$ 700,000.00	\$ -	\$ -	\$ -	\$ -
Safety Technology - Automated Incident Detection Cameras	\$ 4,776,866.49	\$ 4,776,900.00	\$ -	\$ -	\$ -	\$ -	\$ -
Toll Violation Mitigation - Automated License Plate Reader (ALPR) Technology	\$ 3,238,188.24	\$ 3,238,200.00	\$ -	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 11,015,054.73	\$ 8,315,100.00	\$ 1,900,000.00	\$ 800,000.00	\$ -	\$ -	\$ -

Priority Rank #2							
Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028	
Roadway Traveler Communications - 183A Phase I & II Dynamic Message Signs	\$ 1,871,087.10	\$ -	\$ 1,871,087.10	\$ -	\$ -	\$ -	\$ -
Roadway Traveler Communications - MoPac Single Line DMS (6 Locations)	\$ 1,660,777.65	\$ -	\$ 1,660,777.65	\$ -	\$ -	\$ -	\$ -
Safety Technology - Lane Violation Detection	\$ 1,588,124.06	\$ -	\$ 1,588,124.06	\$ -	\$ -	\$ -	\$ -
TIM Center Expansion and Technology	\$ 6,760,000.00	\$ 6,760,000.00	\$ -	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 11,879,988.81	\$ 6,760,000.00	\$ 5,119,988.81	\$ -	\$ -	\$ -	\$ -

Priority Rank #3							
Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028	
Safety Technology - Wrong Way Driving MIP (6 Locations)	\$ 2,128,944.52	\$ -	\$ 2,128,944.52	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 2,128,944.52	\$ -	\$ 2,128,944.52	\$ -	\$ -	\$ -	\$ -

	Sum of Total Project Cost	2024	2025	2026	2027	2028	
OPS Total All Ranks	\$ 25,023,988.06	\$ 15,075,100.00	\$ 9,148,933.33	\$ 800,000.00	\$ -	\$ -	\$ -

Project Detail

Project ID:	033	Budget Fiscal Year (FY):	2025
Project Title:	Roadway Traveler Communications - 183A Phase I & II Dynamic Message Signs	Roadway Impacted:	183A
Fund:	General	Total Project Cost:	\$ 1,871,087.10
Department:	Operations		

Description: Installation of four (4) front-access, color, full-matrix dynamic message signs (DMS) along the 183A corridor to enable the Mobility Authority to disseminate real-time information related to traffic and roadway conditions (e.g., weather, queues, incidents, detours, work zones) to improve mobility and safety. The project will include new cantilevered structures, displays, cabinet assemblies, power services (120/240V), conduit, ground boxes, and ancillary infrastructure for a complete installation. Small-form verification cameras will be installed using wide-angle lenses providing operational staff the ability to remotely verify current messages in real-time.

Strategic Plan Alignment: Safety, Reliability, Innovation, Service

Project Forecast		Forecast
Year (FY)		
2024	\$	-
2025	\$	1,871,087.10
2026	\$	-
2027	\$	-
2028	\$	-
	\$	1,871,087.10

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	036	Budget Fiscal Year (FY):	2025
Project Title:	Safety Technology - Lane Violation Detection	Roadway Impacted:	MOPAC MNLN & 183N
Fund:	General	Total Project Cost:	\$ 1,588,124.06
Department:	Operations		

Description: Installation of fourteen (14) integrated systems to detect illegal “lane diving” maneuvers into and out of the express lanes along the MoPac Expressway and 183N corridors allowing the Mobility Authority to better identify, quantify, prohibit, and enforce these events. The integrated system will include multiple fixed CCTV cameras equipped with embedded video analytics, as well as an edge-compute processor and networking equipment to identify “lane diving” events and trigger the appropriate response (e.g., notify operational staff, collect license plate information). Installation of lane violation detection systems will leverage existing overhead gantries and sign bridges, while the project includes new cabinet assemblies, power services, conduit, ground boxes, and ancillary infrastructure necessary for a complete installation.

Strategic Plan Alignment: Safety, Stewardship, Innovation

Project Forecast		Forecast
Year (FY)		
2024	\$	-
2025	\$	1,588,124.06
2026	\$	-
2027	\$	-
2028	\$	-
	\$	1,588,124.06

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	037	Budget Fiscal Year (FY):	2024
Project Title:	Safety Technology - Automated Incident Detection Cameras	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 4,776,866.49
Department:	Operations		

Description: Installation of two-hundred forty-five (245) fixed camera in arrays along all of the Mobility Authority roadways (i.e., MoPac Expressway, 290E, 183A, 183S, SH71, 45SW) providing coverage and real-time video for the video analytics platform to identify, track, and monitor events more efficiently. Minimizing the time needed for the operational staff to identify and verify an event (e.g., crash, debris on roadway, stalled vehicle, wrong way vehicle, pedestrian on shoulder) will decrease the likelihood for secondary incidents. This project will include the physical infrastructure—including cameras, cabinet assemblies, device poles, power services, fiber optic communication drops, conduit, ground boxes, and ancillary hardware—as well as the software licenses necessary for a complete installation. Existing infrastructure— including structures, fiber optic communications, electrical power services, conduit duct bank, junction boxes, fiber optic backhaul communications, and cabinet assemblies—will

Strategic Plan Alignment: Safety, Stewardship, Innovation

Project Forecast		Forecast
Year (FY)		
2024	\$	4,776,900.00
2025	\$	-
2026	\$	-
2027	\$	-
2028	\$	-
	\$	4,776,900.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	038	Budget Fiscal Year (FY):	2024 -2025
Project Title:	Toll Violation Mitigation - Automated License Plate Reader (ALPR) Technology	Roadway Impacted:	71E, 45SW, 183S, 183A
Fund:	General	Total Project Cost:	\$ 3,238,188.24
Department:	Operations		

Description: Installation of one-hundred seven (107) Automated License Plate Reader (ALPR) sensors on existing mainline tolling gantries—one per lane and instrumented shoulders. The system will allow the Mobility Authority to identify toll violators using the new technology, as well as capture real-time data about corridor utilization, traffic volumes, and more. This project will require the installation of new cabinet assemblies, electrical power services, fiber optic communication drops, and underground infrastructure for a complete installation. To the greatest extent possible, the existing infrastructure—including conduit duct bank, junction boxes, fiber optic backhaul communications—will be re-utilized.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast		Forecast
Year (FY)		
2024	\$	3,238,200.00
2025	\$	-
2026	\$	-
2027	\$	-
2028	\$	-
	\$	3,238,200.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	044	Budget Fiscal Year (FY):	2025
Project Title:	Roadway Traveler Communications - MoPac Single Line DMS (6 Locations)	Roadway Impacted:	MOPAC MNLN
Fund:	General	Total Project Cost:	\$ 1,660,777.65
Department:	Operations		

Description: Installation of six (6) front-access, single-line dynamic message signs (DMS) along the MoPac Expressway corridor to enable the Mobility Authority to disseminate real-time information related to the status of the express lane (e.g., OPEN, CLOSED, CONGESTED, TOLLING ENFORCED). The project will include new electronic displays, cabinet assemblies, power services (120/240V), conduit, ground boxes, and ancillary infrastructure and leverage existing overhead structures, conduit duct bank, junction boxes, and fiber optic backhaul communications.

Strategic Plan Alignment: Safety, Reliability, Innovation

Project Forecast		Forecast
Year (FY)		
2024	\$	-
2025	\$	1,660,777.65
2026	\$	-
2027	\$	-
2028	\$	-
	\$	1,660,777.65

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	046	Budget Fiscal Year (FY):	2025
Project Title:	Safety Technology - Wrong Way Driving MIP (6 Locations)	Roadway Impacted:	MOPAC MNLN
Fund:	General	Total Project Cost:	\$ 2,128,944.52
Department:	Operations		

Description: Installation of six (6) wrong-way vehicle detection systems (WWVDS) within the off-ramp facilities of MoPac Expressway to detect, correct, and notify the Mobility Authority of vehicles entering the corridor improperly. The system will improve the overall safety of the corridor by immediately detecting wrong-way driving events and actuating a localized response to correct driver behavior before entering the corridor in the wrong direction at full speed. This project will include the physical infrastructure—including cameras, sensors, cabinet assemblies, device poles, power services, fiber optic communication drops, conduit, ground boxes, and ancillary hardware—as well as the software licenses necessary for a complete installation. Existing infrastructure—including fiber optic communications, electrical power services, conduit duct bank, junction boxes, fiber optic backhaul communications—will be re-utilized to the greatest extent possible.

Strategic Plan Alignment: Safety, Reliability, Innovation, Service

Project Forecast		Forecast
Year (FY)		
2024	\$	-
2025	\$	2,128,944.52
2026	\$	-
2027	\$	-
2028	\$	-
	\$	2,128,944.52

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	063	Budget Fiscal Year (FY):	2024-2025
Project Title:	Pay-By-Mail Procurement	Roadway Impacted:	SYSTEM
Fund:	Operating	Total Project Cost:	\$ 1,000,000.00
Department:	Operations		

Description: Procurement of a Pay-By-Mail processing services contract

Strategic Plan Alignment: Stewardship, Service

Project Forecast Year (FY)	Forecast
2024	\$ 300,000.00
2025	\$ 700,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/> \$ 1,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	064	Budget Fiscal Year (FY):	2024-2025
Project Title:	Pay-By-Mail Implementation	Roadway Impacted:	SYSTEM
Fund:	Operating	Total Project Cost:	\$ 2,000,000.00
Department:	Operations		

Description: Implementation of Pay-By-Mail processing services contract

Strategic Plan Alignment: Stewardship, Service

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 1,200,000.00
2026	\$ 800,000.00
2027	\$ -
2028	\$ -
	<hr/>
	\$ 2,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	084	Budget Fiscal Year (FY):	2024
Project Title:	TIM Center Expansion and Technology	Roadway Impacted:	SYSTEM
Fund:	Operating	Total Project Cost:	\$ 6,760,000.00
Department:	Operations		

Description: Major and minor renovation of the existing TIM Center building, as well as construction of a building addition to the existing structure. Additional technology is planned to include a video wall and software upgrades.

Strategic Plan Alignment: Safety, Reliability, Collaboration, Service

Project Forecast Year (FY)	Forecast
2024	\$ 6,760,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 6,760,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	Yes



FAVOR
Restaurants and more
delivered to your door
PART OF THE CEC FAMILY
Download
Power Today



INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY

The IT Department is responsible for maintaining the integrity of the agency's toll system, supporting revenue collection activities, and safeguarding the agency's internal and communication network. The IT Department also supports the agency's emerging technology efforts by lending technical expertise and implementing approved initiatives.

The core services provided by the Information Technology Department in support of its internal and external customers are outlined below:

- Information Technology (IT) Ensure the integrity of the Mobility Authority's computers, storage, network and other physical devices, infrastructure and processes used to create, process, store, secure and exchange all forms of electronic data.
- Intelligent Transportation Systems (ITS) Deploy various ITS technologies on Authority roads to detect, manage and report on roadway incidents. ITS technologies also assist in improving safety and the customer experience for our roadways through early detection and notification to public safety agencies.
- Toll Systems Oversee daily operation of the electronic toll collection systems operations. Monitor system performance and transaction reconciliation. Oversee system maintenance to ensure accuracy and dependability. Manage new toll collection system installation while maintaining current operational metrics.
- Transaction Processing. Manage the workflows associated with transaction processing, product management, discount management, billing management and product pricing. Ensure that transactions process in a predictable, consistent manner in compliance with the mobility authority's business rules and within compliance with national interoperability requirements. Monitor the data exchange operations support functions. Manage the Transaction Operations Management Solution (TOMS). Oversee reporting and analytics processes.

The IT Department will continue to set a solid foundation for the Mobility Authority's future. These efforts include continued development of the Data Platform System, the integration point for all transaction processing and data analytics; managing the replacement of the Authority's aging toll systems; upgrading the agency's communication infrastructure; and supporting regional and national interoperability efforts.

Strategic Goals

- Deliver on Commitments to our Customers and our Investors, Explore Efforts that Extend Beyond Roadways, Explore Transformative Technology and Adopt Industry Best Practices
- Employ a Collaborative Approach to Implementing Mobility Solutions, Deliver Responsible Mobility Solutions that Respect the Communities We Serve, Deliver on Commitments to our Customers and our Investors

Five-Year Capital Plan Information Technology Department

Priority Rank #1

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Toll System Replacement	\$ 46,072,032.76	\$ 27,533,200.00	\$ 7,104,975.15	\$ 1,433,857.61	\$ -	\$ 10,000,000.00
Kapsch Central Host Upgrades	\$ 1,000,000.00	\$ 1,000,000.00	\$ -	\$ -	\$ -	\$ -
DPS Enh-Release 5	\$ 1,154,000.00	\$ 1,154,000.00	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 48,226,032.76	\$ 29,687,200.00	\$ 7,104,975.15	\$ 1,433,857.61	\$ -	\$ 10,000,000.00

Priority Rank #2

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Kapsch Mopac Upgrades	\$ 300,000.00	\$ -	\$ 300,000.00	\$ -	\$ -	\$ -
Grand Total	\$ 300,000.00	\$ -	\$ 300,000.00	\$ -	\$ -	\$ -

Priority Rank #3

Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Roadway Traveler Communications - roadside units 183N	\$ 439,843.55	\$ -	\$ -	\$ 439,843.55	\$ -	\$ -
Roadway Traveler Communications - roadside units 183S	\$ 733,444.18	\$ -	\$ 733,444.18	\$ -	\$ -	\$ -
Roadway Traveler Communications - roadside units 290E	\$ 627,732.01	\$ -	\$ 627,732.01	\$ -	\$ -	\$ -
Roadway Traveler Communications - roadside units 71E	\$ 20,049.90	\$ -	\$ 20,049.90	\$ -	\$ -	\$ -
Roadway Traveler Communications - Roadside Units MIP	\$ 235,638.00	\$ -	\$ 235,638.00	\$ -	\$ -	\$ -
Grand Total	\$ 2,056,707.64	\$ -	\$ 1,616,864.09	\$ 439,843.55	\$ -	\$ -

	Sum of Total Project Cost	2024	2025	2026	2027	2028
IT Total All Ranks	\$ 50,582,740.40	\$ 29,687,200.00	\$ 9,021,839.24	\$ 1,873,701.16	\$ -	\$ 10,000,000.00

Project Detail

Project ID:	010	Budget Fiscal Year (FY):	2025
Project Title:	Roadway Traveler Communications - roadside units 290E	Roadway Impacted:	290E
Fund:	General	Total Project Cost:	\$ 627,732.01
Department:	IT		

Description: Installation of nine (9) roadside units (RSU) along the 290E corridor to enable Connected Vehicle (CV) applications for the Mobility Authority to communicate directly to in-vehicle systems and improve the overall safety and mobility of the corridor.

Strategic Plan Alignment: Innovation

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 627,732.01
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 627,732.01

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	013	Budget Fiscal Year (FY):	2025
Project Title:	Roadway Traveler Communications - roadside units 71E	Roadway Impacted:	71E
Fund:	General	Total Project Cost:	\$ 20,049.90
Department:	IT		

Description: Installation of one (1) roadside units (RSU) along the SH71 corridor to enable Connected Vehicle (CV) applications for the Mobility Authority to communicate directly to in-vehicle systems and improve the overall safety and mobility of the corridor.

Strategic Plan Alignment: Innovation

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 20,049.90
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 20,049.90

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	020	Budget Fiscal Year (FY):	2025
Project Title:	Roadway Traveler Communications - roadside units 183S	Roadway Impacted:	183S
Fund:	General	Total Project Cost:	\$ 733,444.18
Department:	IT		

Description: Installation of eleven (11) roadside units (RSU) along the 183S corridor to enable Connected Vehicle (CV) applications for the Mobility Authority to communicate directly to in-vehicle systems and improve the overall safety and mobility of the corridor.

Strategic Plan Alignment: Innovation

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 733,444.18
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 733,444.18

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	022	Budget Fiscal Year (FY):	2026
Project Title:	Roadway Traveler Communications - roadside units 183N	Roadway Impacted:	183N
Fund:	General	Total Project Cost:	\$ 439,843.55
Department:	IT		

Description: Installation of ten (10) roadside units (RSU) along the 183N corridor to enable Connected Vehicle (CV) applications for the Mobility Authority to communicate directly to in-vehicle systems and improve the overall safety and mobility of the corridor.

Strategic Plan Alignment: Innovation

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ 439,843.55
2027	\$ -
2028	\$ -
	\$ 439,843.55

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	032	Budget Fiscal Year (FY):	2025-26
Project Title:	Toll System Replacement	Roadway Impacted:	183A
Fund:	Renewal & Replacement	Total Project Cost:	\$ 7,104,975.15
Department:	IT		

Description: 183A - Provide Electronic Toll Collection Integration and Maintenance Services (ETCS) including roadside functionality (AVI, AVC, VES, DVAS) and Toll Facility Host (TFH) functionality. The TFH functionality includes trip building, dynamic pricing, image processing, reporting/auditing, and interfaces with other CTRMA third-party systems.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast		Forecast
Year (FY)		
2024	\$	-
2025	\$	7,104,975.15
2026	\$	-
2027	\$	-
2028	\$	-
	\$	7,104,975.15

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	045	Budget Fiscal Year (FY):	2025
Project Title:	Roadway Traveler Communications - Roadside Units MIP	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac General	Total Project Cost:	\$ 235,638.00
Department:	IT		

Description: Installation of fifteen (15) roadside units (RSU) along the MoPac corridor to enable Connected Vehicle (CV) applications for the Mobility Authority to communicate directly to in-vehicle systems and improve the overall safety and mobility of the corridor.

Strategic Plan Alignment: Safety, Reliability, Innovation

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 235,638.00
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 235,638.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	052	Budget Fiscal Year (FY):	2028
Project Title:	Toll System Replacement	Roadway Impacted:	183S
Fund:	Renewal & Replacement	Total Project Cost:	\$ 10,000,000.00
Department:	IT		

Description: 183S - Provide Electronic Toll Collection Integration and Maintenance Services (ETCS) including roadside functionality (AVI, AVC, VES, DVAS) and Toll Facility Host (TFH) functionality. The TFH functionality includes trip building, dynamic pricing, image processing, reporting/auditing, and interfaces with other CTRMA third-party systems.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast		Forecast
Year (FY)		
2024	\$	-
2025	\$	-
2026	\$	-
2027	\$	-
2028	\$	10,000,000.00
	\$	10,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	053	Budget Fiscal Year (FY):	2023-24
Project Title:	Toll System Replacement	Roadway Impacted:	290E
Fund:	Renewal & Replacement	Total Project Cost:	\$ 12,396,000.00
Department:	IT		

Description: 290E - Provide Electronic Toll Collection Integration and Maintenance Services (ETCS) including roadside functionality (AVI, AVC, VES, DVAS) and Toll Facility Host (TFH) functionality. The TFH functionality includes trip building, dynamic pricing, image processing, reporting/auditing, and interfaces with other CTRMA third-party systems.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast		Forecast
Year (FY)		
2024	\$	12,396,000.00
2025	\$	-
2026	\$	-
2027	\$	-
2028	\$	-
	\$	12,396,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	054	Budget Fiscal Year (FY):	2026
Project Title:	Toll System Replacement	Roadway Impacted:	45SW
Fund:	Renewal & Replacement	Total Project Cost:	\$ 1,433,857.61
Department:	IT		

Description: 45SW - Provide Electronic Toll Collection Integration and Maintenance Services (ETCS) including roadside functionality (AVI, AVC, VES, DVAS) and Toll Facility Host (TFH) functionality. The TFH functionality includes trip building, dynamic pricing, image processing, reporting/auditing, and interfaces with other CTRMA third-party systems.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ 1,433,857.61
2027	\$ -
2028	\$ -
	\$ 1,433,857.61

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	055	Budget Fiscal Year (FY):	2023-2024
Project Title:	Toll System Replacement	Roadway Impacted:	71E
Fund:	Renewal & Replacement	Total Project Cost:	\$ 11,109,500.00
Department:	IT		

Description: 71E - Provide Electronic Toll Collection Integration and Maintenance Services (ETCS) including roadside functionality (AVI, AVC, VES, DVAS) and Toll Facility Host (TFH) functionality. The TFH functionality includes trip building, dynamic pricing, image processing, reporting/auditing, and interfaces with other CTRMA third-party systems.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast		Forecast
Year (FY)		
2024	\$	11,109,500.00
2025	\$	-
2026	\$	-
2027	\$	-
2028	\$	-
	\$	11,109,500.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	056	Budget Fiscal Year (FY):	2024
Project Title:	Toll System Replacement	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac General	Total Project Cost:	\$ 4,027,700.00
Department:	IT		

Description: MoPac - Provide Electronic Toll Collection Integration and Maintenance Services (ETCS) including roadside functionality (AVI, AVC, VES, DVAS) and Toll Facility Host (TFH) functionality. The TFH functionality includes trip building, dynamic pricing, image processing, reporting/auditing, and interfaces with other CTRMA third-party systems.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ 4,027,700.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 4,027,700.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	081	Budget Fiscal Year (FY):	2024
Project Title:	Kapsch Central Host Upgrades	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac Operating	Total Project Cost:	\$ 1,000,000.00
Department:	IT		

Description: Replacement, configuration, and data migration of core infrastructure equipment within the CTRMA TCS. This project is considered a hardware refresh of the image storage, data storage, application servers, and host servers for both primary and secondary systems.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ 1,000,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 1,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	082	Budget Fiscal Year (FY):	2024
Project Title:	DPS Enh-Release 5	Roadway Impacted:	SYSTEM
Fund:	Operating	Total Project Cost:	\$ 1,154,000.00
Department:	IT		

Description: Expected enhancements include a CSR Lookup Tool, enhancements for ease of use in DPS, additional reports, and dashboards. Additional long-term enhancements of Data Platform could include additional discount programs, account management, parking / airport parking, and data access for research or public use.

Strategic Plan Alignment: Reliability, Innovation

Project Forecast		Forecast
Year (FY)		
2024	\$	1,154,000.00
2025	\$	-
2026	\$	-
2027	\$	-
2028	\$	-
	\$	1,154,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	083	Budget Fiscal Year (FY):	2025
Project Title:	Kapsch Mopac Upgrades	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac Operating	Total Project Cost:	\$ 300,000.00
Department:	IT		

Description: Replacement, configuration, and data migration of core infrastructure equipment within the CTRMA TCS. This project is considered a hardware refresh of the image storage, data storage, application servers, and host servers for both primary and secondary systems.

Strategic Plan Alignment: Safety, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 300,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 300,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No



ENGINEERING

ENGINEERING

The role of the Engineering Department is to plan, develop, construct, and maintain major capital improvement projects in Williamson and Travis counties (from initial concept through final construction acceptance and into long term operations and maintenance).

The Engineering Department works extensively internally and externally to develop projects for the agency and region. These efforts include:

- **Project Inception and Feasibility.** Coordinate with other transportation providers in the region Texas Department of Transportation (TxDOT), Capital Area Metropolitan Planning Organization (CAMPO), City of Austin, City of Cedar Park, Travis County, and Williamson County to assure that all mobility needs are included in the region's Long Range Transportation Plan. Provide feasibility analysis for selected projects to evaluate implementation priority.
- **Project Development and Implementation.** Develop and implement priority projects based upon preliminary designs, appropriate level of environmental study, and input from regional transportation partners. Evaluate and determine the appropriate project delivery method based on complexity, stakeholders, and financial considerations. Manage the construction of all agency projects through project final acceptance.
- **Roadway and Facility Maintenance.** Inspect and manage routine roadway and facility maintenance, including all aspects of the roadway within the limits of the right-of-way, excluding the toll collection and toll systems infrastructure (which is maintained by the Operations Department). Develop, design, and manage repair and replacement projects. Roadway maintenance includes assuming responsibility for vegetative maintenance such as mowing, snow and ice operations, incident response, removal of debris and remedial repairs, as needed. The Mobility Authority takes the lead on managing the Performance Based Maintenance Contract (PBMC) with TxDOT reimbursing the agency for its portion of the maintenance responsibilities for shared facilities. Non-capital improvement initiatives are anticipated, including guardrail, cable barrier, bollard replacement and large sign replacement, to maintain safety.

Strategic Goals

- Build, operate and maintain toll and non-toll roads that reduce congestion and connect our region in innovative and safe ways
- Develop and adhere to a system-wide capital improvement plan
- Implement financial strategy and policies that prioritize long-term system health and growth, a decreased reliance on debt, and good financial stewardship
- Maintain and enhance our strategic partnerships to advance the common goals we share with our regional partner agencies
- Make targeted investments in other transportation solutions that connect to our system and enhance quality of life

Five-Year Capital Plan Engineering Department

Priority Rank #1						
Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
183A Added Capacity (Design)	\$ 27,000,000.00	\$ 8,714,000.00	\$ 8,714,000.00	\$ 8,714,000.00	\$ 858,000.00	\$ -
183A Phase II Small Sign Replacement	\$ 1,518,000.00	\$ 637,184.57	\$ -	\$ -	\$ -	\$ -
290E Maintenance Yard Expansion	\$ 85,000.00	\$ 85,000.00	\$ -	\$ -	\$ -	\$ -
290E Maintenance Yard Pond Expansion	\$ 35,000.00	\$ 35,000.00	\$ -	\$ -	\$ -	\$ -
290E PH IV (Design - Full Build - Schematic/Environmental)	\$ 50,000,000.00	\$ -	\$ 16,600,000.00	\$ 16,600,000.00	\$ 16,800,000.00	\$ -
Barton Skyway Development + Construction	\$ 10,107,058.93	\$ 5,300,000.00	\$ -	\$ -	\$ -	\$ -
CTB Delineator - 100' Spacing, 290@183, 290@130, 183@71, 71@130, 45SW@MoPac	\$ 62,700.00	\$ 62,700.00	\$ -	\$ -	\$ -	\$ -
CTB Delineator - 100' Spacing, 45SW	\$ 15,200.00	\$ 15,200.00	\$ -	\$ -	\$ -	\$ -
CTB Delineator - 100' Spacing, MoPac EL, North of FM 2222	\$ 37,150.00	\$ 37,150.00	\$ -	\$ -	\$ -	\$ -
CTB Delineator - 100' Spacing, MoPac EL, South of FM 2222	\$ 32,350.00	\$ 32,350.00	\$ -	\$ -	\$ -	\$ -
Maintenance Yard Improvement Support + Add'tl Site Investigations	\$ 800,000.00	\$ 800,000.00	\$ -	\$ -	\$ -	\$ -
MBGF Improvements - Project #2	\$ 3,000,000.00	\$ 3,000,000.00	\$ -	\$ -	\$ -	\$ -
MoPac PFC - Flexible Pavement w/Delineator Replacement	\$ 11,390,000.00	\$ -	\$ -	\$ 11,390,000.00	\$ -	\$ -
MoPac PFC Fog Seal and Surface Repair	\$ 1,800,000.00	\$ 1,800,000.00	\$ -	\$ -	\$ -	\$ -
Snow Equipment	\$ 35,000.00	\$ 35,000.00	\$ -	\$ -	\$ -	\$ -
Wall Monitoring - System Wide	\$ 300,000.00	\$ 300,000.00	\$ -	\$ -	\$ -	\$ -
45SW at 1626 Intersection	\$ 1,300,000.00	\$ 1,300,000.00	\$ -	\$ -	\$ -	\$ -
MoPac South (Preliminary Engineering/Procurement)	\$ 7,500,000.00	\$ -	\$ 3,750,000.00	\$ 3,750,000.00	\$ -	\$ -
Badger Pond Repair	\$ 405,000.00	\$ 405,000.00	\$ -	\$ -	\$ -	\$ -
Grand Total	\$ 115,422,458.93	\$ 22,558,584.57	\$ 29,064,000.00	\$ 40,454,000.00	\$ 17,658,000.00	\$ -

Priority Rank #2						
Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
183A Added Capacity (Construction)	\$ 142,000,000.00	\$ -	\$ -	\$ -	\$ 47,249,800.00	\$ 62,999,733.33
290E Added Capacity	\$ 94,000,000.00	\$ -	\$ -	\$ 8,367,450.00	\$ 8,367,450.00	\$ 25,811,500.00
290E Large & Small Sign Replacement	\$ 3,850,000.00	\$ -	\$ 3,850,000.00	\$ -	\$ -	\$ -
Maintenance Vehicle (1)	\$ 65,000.00	\$ -	\$ 65,000.00	\$ -	\$ -	\$ -
Maintenance Yard Site Acquisition (ROW Purchase)	\$ 4,400,000.00	\$ -	\$ 4,400,000.00	\$ -	\$ -	\$ -
Slab Stabilization for 183N	\$ 300,000.00	\$ -	\$ -	\$ 150,000.00	\$ 150,000.00	\$ -
Slab Stabilization for 183S	\$ 102,532.00	\$ -	\$ 102,532.00	\$ -	\$ -	\$ -
Slab Stabilization for 290E	\$ 1,000,000.00	\$ -	\$ 500,000.00	\$ 250,000.00	\$ 250,000.00	\$ -
MoPac South (D/B Construction)	\$ 1,000,000,000.00	\$ -	\$ -	\$ 195,200,000.00	\$ 195,200,000.00	\$ 195,200,000.00
290E PH IV (Construction - Full Build)	\$ 1,500,000,000.00	\$ -	\$ -	\$ -	\$ -	\$ 250,000,000.00
Grand Total	\$ 2,745,717,532.00	\$ -	\$ 8,917,532.00	\$ 203,967,450.00	\$ 251,217,250.00	\$ 534,011,233.33

Priority Rank #3						
Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
Bliss Spillar Drainage	\$ 840,000.00	\$ -	\$ 840,000.00	\$ -	\$ -	\$ -
Escarpment Turnaround	\$ 1,120,000.00	\$ -	\$ 1,120,000.00	\$ -	\$ -	\$ -
SB Windsor Exit Ramp	\$ 440,000.00	\$ -	\$ -	\$ -	\$ 440,000.00	\$ -
SH 71 TOM- Flexible Pavement	\$ 2,900,000.00	\$ -	\$ -	\$ 2,900,000.00	\$ -	\$ -
System-wide ITS SUE Investigations	\$ 2,760,000.00	\$ -	\$ 2,760,000.00	\$ -	\$ -	\$ -
Truss Bridge Aesthetics & Lighting (Montopolis Bridge)	\$ 7,166,000.00	\$ -	\$ -	\$ -	\$ -	\$ 7,166,000.00
Trails - SUP/Sidewalk	\$ 4,000,000.00	\$ -	\$ 1,000,000.00	\$ 1,000,000.00	\$ 1,000,000.00	\$ 1,000,000.00
Grand Total	\$ 19,226,000.00	\$ -	\$ 5,720,000.00	\$ 3,900,000.00	\$ 1,440,000.00	\$ 8,166,000.00

Priority Rank #4						
Project Title	Sum of Total Project Cost	2024	2025	2026	2027	2028
ENG Total All Ranks	\$ 2,880,365,990.93	\$ 22,558,584.57	\$ 43,701,532.00	\$ 248,321,450.00	\$ 270,315,250.00	\$ 542,177,233.33

Project Detail

Project ID:	003	Budget Fiscal Year (FY):	2023-2024
Project Title:	183A Phase II Small Sign Replacement	Roadway Impacted:	183A
Fund:	Renewal & Replacement	Total Project Cost:	\$ 1,518,000.00
Department:	Engineering		

Description: Replace all small signs along 183A Phase I & II

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 637,184.57
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 637,184.57

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	009	Budget Fiscal Year (FY):	2025
Project Title:	290E Large & Small Sign Replacement	Roadway Impacted:	290E
Fund:	Renewal & Replacement	Total Project Cost:	\$ 3,850,000.00
Department:	Engineering		

Description: Phase I & II Large and Small Sign Replacement

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 3,850,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 3,850,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	012	Budget Fiscal Year (FY):	2026
Project Title:	SH 71 TOM- Flexible Pavement	Roadway Impacted:	71E
Fund:	Renewal & Replacement	Total Project Cost:	\$ 2,900,000.00
Department:	Engineering		

Description: 1" TOM overlay of Express Lane

Strategic Plan Alignment: Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ 2,900,000.00
2027	\$ -
2028	\$ -
	\$ 2,900,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	015	Budget Fiscal Year (FY):	2025
Project Title:	Bliss Spillar Drainage	Roadway Impacted:	45SW
Fund:	General	Total Project Cost:	\$ 840,000.00
Department:	Engineering		

Description: Proposing to construct a detention pond at the intersection of Bliss Spillar to capture runoff causing issues and that wasn't accounted for in the initial design

Strategic Plan Alignment: Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 840,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 840,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	018	Budget Fiscal Year (FY):	2028
Project Title:	Truss Bridge Aesthetics & Lighting (Montopolis Bridge)	Roadway Impacted:	183S
Fund:	General	Total Project Cost:	\$ 7,166,000.00
Department:	Engineering		

Description: Aesthetic and pedestrian improvements along the Montopolis Truss Bridge

Strategic Plan Alignment: Innovation

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ 7,166,000.00
	\$ 7,166,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	019	Budget Fiscal Year (FY):	2025
Project Title:	Slab Stabilization for 183S	Roadway Impacted:	183S
Fund:	Renewal & Replacement	Total Project Cost:	\$ 102,532.00
Department:	Engineering		

Description: Slab Stabilization as necessary, locations TBD

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 102,532.00
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 102,532.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	021	Budget Fiscal Year (FY):	2026
Project Title:	Slab Stabilization for 183N	Roadway Impacted:	183N
Fund:	Renewal & Replacement	Total Project Cost:	\$ 150,000.00
Department:	Engineering		

Description: Slab Stabilization as necessary, locations TBD

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ 150,000.00
2027	\$ -
2028	\$ -
	<hr/>
	\$ 150,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	023	Budget Fiscal Year (FY):	2025
Project Title:	Maintenance Vehicle (1)	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 65,000.00
Department:	Engineering		

Description: Purchase of a new maintenance vehicle

Strategic Plan Alignment: Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 65,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 65,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	024	Budget Fiscal Year (FY):	2024
Project Title:	Maintenance Yard Improvement Support + Add'tl Site Investigations	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 800,000.00
Department:	Engineering		

Description: Research and site investigation for potential maintenance yard along 183A

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ 800,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 800,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	025	Budget Fiscal Year (FY):	2025
Project Title:	Maintenance Yard Site Acquisition (ROW Purchase)	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 4,400,000.00
Department:	Engineering		

Description: ROW purchase for potential maintenance yard along 183A

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 4,400,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 4,400,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	028	Budget Fiscal Year (FY):	2025
Project Title:	System-wide ITS SUE Investigations	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 2,760,000.00
Department:	Engineering		

Description: Includes 183A, MoPac Express, 290 Toll, 183 Toll, SH 71 Toll, and 45SW: Level B SUE for all ITS, with Level A potholes to confirm location every 200'.

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 2,760,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 2,760,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	029	Budget Fiscal Year (FY):	2024
Project Title:	Snow Equipment	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 35,000.00
Department:	Engineering		

Description: Snow Plow Truck attachment acquisition, truck mounted temp equipment, spreader truck mounted, ATV

Strategic Plan Alignment: Safety, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ 35,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 35,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	030	Budget Fiscal Year (FY):	2027-2029
Project Title:	183A Added Capacity (Construction)	Roadway Impacted:	SYSTEM
Fund:	Project	Total Project Cost:	\$ 142,000,000.00
Department:	Engineering		

Description: 183A additional lane in each direction from RM 1431 to Lakeline Mall Drive

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ -
2027	\$ 47,249,800.00
2028	\$ 62,999,733.33
	\$ 110,249,533.33

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	031	Budget Fiscal Year (FY):	2023-2024
Project Title:	Barton Skyway Development + Construction	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 10,107,058.93
Department:	Engineering		

Description: SB MoPac widening for an auxiliary lane and ramp merge lane between Barton Skyway and Loop 360

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 5,300,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 5,300,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	041	Budget Fiscal Year (FY):	2027
Project Title:	SB Windsor Exit Ramp	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac General	Total Project Cost:	\$ 440,000.00
Department:	Engineering		

Description: Mopac safety and operational improvements at the Southbound exit to Windsor Road

Strategic Plan Alignment: Safety, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ -
2027	\$ 440,000.00
2028	\$ -
	\$ 440,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	042	Budget Fiscal Year (FY):	2025
Project Title:	Escarpment Turnaround	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac General	Total Project Cost:	\$ 1,120,000.00
Department:	Engineering		

Description: 45SW addition of a Westbound to Eastbound U-Turn at Escarpment Blvd

Strategic Plan Alignment: Safety, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 1,120,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 1,120,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	043	Budget Fiscal Year (FY):	2026
Project Title:	MoPac PFC - Flexible Pavement w/Delineator Replacement	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac General	Total Project Cost:	\$ 11,390,000.00
Department:	Engineering		

Description: 1.5" PFC Mill and Inlay & delineator replacement, Parmer Ln to Cesar Chavez St

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ 11,390,000.00
2027	\$ -
2028	\$ -
	\$ 11,390,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	047	Budget Fiscal Year (FY):	2026-2030
Project Title:	MoPac South (D/B Construction)	Roadway Impacted:	MOPAC ML S
Fund:	Project	Total Project Cost:	\$ 1,000,000,000.00
Department:	Engineering		

Description: 2 Express Lanes in each direction from Cesar Chavez St. to Slaughter Ln.

Strategic Plan Alignment: Safety, Reliability

Project Forecast		Forecast
Year (FY)		
2024	\$	-
2025	\$	-
2026	\$	195,200,000.00
2027	\$	195,200,000.00
2028	\$	195,200,000.00
	\$	585,600,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	Yes

Project Detail

Project ID:	048	Budget Fiscal Year (FY):	2028-2033
Project Title:	290E PH IV (Construction - Full Build)	Roadway Impacted:	290E PH IV
Fund:	Project	Total Project Cost:	\$ 1,500,000,000.00
Department:	Engineering		

Description: 3 Tolled Lane and 3 GP lanes in each direction from SH 130 to SH 95

Strategic Plan Alignment: Safety, Reliability, Collaboration

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ 250,000,000.00
	\$ 250,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	Yes

Project Detail

Project ID:	049	Budget Fiscal Year (FY):	2026-2029
Project Title:	290E Added Capacity	Roadway Impacted:	290E
Fund:	Project	Total Project Cost:	\$ 94,000,000.00
Department:	Engineering		

Description: 290 Phase I & II, 1 additional lane in each direction from US 183 to SH 130

Strategic Plan Alignment: Safety, Reliability, Collaboration

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ 8,367,450.00
2027	\$ 8,367,450.00
2028	\$ 25,811,500.00
	\$ 42,546,400.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	058	Budget Fiscal Year (FY):	2025
Project Title:	Slab Stabilization for 290E	Roadway Impacted:	290E
Fund:	Renewal & Replacement	Total Project Cost:	\$ 250,000.00
Department:	Engineering		

Description: Slab Stabilization as necessary, locations TBD

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 250,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 250,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	059	Budget Fiscal Year (FY):	2025
Project Title:	Slab Stabilization for 290E	Roadway Impacted:	290E
Fund:	Renewal & Replacement	Total Project Cost:	\$ 250,000.00
Department:	Engineering		

Description: Slab Stabilization as necessary, locations TBD

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 250,000.00
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 250,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	060	Budget Fiscal Year (FY):	2026
Project Title:	Slab Stabilization for 290E	Roadway Impacted:	290E
Fund:	Renewal & Replacement	Total Project Cost:	\$ 250,000.00
Department:	Engineering		

Description: Slab Stabilization as necessary, locations TBD

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ 250,000.00
2027	\$ -
2028	\$ -
	<hr/>
	\$ 250,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	061	Budget Fiscal Year (FY):	2027
Project Title:	Slab Stabilization for 290E	Roadway Impacted:	290E
Fund:	Renewal & Replacement	Total Project Cost:	\$ 250,000.00
Department:	Engineering		

Description: Slab Stabilization as necessary, locations TBD

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ -
2027	\$ 250,000.00
2028	\$ -
	\$ 250,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	062	Budget Fiscal Year (FY):	2027
Project Title:	Slab Stabilization for 183N	Roadway Impacted:	183N
Fund:	Renewal & Replacement	Total Project Cost:	\$ 150,000.00
Department:	Engineering		

Description: Slab Stabilization as necessary, locations TBD

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ -
2026	\$ -
2027	\$ 150,000.00
2028	\$ -
	\$ 150,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	065	Budget Fiscal Year (FY):	2024-2027
Project Title:	183A Added Capacity (Design)	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 27,000,000.00
Department:	Engineering		

Description: 183A additional lane in each direction from RM 1431 to Lakeline Mall Dr.

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 8,714,000.00
2025	\$ 8,714,000.00
2026	\$ 8,714,000.00
2027	\$ 858,000.00
2028	\$ -
	\$ 27,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	066	Budget Fiscal Year (FY):	2024
Project Title:	MoPac South (Preliminary Engineering/Procurement)	Roadway Impacted:	MOPAC ML S
Fund:	General	Total Project Cost:	\$ 7,500,000.00
Department:	Engineering		

Description: 2 Express Lanes in each direction from Cesar Chavez St. to Slaughter Ln.

Strategic Plan Alignment: Safety, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 3,750,000.00
2026	\$ 3,750,000.00
2027	\$ -
2028	\$ -
	<hr/>
	\$ 7,500,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	067	Budget Fiscal Year (FY):	2024-2026
Project Title:	290E PH IV (Design - Full Build - Schematic/Environmental)	Roadway Impacted:	290E PH IV
Fund:	Project	Total Project Cost:	\$ 50,000,000.00
Department:	Engineering		

Description: 3 Tolled Lane and 3 GP lanes in each direction from SH 130 to SH 95

Strategic Plan Alignment: Safety, Reliability, Collaboration

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 16,600,000.00
2026	\$ 16,600,000.00
2027	\$ 16,800,000.00
2028	\$ -
	\$ 50,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	Yes

Project Detail

Project ID:	068	Budget Fiscal Year (FY):	2024
Project Title:	MBGF Improvements - Project #2	Roadway Impacted:	183A
Fund:	Renewal & Replacement	Total Project Cost:	\$ 3,000,000.00
Department:	Engineering		

Description: 183A Ph. I & II MBGF Upgrades to the remaining tolled lanes and ramps

Strategic Plan Alignment: Safety, Stewardship, Innovation

Project Forecast Year (FY)	Forecast
2024	\$ 3,000,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 3,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	069	Budget Fiscal Year (FY):	2024
Project Title:	Wall Monitoring - System Wide	Roadway Impacted:	SYSTEM
Fund:	Renewal & Replacement	Total Project Cost:	\$ 300,000.00
Department:	Engineering		

Description: Procurement and implementation of wall monitoring system - System Wide

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 300,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 300,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	070	Budget Fiscal Year (FY):	2024
Project Title:	MoPac PFC Fog Seal and Surface Repair	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac Operating	Total Project Cost:	\$ 1,800,000.00
Department:	Engineering		

Description: MoPac EL Fog seal + Repair of 5% of area

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 1,800,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/> \$ 1,800,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	072	Budget Fiscal Year (FY):	2024
Project Title:	45SW at 1626 Intersection	Roadway Impacted:	45SW
Fund:	Renewal & Replacement	Total Project Cost:	\$ 1,300,000.00
Department:	Engineering		

Description: Milling off PFC and replacing with HMA at the 45SW & FM 1626 Intersection

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 1,300,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	\$ 1,300,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	073	Budget Fiscal Year (FY):	2024
Project Title:	Badger Pond Repair	Roadway Impacted:	183A
Fund:	Renewal & Replacement	Total Project Cost:	\$ 405,000.00
Department:	Engineering		

Description: Repairing pond outfall and replacing sedimentation basin base

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 405,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 405,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	074	Budget Fiscal Year (FY):	2024
Project Title:	290E Maintenance Yard Pond Expansion	Roadway Impacted:	290E
Fund:	General	Total Project Cost:	\$ 35,000.00
Department:	Engineering		

Description: Water quality pond expansion related to parking lot expansion at the 290E maintenance yard

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ 35,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 35,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	075	Budget Fiscal Year (FY):	2024
Project Title:	290E Maintenance Yard Expansion	Roadway Impacted:	290E
Fund:	General	Total Project Cost:	\$ 85,000.00
Department:	Engineering		

Description: Parking Lot expansion at the 290E maintenance yard

Strategic Plan Alignment: Stewardship, Reliability

Project Forecast Year (FY)	Forecast
2024	\$ 85,000.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 85,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	077	Budget Fiscal Year (FY):	2024
Project Title:	CTB Delineator - 100' Spacing, 290@183, 290@130, 183@71, 71@130, 45SW@MoPac	Roadway Impacted:	SYSTEM
Fund:	Renewal & Replacement	Total Project Cost:	\$ 62,700.00
Department:	Engineering		

Description: Replacement of Concrete Traffic Barrier (CTB) Delineators

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 62,700.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/> \$ 62,700.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	078	Budget Fiscal Year (FY):	2024
Project Title:	CTB Delineator - 100' Spacing, MoPac EL, South of FM 2222	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac General	Total Project Cost:	\$ 32,350.00
Department:	Engineering		

Description: Replacement of Concrete Traffic Barrier (CTB) Delineators

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 32,350.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 32,350.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	079	Budget Fiscal Year (FY):	2024
Project Title:	CTB Delineator - 100' Spacing, MoPac EL, North of FM 2222	Roadway Impacted:	MOPAC MNLN
Fund:	MoPac General	Total Project Cost:	\$ 37,150.00
Department:	Engineering		

Description: Replacement of Concrete Traffic Barrier (CTB) Delineators

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 37,150.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 37,150.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No

Project Detail

Project ID:	080	Budget Fiscal Year (FY):	2024
Project Title:	CTB Delineator - 100' Spacing, 45SW	Roadway Impacted:	45SW
Fund:	Renewal & Replacement	Total Project Cost:	\$ 15,200.00
Department:	Engineering		

Description: Replacement of Concrete Traffic Barrier (CTB) Delineators

Strategic Plan Alignment: Safety, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ 15,200.00
2025	\$ -
2026	\$ -
2027	\$ -
2028	\$ -
	<hr/>
	\$ 15,200.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
No	No

Project Detail

Project ID:	085	Budget Fiscal Year (FY):	2025
Project Title:	Trails - SUP/Sidewalk	Roadway Impacted:	SYSTEM
Fund:	General	Total Project Cost:	\$ 4,000,000.00
Department:	Engineering		

Description: Project Call; connecting our trail system with other entities

Strategic Plan Alignment: Safety, Reliability, Stewardship

Project Forecast Year (FY)	Forecast
2024	\$ -
2025	\$ 1,000,000.00
2026	\$ 1,000,000.00
2027	\$ 1,000,000.00
2028	\$ 1,000,000.00
	\$ 4,000,000.00

Impact to Future Operating Budget (Y/N)	FTE Needed (Y/N)
Yes	No



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

3300 N IH-35, Suite 300
Austin, TX 78705



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #9

Discuss and consider approving and interlocal agreement with the Cameron County Regional Mobility Authority for transaction processing services

Strategic Plan Relevance:	Collaboration, Service, Stewardship
Department:	Operations
Contact:	Tracie Brown, Director of Operations
Associated Costs:	None
Funding Source:	Operating Budget
Action Requested:	Consider and act on draft resolution

Background: As the first regional mobility authority established in Texas, the Central Texas Regional Mobility Authority has always sought to assist other regional mobility authorities in achieving their mission. In keeping with this sentiment, the CTRMA Board of Directors approved interlocal agreements with the Cameron County Regional Mobility Authority (CCRMA), the Camino Real Regional Mobility Authority (CRRMA) and the North East Texas Regional Mobility Authority (NET RMA) to facilitate their toll tag transactions through the interoperability hub and reconcile payment. The agreement also allowed the RMAs to process their video toll transactions through CTRMA's third-party vendor if requested. This approach allowed the Mobility Authority to keep its sister RMA's initial operational costs down as they ramped up their operations.

In 2017 CCRMA assumed responsibility for its own video toll collection program and requested that the Mobility Authority continue to provide tag transaction processing services through a new Interlocal Agreement. The term of the previous ILA concluded on August 31, 2023. The ILA included a provision that the term could be extended by written agreement by both parties and terminated upon ninety (90) days written notice.

Current Action: The new Interlocal Agreement sets forth the terms and conditions under which the Mobility Authority will provide the same transaction processing services as requested before. CCRMA's transactions will be forwarded to CTRMA's Data Platform

System (DPS) which will route them to the Central United States Interoperability (CUSIOP) or Southeast Interoperability (SEIOP) hub for attempted posting. Transactions that do not post to a valid customer account will be routed back to CCRMA for invoicing.

The new ILA set forth a fee for every CCRMA transaction processed through the DPS to offset the related operations and maintenance costs. In addition, CCRMA will pay its proportionate share of the annual interoperability hub software and hardware maintenance costs required by CTRMA as a part of the Central United States Interoperability (CUSIOP) Agreement as well as any CUSIOP hub enhancements.

The term of the ILA will conclude on August 31, 2028, subject to early termination of the CSIOP or SEIOP Agreement. CTRMA is required to provide written notice to CCRMA within five days of such termination. The ILA may be terminated upon ninety (90) days written notice of either party to the other or by mutual written agreement of both parties.

Previous Actions & Brief History of the Program/Project: In December 2011 to provide electronic toll transaction processing and video toll collection services through the Mobility Authority's third-party vendors. This agreement was extended in November 2020 to a new termination date of June 30, 2020.

Financing: N/A

Action requested/Staff Recommendation: Staff recommends approval of the new interlocal agreement with the Cameron County Regional Mobility Authority.

Backup provided: Draft resolution
CTRMA - CCRMA Interlocal Agreement

**GENERAL MEETING OF THE BOARD OF DIRECTORS
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**

RESOLUTION NO. 23-0XX

**APPROVING AN INTERLOCAL AGREEMENT TO PROVIDE
TRANSPONDER TRANSACTION PROCESSING SERVICES TO THE
CAMERON COUNTY REGIONAL MOBILITY AUTHORITY**

WHEREAS, by Resolution No. 20-088, dated December 16, 2020, the Board approved an interlocal agreement with the Cameron County Regional Mobility Authority (“CCRMA”) under Chapter 791 of the Texas Government Code and Section 370.033 of the Transportation Code by which the Mobility Authority provided toll processing and collection services to CCRMA; and

WHEREAS, the current interlocal agreement with CCRMA expired on August 31, 2023; and

WHEREAS, CCRMA has requested that the Mobility Authority continue providing them transponder transaction processing services; and

WHEREAS, the Executive Director and CCRMA have negotiated a new interlocal agreement whereby the Mobility Authority would continue providing transponder transaction processing services to CCRMA with all costs associated with the services to be borne by CCRMA, including a proportionate share of the annual interoperability hub software and hardware maintenance costs; and

WHEREAS, the Executive Director recommends that the Board approve the proposed interlocal agreement with CCRMA in the form or substantially the same form attached hereto as Exhibit A.

NOW THEREFORE, BE IT RESOLVED that the Board hereby approves the proposed interlocal agreement with CCRMA to continue providing transponder transaction processing services and authorizes the Executive Director to finalize and execute the interlocal agreement on behalf of the Mobility Authority in the form or substantially the same form as Exhibit A hereto.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

Robert W. Jenkins, Jr.
Chairman, Board of Directors

Exhibit A

INTERLOCAL AGREEMENT

THIS INTERLOCAL AGREEMENT (the “Agreement”) is made and entered into effective as of the October 1, 2023, by and between the CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY (“CTRMA”) and the CAMERON COUNTY REGIONAL MOBILITY AUTHORITY (“CCRMA”), political subdivisions of the State of Texas (collectively, the “Parties”).

WITNESSETH:

WHEREAS, CTRMA is a regional mobility authority created pursuant to the request of Travis and Williamson Counties and operating pursuant to Chapter 370 of the Texas Transportation Code (the “RMA Act”) and 43 TEX. ADMIN. CODE §§ 26.1 *et seq.* (the “RMA Rules”); and

WHEREAS, CTRMA is a party to the Central United States Interoperability Agreement and the Southern States Interoperability Agreement (collectively, the “Interoperability Agreements”), through which toll transactions on various tolled facilities throughout the central and southeast United States are processed and credited to the operator of the facility on which the transaction occurred; and

WHEREAS, CTRMA has developed a proprietary Data Platform System (“DPS”) to submit transactions to the Central United States Interoperability Hub and the South-East Interoperability Hub (collectively, the “Interoperability Hubs”) for processing pursuant to the Interoperability Agreements; and

WHEREAS, CCRMA is a regional mobility authority created pursuant to the request of Cameron County and operating pursuant to the RMA Act and the RMA Rules; and

WHEREAS, CCRMA currently operates the SH 550 Phase I, Segment 1, Direct Connectors and North Port Spur facilities (collectively, the “CCRMA Projects”) and

WHEREAS, CCRMA is in need of transponder-based toll transaction processing services related to the CCRMA Projects and potentially other future transportation projects; and

WHEREAS, Chapter 791 of the Texas Government Code provides that any one or more public agencies may contract with each other for the performance of governmental functions or services in which the contracting parties are mutually interested; and

WHEREAS, Section 370.033 of the RMA Act provides that a regional mobility authority may enter into contracts or agreements with another governmental entity; and

WHEREAS, the Parties have agreed that it would be to their mutual benefit for CTRMA to facilitate the processing of CCRMA’s transactions with CTRMA’s connection to the Interoperability Hubs through its DPS and the Interoperability Agreements; and

WHEREAS, this Interlocal Agreement is made in accordance with TEX. GOV'T CODE § 791.025 to the extent applicable;

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the undersigned Parties agree as follows:

I. FINDINGS

Recitals. The recitals set forth above are incorporated herein for all purposes and are found by the Parties to be true and correct. It is further found and determined that the Parties have authorized and approved the Agreement by resolution or order adopted by their respective governing bodies, and that this Agreement will be in full force and effect when approved by each party.

II. ACTIONS

1. Provision of Services. Subject to the terms of this Agreement, CTRMA and/or its consultants shall facilitate CCRMA's utilization of the resources and services provided through (i) CTRMA's DPS; (ii) the Interoperability Agreements; and (iii) any amendments or successor agreements, in connection with the provision of transponder-based transaction processing for the CCRMA Projects and any future CCRMA transportation projects.

2. Transponder-based Transactions and Associated Expenses. CTRMA shall submit transponder-based transactions received from CCRMA's Kapsch Project Host Server to the Interoperability Hubs (or any subsequent hub established for transaction processing). The Scope of Services associated with transponder-based transaction processing provided for hereunder is set forth on Attachment "A"; and the fees for such services are set forth on Attachment "B".

3. Associated Expenses. CTRMA is periodically assessed certain costs for maintenance, hardware, software, third party audits, required testing, host server processing enhancements and other miscellaneous costs as a party to the Central United States Interoperability Agreement. Such costs are borne by all the parties to that agreement based on the relative volume of transactions processed for each party in relation to the total volume of transactions processed by the Central United States Interoperability Hub. Because costs are charged to CTRMA as a result of CCRMA's transactions, CCRMA shall reimburse CTRMA for the portion of CTRMA's costs that are attributable to the proportional volume of CCRMA's transactions. The calculation will be based on CCRMA and CTRMA transactions for the previous calendar year. In the event that changes occur to cost sharing under either of the Interoperability Agreements or CCRMA becomes a direct party to either of the Interoperability Agreements or the Interoperability Hubs, the Parties agree to amend this Agreement as necessary to accommodate the changes.

III.
GENERAL AND MISCELLANEOUS

1. Term and Termination. Subject to the following, this Agreement shall be effective as of the date first written above and shall continue in full force and effect until August 31, 2028, unless otherwise terminated as set forth below:

- a. if the Central United States Interoperability Agreement or the Southern States Interoperability Agreement is terminated, this Agreement shall terminate on the same day that the Central United States Interoperability Agreement or the Southern States Interoperability Agreement terminates. CTRMA shall give CCRMA written notice of the termination within five (5) business days of the termination;
- b. either party may terminate this Agreement upon ninety (90) days written notice to the other; or
- c. this Agreement may be terminated by mutual written agreement of the Parties.

2. Prior Written Agreements. This Agreement is without regard to any and all prior written contracts or agreements between the Parties regarding any other subject matter and does not modify, amend, ratify, confirm, or renew any such other prior contract or agreement between the Parties.

3. Other Services. Nothing in this Agreement shall be deemed to create, by implication or otherwise, any duty or responsibility of either of the Parties to undertake or not to undertake any other service, or to provide or not to provide any service, except as specifically set forth in this Agreement or in a separate written instrument executed by both Parties.

4. Governmental Immunity. Nothing in this Agreement shall be deemed to waive, modify, or amend any legal defense available at law or in equity to either of the Parties nor to create any legal rights or claims on behalf of any third party. Neither of the Parties waives, modifies, or alters to any extent whatsoever the availability of the defense of governmental immunity under the laws of the State of Texas and of the United States.

5. Amendments and Modifications. This Agreement may not be amended or modified except in writing and executed by both Parties to this Agreement and authorized by their respective governing bodies.

6. Severability. If any provision of this Agreement shall be held invalid or unenforceable by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision hereof, but rather this entire Agreement will be construed as if not containing the particular invalid or unenforceable provision(s), and the rights and obligations of the Parties shall be construed and enforced in accordance therewith. The Parties acknowledge that if any provision of this Agreement is determined to be invalid or unenforceable, it is their desire and intention that such provision be reformed and construed in such a manner that it will, to the maximum extent practicable, give effect to the intent of this Agreement and be deemed to be validated and enforceable.


7. **Execution in Counterparts.** This Agreement may be simultaneously executed in several counterparts, each of which shall be an original and all of which shall be considered fully executed as of the date first written above, when both Parties have executed an identical counterpart, notwithstanding that all signatures may not appear on the same counterpart.

IN WITNESS WHEREOF, the Parties have executed and attested this Agreement by their officers thereunto duly authorized.

**CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY**

By: _____
James M. Bass
Executive Director

**CAMERON COUNTY
REGIONAL MOBILITY AUTHORITY**

By:  _____
Pete Sepulveda, Jr.
Executive Director

ATTACHMENT "A"

SCOPE OF SERVICES-TRANSPONDER TRANSACTIONS

1. CCRMA shall submit transponder-based transactions to CTRMA's DPS through CCRMA's Kapsch Project Host Server.
2. CTRMA shall submit transponder-based transactions received from CCRMA to the Interoperability Hubs (or any subsequent hub established for transaction processing), in accordance with the approved interoperable business rules and interface control documents. CTRMA will ensure the transactions are submitted to the Interoperability Hubs but does not guarantee any performance related to acceptance by the Interoperability Hubs, collections or payment.
3. CTRMA shall collect and distribute to CCRMA toll funds collected on behalf of CCRMA within two weeks after CTRMA has received funds due from the last of the other toll agencies remitting funds for CTRMA and/or CCRMA transactions for the preceding month. CTRMA will only forward funds to CCRMA that it receives related to CCRMA's transactions. CTRMA bears no responsibility for funds that have not been reconciled or paid. Payments due to CCRMA shall be made via wire transfer to Texas Regional Bank.
4. CTRMA shall provide timely assistance to CCRMA in properly reconciling the payments from CTRMA to CCRMA.
5. CTRMA shall make a good faith effort to include CCRMA in the review of toll transaction processing agreements that affect the processing of CCRMA transactions or may result in a change to the toll transaction fee structure or performance measures.
6. Either directly or through access to consultant-provided systems and reports, CTRMA shall make all reasonable efforts to provide to CCRMA the same access to information and reports that CTRMA requires to audit, reconcile, or resolve customer service or financial related matters related to electronic toll transactions.
7. CTRMA shall make all reasonable efforts to provide to CCRMA the same ownership of toll transaction related information that CTRMA is afforded through their consultant agreements.
8. Per Article II.3 of the Agreement, CCRMA will reimburse CTRMA for a proportional share of certain actual costs incurred as a party to the Central United States Interoperability Agreement.

ATTACHMENT “B”

TRANSPONDER TRANSACTION FEES

Transactions submitted to the Central United States Interoperability Hub through CTRMA shall be processed at the cost prescribed in the Central United States Interoperability Agreement. The current transaction fees are \$0.05 + 3% of the toll for each transaction or a minimum of \$0.08. These fees will be deducted from the amounts due to CCRMA.

Transactions submitted to the Southern States Interoperability Hub through CTRMA shall be processed at the cost prescribed in the Southern States Interoperability Agreement. The current transaction fees are 3% of the toll for each transaction. These fees will be deducted from the amounts due to CCRMA.

CTRMA DATA PLATFORM TRANSACTION PROCESSING FEES

Transactions submitted to CTRMA’s Data Platform System (DPS) through CCRMA’s Kapsch Project Host Server shall be processed at a cost of \$0.0163 for each transaction. These fees will be deducted from the amounts due to CCRMA.



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #10

Discuss and consider approving a contract with Kapsch TrafficCom USA, Inc. to provide intelligent transportation system performance-based maintenance services for the Mobility Authority's toll system

Strategic Plan Relevance:	Innovation
Department:	Operations
Contact:	Greg Mack, Director of IT and Toll Systems
Associated Costs:	Not to Exceed \$1,940,000
Funding Source:	Operating Budget
Action Requested:	Consider and act on draft resolution

Project Description/Background: The Intelligent Transportation System (ITS) Performance-based Maintenance Services will include maintenance and construction services by a qualified ITS device maintenance and construction firm for all work related to ITS devices, communications, electrification, and infrastructure. The services will cover all existing and future ITS elements on the Mobility Authority's system.

The objective of these services is to ensure continuous (24 hours/day, 7 days/week, 365 days/year) operation and functionality of all components of the Mobility Authority's ITS system and provide locate services for all ITS equipment. The provider shall be on-call on a 24/7/365 basis for the duration of the contract to respond to emergency repair and/or replacement work, including but not limited to severe weather events and warnings. Normal maintenance activities will be covered under one work authorization, while separate work authorizations will be issued for other services, such as emergency and major repairs.

Each corridor of the Mobility Authority roadway system contains a segment of the Mobility Authority's ITS, tolling, and communications network. The field communications network provides the link between the ITS and tolling elements to the

Traffic Incident Management Center hub. In the majority of locations, ITS infrastructure and tolling facilities are physically separated, however in several locations ITS and tolling infrastructure are collocated.

ITS Field Components consist of all field equipment deployed for the real-time collection, processing, analysis and dissemination of traffic and roadway data, that is not utilized by the tolling system. Field components include field devices (e.g., CCTV cameras, radar vehicle sensing devices, dynamic message signs, connected vehicle roadside units); device cabinet assemblies; network communication equipment (e.g., managed field ethernet switches, fiber optic patch panels, wireless radios); electrification equipment (e.g., power panels, power distribution unit, surge protection devices, power supplies, service disconnects, service transformers, utility meters, grounding); and physical infrastructure (e.g., cabling, conduit, ductbank, underground cable vaults, ground boxes, device poles).

Kapsch TrafficCom USA, Inc. is currently tasked with installing and maintaining the Mobility Authority's tolling and ITS systems. These services will be transitioned to the new provider.

Previous Actions & Brief History of the Program/Project:

The procurement milestones are detailed below.

- Board Approval to Issue Request for Proposals (RFP): October 26, 2022
- Issuance of RFP: January 27, 2023
- RFP Q&A Period: January 30 – March 15, 2023
- Deadline for submitting RFPs: March 31, 2023
- Issuance of request for Best and Final Offer (BAFO): June 7, 2023
- BAFO Q&A Period: June 8 – June 28, 2023
- Proposer Interviews: June 20 – June 21, 2023
- Deadline for submitting BAFOs: July 12, 2023
- Proposer BAFO Clarification Interviews: August 11 – August 14, 2023

By the deadline of March 31, 2023, each of the following firms had submitted a response to the RFP:

- Kapsch TrafficCom USA, Inc.
- Lumin8 Transportation Technologies, LLC
- SICE Inc.

Evaluation committees evaluated responses. The committees reviewed the proposals, conducted interviews for all proposers, and scored the results. Scoring is weighted, based on the following criteria:

		Pass/Fail
Financial Review		
Technical Response	30%	-----
Personnel and DBE Participation	30%	
Cost Proposal		60%
		40%
TOTAL		100%

The highest score, based on the evaluated responses and pricing, was given to Kapsch TrafficCom USA, Inc.

Financing: Operations Budget

Action requested/Staff Recommendation: Staff recommends awarding a contract to Kapsch TrafficCom USA, Inc. for Intelligent Transportation System (ITS) Performance-Based Maintenance Services.

Backup provided: Draft resolution
Draft contract

**GENERAL MEETING OF THE BOARD OF DIRECTORS
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**

RESOLUTION NO. 23-0XX

**APPROVE A CONTRACT WITH KAPSCH TRAFFICOM USA, INC. FOR INTELLIGENT
TRANSPORTATION SYSTEM PERFORMANCE-BASED MAINTENANCE SERVICES**

WHEREAS, the Mobility Authority has an ongoing need for intelligent transportation system (ITS) maintenance and construction services for all existing and future ITS elements on the Mobility Authority's system, including installation services, on-call emergency repair and/or replacement work, and regular maintenance related to ITS devices, communications, electrification, and infrastructure; and

WHEREAS, by Resolution No. 22-049, dated October 26, 2022, the Board approved the release of a request for proposals (RFP) for ITS Performance-Based Maintenance Services; and

WHEREAS, the Mobility Authority issued an RFP for ITS Performance-Based Maintenance Services on January 27, 2023, and subsequently issued a request for best and final offers (BAFO) on June 7, 2023, to the three firms that responded to the RFP; and

WHEREAS, each of the three offers received by the July 12, 2023 deadline to respond to the BAFO were evaluated by Mobility Authority operations and information technology staff who determined that the offer submitted by Kapsch TrafficCom USA, Inc, provides the best value to the Mobility Authority based on the criteria established in the RFP; and

WHEREAS, based on the results of the Mobility Authority staff's evaluations, the Executive Director recommends that the Board approve a contract Kapsch TrafficCom USA, Inc. for ITS performance-based maintenance services in an amount not to exceed \$1,940,000.00 and in the form or substantially the same form attached hereto as Exhibit A.

NOW THEREFORE, BE IT RESOLVED that the Board hereby approves a contract with Kapsch TrafficCom USA, Inc. for ITS performance-based maintenance services in an amount not to exceed \$1,940,000.00 and authorizes the Executive Director to finalize and execute the contract in the form or substantially the same form attached hereto as Exhibit A

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

Robert W. Jenkins, Jr.
Chairman, Board of Directors

Exhibit A

CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY

AGREEMENT FOR

INTELLIGENT TRANSPORTATION SYSTEM

PERFORMANCE-BASED MAINTENANCE SERVICES

Table of Contents

	<u>Page</u>
<u>ARTICLE 1</u> THE SERVICES	1
<u>ARTICLE 2</u> PROSECUTION OF WORK AND COMPENSATION.....	2
<u>ARTICLE 3</u> TERM OF AGREEMENT.....	6
<u>ARTICLE 4</u> TERMINATION FOR DEFAULT	6
<u>ARTICLE 5</u> OPTIONAL TERMINATION.....	7
<u>ARTICLE 6</u> TERMINATION, GENERALLY	8
<u>ARTICLE 7</u> SERVICE LEVEL AGREEMENTS AND PERFORMANCE GUARANTY	8
<u>ARTICLE 8</u> SUSPENSION OR MODIFICATION OF SERVICES; DELAYS AND DAMAGES.....	11
<u>ARTICLE 9</u> PERSONNEL, EQUIPMENT AND MATERIAL, GENERALLY	11
<u>ARTICLE 10</u> KEY PERSONNEL	12
<u>ARTICLE 11</u> BUSINESS OPPORTUNITY PROGRAM AND POLICY COMPLIANCE	12
<u>ARTICLE 12</u> PLANNING AND PERFORMANCE REVIEWS; INSPECTIONS.....	13
<u>ARTICLE 13</u> OWNERSHIP OF REPORTS.....	13
<u>ARTICLE 14</u> SUBLETTING OF WORK.....	15
<u>ARTICLE 15</u> APPEARANCE AS WITNESS AND ATTENDANCE AT MEETINGS	15
<u>ARTICLE 16</u> COMPLIANCE WITH LAWS AND AUTHORITY POLICIES; PROTECTION OF DATA AND INFORMATION.....	15
<u>ARTICLE 17</u> AUTHORITY INDEMNIFIED	18
<u>ARTICLE 18</u> CONFLICTS OF INTEREST	18
<u>ARTICLE 19</u> INSURANCE.....	19
<u>ARTICLE 20</u> COORDINATION OF CONTRACT DOCUMENTS	20
<u>ARTICLE 21</u> MAINTENANCE OF, ACCESS TO, AND AUDIT OF RECORDS	21
<u>ARTICLE 22</u> RELATIONSHIP BETWEEN THE PARTIES	22
<u>ARTICLE 23</u> DELIVERY OF NOTICES, ETC.	23

Table of Contents
(continued)

	<u>Page</u>
<u>ARTICLE 24</u> REPORTING OF SUBPOENAS, NOTICES, ETC.	23
<u>ARTICLE 25</u> AUTHORITY’S ACTS.....	23
<u>ARTICLE 26</u> LIMITATIONS	24
<u>ARTICLE 27</u> CAPTIONS NOT A PART HEREOF	24
<u>ARTICLE 28</u> CONTROLLING LAW, VENUE.....	24
<u>ARTICLE 29</u> COMPLETE AGREEMENT	24
<u>ARTICLE 30</u> TIME OF ESSENCE	24
<u>ARTICLE 31</u> SEVERABILITY	25
<u>ARTICLE 32</u> AUTHORIZATION.....	25
<u>ARTICLE 33</u> SUCCESSORS	25
<u>ARTICLE 34</u> INTERPRETATION.....	25
<u>ARTICLE 35</u> BENEFITS INURED.....	25
<u>ARTICLE 36</u> SURVIVAL	26
<u>ARTICLE 37</u> FORCE MAJEURE	26
<u>ARTICLE 38</u> DISPUTE RESOLUTION.....	27
<u>ARTICLE 39</u> CONTRACTOR CERTIFICATIONS	28
 APPENDICES:	
APPENDIX A — Scope of Services	
APPENDIX B — Form of Work Authorization	
APPENDIX C — ITS Equipment Prices	
APPENDIX D — Maintenance Services Unit Prices	
APPENDIX E — Labor Rates	
APPENDIX F — Service Level Agreements	
APPENDIX G — Key Personnel	
APPENDIX H — Contractor’s Proposal	
APPENDIX I-1 — Form of Installation Performance Bond	
APPENDIX I-2 — Form of Installation Payment Bond	
APPENDIX J-1 — Form of Maintenance Performance Bond	
APPENDIX J-2 — Form of Maintenance Payment Bond	

**CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY
AGREEMENT FOR
INTELLIGENT TRANSPORTATION SYSTEM PERFORMANCE-BASED
MAINTENANCE SERVICES**

This Agreement for Intelligent Transportation System Performance-Based Maintenance Services (the “Agreement”) is made and entered into by and between the Central Texas Regional Mobility Authority (the “CTRMA”), a regional mobility authority and a political subdivision of the State of Texas, and Kapsch TrafficCom USA, Inc. (the “Contractor”), to be effective as of the 1 day of November, 2023 (the “Effective Date”).

WITNESSETH:

The parties acknowledge the following:

WHEREAS, pursuant to that certain Request for Proposals dated January 27, 2023 (the “RFP”), the CTRMA sought to identify and obtain the services of a qualified firm to provide intelligent transportation system (“ITS”) performance-based maintenance services (PBMC) for the CTRMA, and, potentially, other toll authorities; and

WHEREAS, three (3) firms were shortlisted from a total of three (3) firms that submitted responses setting forth their respective qualifications and proposals for the work; and

WHEREAS, pursuant to Resolution No. _____, approved on October 25, 2023, the Board authorized the execution of this Agreement; and

WHEREAS, this Agreement has been negotiated and finalized between the parties whereby services will be provided by the Contractor and compensation will be paid by the CTRMA pursuant to the terms hereof.

NOW, THEREFORE, in consideration of the benefits received and realized by the respective parties hereto, the parties do hereby agree as follows:

**ARTICLE 1
THE SERVICES**

The CTRMA hereby retains the Contractor, as an independent contractor, and the Contractor agrees to provide ITS performance-based maintenance services to the CTRMA, and possibly other toll authorities upon the terms and conditions provided in this Agreement. The scope of services are described in Appendix “A”, and shall include, but not be limited to: (1) the maintenance of CTRMA’s ITS facilities and equipment (the “Maintenance Services”); and (2) the construction and installation of replacement CTRMA’s ITS facilities and equipment (the “Installation Services”) (the Maintenance Services and Installation Services, along with other services described in Appendix “A”, are collectively referred to herein as the “Services”).

The Contractor acknowledges and agrees that the Services provided for herein will be provided to the CTRMA and may also be provided for the benefit of other toll authorities through

agreements between the CTRMA and the other entities. All terms related to the performance of the Services hereunder to and for the CTRMA shall apply equally to Services provided to other toll authorities, and the CTRMA shall have the right, without objection from the Contractor, to seek performance hereunder and enforce the terms of this Agreement on its own behalf and on behalf of any other entities receiving the Services provided for herein.

The Contractor shall be expected to operate independently from the CTRMA and without extensive oversight and direction. The Contractor represents and warrants that it shall commit the personnel and resources required to respond promptly and fully to the responsibilities and tasks assigned by the CTRMA throughout the term of the Contractor's performance of the Services described in this Agreement.

ARTICLE 2 **PROSECUTION OF WORK AND COMPENSATION**

A not to exceed amount for this Agreement will be established by the CTRMA Board of Directors in the CTRMA annual operating budget. In no event will the not to exceed amount for a given year be exceeded without prior approval by the CTRMA Board of Directors. No compensation shall be paid for work performed that is not authorized by the CTRMA Executive Director in a written Work Authorization, as described below. Authorization for Contractor to perform the Services, payment of compensation for Contractor's work, and other aspects of the mutual obligations concerning Contractor's work and payment therefore are as follows:

2.1 INSTALLATION SERVICES

a. Commencement of Work. The Contractor shall not proceed with any Installation Services until a Work Authorization has been issued pursuant to subsection 2.1.b. below.

b. Work Authorizations. Each activity, task, or project related to the Installation Services shall be performed pursuant to a separate Work Authorization, signed by the CTRMA and the Contractor. Work shall be performed in accordance with the scope, schedule, and budget set forth in said Work Authorization. The standard form of Work Authorization is attached hereto as Appendix "B" and made a part hereof. The standard form of Work Authorization may be modified during the term of this Agreement at the direction of the CTRMA or as agreed to by the Parties. No amendment of this Agreement is required if the standard form of Work Authorization is amended.

Upon written (including emailed) request from the CTRMA, the Contractor shall prepare a Work Authorization for a specific task or project, to be submitted for the CTRMA's approval. A proposed Work Authorization must be submitted within thirty (30) days of receipt of the written (or emailed) request. No work shall begin on the activity until the Work Authorization is approved by the CTRMA's Executive Director and is fully executed. The basis for payment on each Work Authorization will be stated in the Work Authorization as either (i) a lump sum, which may be paid in multiple milestone payments, or (ii) cost plus, using the ITS Equipment Prices shown in Appendix "C" and estimated hours calculated based on the labor rates shown in Appendix "E". In all cases a maximum "not-to-exceed" amount for the work will be identified in the Work

Authorization, and in no event will the maximum be exceeded without prior approval by the CTRMA Executive Director.

The assignment and authorization of work, if any, shall be at the sole discretion of the CTRMA.

c. Delays in Completing Installation Services. It is critical to the financial stability of the CTRMA and essential for the convenience of the traveling public that the performance of Installation Services is carried out in accordance with the schedules set forth in any Work Authorization. Damages for failure to meet a schedule deadline are difficult to estimate, and therefore shall result in liquidated damages being assessed by the CTRMA at a rate specified in the applicable Work Authorization, unless specific time extensions have been requested by the Contractor and approved by the CTRMA, at its sole discretion. The CTRMA reserves the right to deduct the amount of liquidated damages from any funds due the Contractor. If retained funds or other funds due the Contractor are not sufficient to cover the liquidated damages, the Contractor, or surety (as set forth in Article 7) shall promptly pay the amount due. Nothing herein shall preclude the delay in performance from being an event providing for notice and possible termination under Article 4. Without waiving the foregoing, if at any time during the term of this Agreement the Contractor cannot provide the requested Installation Services within the time required by the CTRMA or for any other reason, the CTRMA may, without waiving any other rights it may have under this Agreement, procure the Installation Services from any other source it deems capable of providing those Installation Services.

d. Adjustment of Installation Services Prices. The initial prices to be used for establishing the Installation Services in any Work Authorization are set forth in Appendix "C" and Appendix "E" and shall be adjusted annually commencing on the second anniversary of this Agreement to account for increases or decreases in the costs of labor and materials from the costs as of the Effective Date. Any increase or decrease in the annual adjustment shall not result in rates increasing or decreasing by more than 5% from the prior years' adjustment. Notwithstanding the foregoing, the prices for Installation Services in any Work Authorization in effect at the time of an adjustment will not be subject to such adjustment. Price adjustments subject to this subsection 2.1.d. shall be based on the following indices:

i. labor amounts shall be adjusted in accordance with the Consumer Price Index (CPI) for Urban Wage Earners and Clerical Installation Workers for the Austin, Texas metropolitan area ("all items") as published by the U.S. Department of Labor, Bureau of Labor Statistics.

ii. material amounts shall be adjusted in accordance with the Electrical Machinery and Equipment Index (WPU 117), as published by the U.S. Bureau of Labor Statistics.

2.2 MAINTENANCE SERVICES

a. Commencement of the Maintenance Services. The initiation of the Maintenance Services shall commence with the issuance of a Work Authorization describing the ITS facilities and equipment to be maintained. The Work Authorization for Maintenance Services

will be renewed on an annual basis in connection with the CTRMA Board of Directors' adoption of an annual budget for the Services.

b. Fees and Charges. The CTRMA shall pay a monthly fee (the "Monthly Fee") for the Maintenance Services to be performed using the Maintenance Services Unit Prices set forth in the Appendix "D".

c. Revisions to Scope of Maintenance Services. Any revision to the scope of the Maintenance Services assigned to the Contractor in accordance with this Agreement or an adjustment in the price for the Maintenance Services, shall be implemented pursuant to a Supplemental Work Authorization authorized by the CTRMA, which shall also include any changes to the Monthly Fee.

d. Delays in Completing Maintenance Services. It is critical to the financial stability of the CTRMA and essential for the convenience of the traveling public that the performance of Maintenance Services is carried out in accordance with the Service Level Agreements ("SLAs") set forth in Appendix "F". Damages for failure to meet a schedule deadline are difficult to estimate, and therefore shall result in liquidated damages being assessed by the CTRMA at a rate specified in the Appendix "F", unless specific time extensions have been requested by the Contractor and approved by the CTRMA, at its sole discretion. The CTRMA reserves the right to deduct the amount of liquidated damages from any funds due the Contractor. If retained funds or other funds due the Contractor are not sufficient to cover the liquidated damages, the Contractor, or surety (as set forth in Article 7) shall promptly pay the amount due. Nothing herein shall preclude the delay in performance from being an event providing for notice and possible termination under Article 4. Without waiving the foregoing, if at any time during the term of this Agreement the Contractor cannot provide the requested Maintenance Services within the time required by the CTRMA or for any other reason, the CTRMA may, without waiving any other rights it may have under this Agreement, procure the Maintenance Services from any other source it deems capable of providing those Maintenance Services.

e. Adjustment of Maintenance Services Prices. The Monthly Fee shall not be increased or decreased during the Initial Term except for adjustment as a result of adding or removing ITS facilities or equipment from the scope of work, resulting in an increase or decrease in fees. The initial prices to be used for establishing the Monthly Fee are set forth in Appendix "D" and shall be adjusted annually commencing on the second anniversary of this Agreement to account for increases or decreases in the costs of labor and materials from the costs as of the Effective Date. Any increase or decrease in the annual adjustment shall not result in rates increasing or decreasing by more than 5% from the prior years' adjustment. Price adjustments subject to this subsection 2.2.e. shall be based on the Electrical Machinery and Equipment Index (WPU 117), as published by the U.S. Bureau of Labor Statistics.

2.3 COMPENSATION, GENERALLY

a. EXPENSES. The compensation described above is anticipated by the CTRMA and the Contractor to be full and sufficient compensation and reimbursement for the performance of the Services. The Contractor shall not be entitled to reimbursement from the

CTRMA for out of pocket expenses incurred by the Contractor related to the performance of its duties under this Agreement.

b. **INVOICES AND RECORDS.** The Contractor shall submit a monthly invoice certifying the time sheets reflecting the number of hours worked by Contractor personnel and the costs associated with providing the Services under this Agreement during the previous month, and shall also present a reconciliation of monthly invoices and the Work Authorization (and related estimates) to which the work relates. Each invoice shall be in such detail as is required by the CTRMA, including a breakdown of Services provided pursuant to specified Work Authorizations and, if applicable, a report reflecting the progress on each SLA subject to the specified Work Authorization. The costs associated with work performed on any Work Authorization will be tracked and reported to the CTRMA separately from other work performed by the Contractor. The monthly invoice to the CTRMA will include a progress summary of the work performed the previous month on each ongoing Work Authorization.

Upon request of the CTRMA, the Contractor shall also submit certified time and expense records and copies of invoices that support the invoiced time and expense figures. In the event that the work performed under this Agreement is subject to federal or state reporting requirements, Contractor shall submit any supporting information required to comply with such reporting requirements not otherwise provided for under this Agreement.

c. **EFFECT OF PAYMENTS.** Payment shall be required thirty (30) days after receipt of an undisputed invoice. No payment by the CTRMA shall relieve the Contractor of its obligation to timely deliver the Services required under this Agreement. If after approving or paying for any Service, product or other deliverable, the CTRMA determines that said Service, product, or deliverable does not satisfy the requirements of this Agreement, the CTRMA may reject the same and, if the Contractor fails to correct, cure, or provide a plan acceptable to the CTRMA for cure within a reasonable period of time, but no later than thirty (30) days after receipt of written notice of the manner in which a Service, product, or deliverable does not satisfy the requirements of this Agreement, and at no additional cost to the CTRMA, the Contractor shall return any compensation received therefore. In addition to all other rights provided in this Agreement, the CTRMA shall have the right to set off any amounts owed by the Contractor pursuant to the terms of this Agreement upon providing the Contractor prior written notice thereof. Disputed amounts are to be resolved pursuant to the dispute resolution process as provided in Article 38 of this Agreement. If it is determined that the CTRMA has wrongfully withheld amounts from payment, the CTRMA shall promptly pay all withheld amounts.

Except to the extent amounts owed may be set off as provided above, the CTRMA shall make timely payments for all undisputed amounts. If any undisputed amounts remain outstanding for more than one hundred and eighty (180) days and the Contractor has provided documentation to substantiate its right to be paid for the amount in dispute, the Contractor retains the right to suspend performance under this Agreement (including but not limited to suspending CTRMA's license to Software) without any further obligation or liability. Contractor's right to suspend performance is subject to first providing a written notice to the CTRMA detailing the undisputed amounts which have been outstanding for more than one hundred and eighty (180). If the CTRMA fails to cure such outstanding undisputed amounts no later than thirty (30) days after receipt of the written notice, Contractor may suspend performance under this Agreement.

d. **TAXES.** The Contractor acknowledges that the CTRMA is a tax-exempt entity under Sections 151.309, et seq., of the Texas Tax Code.

ARTICLE 3 **TERM OF AGREEMENT**

It is understood and agreed that the initial term of this Agreement shall be a period of three (3) years, commencing on November 1, 2023, and concluding on October 31, 2026, (the “Initial Term”) subject to the earlier termination of this Agreement pursuant to Articles 4 or 5 below or further extension upon agreement of both parties. There shall be three (3) successive two (2) year renewal terms following the expiration of the Initial Term, each of which shall be subject to approval of the CTRMA Board of Directors.

If at any time during the term of this Agreement the Contractor cannot provide the requested Services within the time required by the CTRMA or for any other reason, the CTRMA may, without waiving any other rights it may have under this Agreement, procure the Services from any other source it deems capable of providing those Services.

ARTICLE 4 **TERMINATION FOR DEFAULT**

Time is of the essence with respect to the performance and completion of all the Services to be furnished by the Contractor pursuant to Work Authorizations issued and which specify an agreed-upon completion or delivery date. Without limiting the foregoing, the Contractor shall furnish all Services in such a manner and at such times as the CTRMA may require. Except as provided below, should the Contractor at any time (a) not carry out its obligations under this Agreement or (b) not be providing the Services to be rendered hereunder in an expeditious and efficient manner and in full compliance with this Agreement, or if the Contractor shall fail in any manner to discharge any other of its obligations under this Agreement, the CTRMA may, upon providing the Contractor with not less than thirty (30) days prior written notice and opportunity to cure (provided that in no event shall the cure period be more than thirty (30) days from receipt of the written notice unless a plan for a longer cure period is provided by Contractor and approved by the CTRMA in its sole discretion), terminate this Agreement. Notwithstanding the foregoing, the CTRMA may terminate this Agreement by providing not less than five (5) days prior written notice (an no opportunity to cure) in the event the Contractor fails to provide any bond, including the renewal of any bond, pursuant to the requirements under Article 7.

Any such termination under this Article 4 shall not constitute a waiver or release by the CTRMA of any claims for damages, claims for additional costs incurred by the CTRMA to complete and/or correct the work described in this Agreement, or any other claims or actions arising under this Agreement or available at law or equity which it may have against the Contractor for its failure to perform satisfactorily any obligation hereunder, nor shall such termination pursuant to this Article 4 or Article 5 below abrogate or in any way affect the indemnification obligations of the Contractor set forth in Article 17 hereof.

Contractor has provided the CTRMA with three (3) years of financial statements as part of its Proposal (as defined in Article 20), and has represented that it has experienced positive cash flow

during that three (3) year period. Contractor shall have a continuing obligation under this Agreement to notify the CTRMA of: (i) any material adverse change in its financial position or the occurrence of any event which may result in an adverse change (such as claims, litigation, etc.); (ii) the failure to maintain a positive cash flow for any fiscal year during the term of this Agreement; or (iii) any event of insolvency or the initiation of any bankruptcy proceeding or other action seeking protection from creditors or claimants during the term of this Agreement. The failure to provide required notification shall be an event of default for which the CTRMA may terminate this Agreement without the requirement for notice as set forth in the preceding paragraph.

If the CTRMA terminates this Agreement as provided either in this Article 4 or Article 5, no fees of any type, other than fees due and payable as of the termination date pursuant to Article 2 hereof for work performed and acceptable to the CTRMA, shall thereafter be paid to or collected by the Contractor, and the CTRMA shall have a right to offset or otherwise recover any damages incurred by reason of the Contractor's breach hereof, together with the right to offset amounts owed to the Contractor pursuant to Article 7 hereof. In determining the amount of any payments owed to the Contractor, the value of the work performed by the Contractor prior to termination shall be no greater than the value that would result by compensating the Contractor in accordance with Article 2 hereof for all Services performed and expenses reimbursable in accordance with this Agreement.

ARTICLE 5 **OPTIONAL TERMINATION**

In addition to the process for termination described above, this Agreement may also be terminated as follows:

a. **GENERALLY.** The CTRMA has the right to terminate this Agreement at its reasonable option, at any time with or without cause, by providing sixty (60) days written notice of such intention to terminate pursuant to this subsection 5.a. hereof and by stating in said notice the optional termination date. Upon such optional termination, the CTRMA shall enter into a settlement with the Contractor upon an equitable basis as determined by the CTRMA, which shall fix the value of the work performed by the Contractor prior to the optional termination date. In determining the value of the work performed, the CTRMA in all events shall compensate the Contractor for any reasonable costs or expenses actually incurred and which are attributable to the exercise of the CTRMA's optional termination, on an equitable basis as determined by the CTRMA as noted above, provided, however, that no consideration will be given to anticipated profit which the Contractor might possibly have made on the uncompleted portion of the Services.

b. **NO FURTHER RIGHTS, ETC.** Termination of this Agreement and payment of an amount in settlement as described in this Article 5 shall extinguish all rights, duties, obligations, and liabilities of the CTRMA and the Contractor under this Agreement (except those which are designated as surviving termination, including without limitation the indemnification obligations of Contractor set forth in Article 17), and this Agreement shall be of no further force and effect, provided, however, such termination shall not act to release the Contractor from liability for any previous default, known or unknown, either under this Agreement or under any standard of conduct set by common law or statute.

c. **NO FURTHER COMPENSATION.** If the CTRMA shall terminate this Agreement as provided in this Article 5, no fees of any type, other than fees due and payable as of the optional termination date, shall thereafter be paid to the Contractor, provided that the CTRMA shall not waive any right to damages incurred by reason of the Contractor's breach thereof. The Contractor shall not receive any compensation for Services performed by the Contractor after the optional termination date, and any such Services performed shall be at the sole risk and expense of the Contractor.

ARTICLE 6 **TERMINATION, GENERALLY**

The CTRMA's rights and options to terminate this Agreement, as provided in any provision of this Agreement, shall be in addition to, and not in lieu of, any and all rights, actions, options, and privileges otherwise available under law or equity to the CTRMA by virtue of this Agreement or otherwise. Failure of the CTRMA to exercise any of its said rights, actions, options, and privileges to terminate this Agreement as provided in any provision of this Agreement or otherwise shall not be deemed a waiver of any of said rights, actions, options, or privileges or of any rights, actions, options, or privileges otherwise available under law or equity with respect to any continuing or subsequent breaches of this Agreement or of any other standard of conduct set by common law or statute.

ARTICLE 7 **SERVICE LEVEL AGREEMENTS AND PERFORMANCE GUARANTY**

a. **SLA NONCOMPLIANCE.** Timely and accurate performance of the Services is critically important to the CTRMA. Contractor has represented that it will perform the Services in a timely and accurate manner, and Contractor acknowledges that the failure to do so will cause material harm to the CTRMA. Without waiving any other rights provided for in this Agreement, the Parties have identified certain SLAs intended to assure that critical aspects of the Services are provided in a timely and reliable manner, and that if they are not that there are consequences for Contractor's failure to perform. The SLAs and a table showing financial consequences for failure to adhere to those SLAs is set for in Appendix "F". In the event Contractor fails to adhere to the standards associated with one or more SLAs, the CTRMA shall notify Contractor of such event of noncompliance and shall be authorized to withhold, or offset, the penalty amount indicated in Appendix "F" from amounts owed to the Contractor for Services performed. Nothing in this Article 7 shall preclude the CTRMA from asserting any other remedies related to the failure to perform in accordance with the SLAs, including without limitation termination pursuant to Article 5.

b. **LOSS OF REVENUE.** Notwithstanding any other provision in this Agreement and whether or not the performance of the Services is in conformance with the requirements specified herein (including the appendices), in the event the CTRMA incurs a loss of revenue due to any action or inaction of the Contractor (or any individual or entity working on Contractor's behalf), the Contractor shall be obligated to make payment to the CTRMA of all lost revenue and other direct damages associated with the loss, including payments made to the CTRMA's third-party vendors. In the event that the CTRMA is unable to determine the amount of lost revenue because data is lost or otherwise unavailable, the Parties agree that lost revenue shall be based on historical

figures (e.g., traffic, payments) maintained by the CTRMA. The CTRMA may offset lost revenue and associated damages by reducing the amount of the subsequent Monthly Fee.

c. **NON-REVENUE DAMAGES.** In the event the CTRMA incurs damages due to any action or inaction of the Contractor (or any individual or entity working on Contractor's behalf) for its failure to perform satisfactorily any obligation under this Agreement, and which are not subject to subsection 7.b., then the Contractor shall be obligated to make payment to the CTRMA for any costs incurred by the CTRMA to complete and/or correct the work for which the Contractor failed to perform. The CTRMA may offset costs incurred by the CTRMA by reducing the amount of the subsequent Monthly Fee. The maximum amount of payments Contractor is required to pay under this subsection 7.c. shall not exceed \$10,000,000, with such amount being exclusive of any proceeds paid under Contractor's insurance policies or by the surety on any bonds required by this Agreement.

d. **PAYMENT AND PERFORMANCE BONDS.** The Contractor shall furnish the performance bonds and a payment bonds described in this subsection 7.d (collectively, the "Bonds") in the exact form set forth in the applicable appendix to this Agreement. The Bonds do not serve as the full extent of the Contractor's liabilities under this Agreement but are intended to secure the Contractor's obligations in providing the Services as well as to ensure adequate compensation for loss of revenue incurred by the CTRMA under subsection 7.b.

i. **Surety Financial Requirements.** The Bonds shall be issued by a surety with an A.M. Best and Company rating level of A-minus (A-) or better, Class VIII or better, or as otherwise approved in writing by the CTRMA, in its sole discretion. If any bond previously provided becomes ineffective, or if the surety that provided the bond no longer meets the requirements hereof, the Contractor shall provide a replacement bond in the same form issued by a surety meeting the foregoing requirements, or other assurance satisfactory to the CTRMA in its sole discretion.

ii. **Installation Performance and Payment Bonds.** Upon issuance of each Work Authorization under Article 2, subsection 2.1, the Contractor shall provide, and continuously maintain in place for the benefit of the CTRMA, a performance bond in the form of Appendix "I-1" (a "Installation Performance Bond") and a payment bond in the form of Appendix "I-2" (a "Installation Payment Bond") for the Installation Services covered by each applicable Work Authorization. The Installation Performance Bond and Installation Payment Bond shall each be in an amount of 100% of the relevant Work Authorization cost. If a price is increased in connection with a Work Authorization, the CTRMA may, in its sole discretion require a corresponding proportionate increase in the amount of the applicable Installation Performance Bond and Installation Payment Bond.

The Contractor's obligation to maintain and provide the Installation Performance Bond and Installation Payment Bond with respect to the Installation Services shall continue throughout the term of the applicable Work Authorization, but the CTRMA will accept the Installation Performance Bond and Installation Payment Bond with a stated term of one (1) year with a statement set forth in the applicable bond that it shall be renewable annually in accordance with the surety's customary renewal practices, provided further that it shall be an event of default if a

bond is not renewed and there is no replacement bond provided prior to the expiration of the bond. If such an event of default occurs, the CTRMA may terminate this Agreement by providing five (5) days written notice to Contractor. The CTRMA will release any individual Installation Performance Bond relating solely to a Work Authorization upon the later of (1) expiration of the applicable warranty period related to such Work Authorization, provided that no outstanding claims are then pending or threatened against the Contractor hereunder, or (2) satisfaction of the conditions required for final acceptance of the Installation Services of the applicable Work Authorization. The CTRMA will release any individual Installation Payment Bond relating solely to a Work Authorization (1) upon receipt of (i) evidence satisfactory to the CTRMA that all persons eligible to file a claim against the bond have been fully paid and (ii) unconditional releases of liens and stop notices from all subcontractors who filed preliminary notice of a claim against the bond, (2) upon expiration of the statutory period for subcontractors to file a claim against the bond if no claims have been filed, or (3) upon satisfaction of the conditions required for final acceptance of the Installation Services of the applicable Work Authorization.

iii. Maintenance Performance and Payment Bonds. Upon the issuance of the Work Authorization under Article 2, subsection 2.2., the Contractor shall furnish the CTRMA with (a) a Maintenance Performance Bond in the form of Appendix "J-1" (with such modifications as the CTRMA approves in writing, in its sole discretion) (the "Maintenance Performance Bond"), and (b) a Maintenance Payment Bond in the form of Appendix "J-2" (with such modifications as the CTRMA approves in writing, in its sole discretion) (the "Maintenance Payment Bond").

The Maintenance Performance Bond and Maintenance Payment Bond shall each be in an amount equal to (a) 100% of the aggregate two-year cost for the Maintenance Services for the Work Authorization under Article 2, subsection 2.2.a. and any Supplemental Work Authorizations under Article 2, subsection 2.2.c. If the price of the Maintenance Services is increased in connection with a Supplemental Work Authorizations under Article 2, subsection 2.2.c., the Contractor shall provide a corresponding proportionate increase in the amount of the Maintenance Performance Bond and Maintenance Payment Bond, provided that it shall be an event of default if the bonds reflecting the increased amounts are not provided within ten (10) business days of the date of the Supplemental Work Authorization providing for the increased amount.

e. The Contractor's obligation to maintain and provide the current Maintenance Performance Bond and Maintenance Payment Bond with respect to the Maintenance Services shall continue throughout the term of this Agreement, but the CTRMA will accept the Maintenance Performance Bond and Maintenance Payment Bond with a stated term of at least two (2) years with a statement set forth in the applicable bond that it shall be renewable annually in accordance with the surety's customary renewal practices. Provided that the Contractor has paid the CTRMA any applicable damages, compensation for revenue losses, and any other amounts that are payable to the CTRMA under this Agreement, the Maintenance Performance Bond shall be released upon expiration of the term of this Agreement and after the satisfaction of all conditions required for completion of the Maintenance Services. Upon expiration of the term of this Agreement, the CTRMA will release the Maintenance Payment Bond (i) upon receipt of (A) evidence satisfactory to the CTRMA that all persons eligible to file a claim against the bond have been fully paid and (B) unconditional releases of liens and stop notices from all subcontractors

who filed preliminary notice of a claim against the bond, or (ii) upon expiration of the statutory period for subcontractors to file a claim against the bond if no claims have been filed.

ARTICLE 8

SUSPENSION OR MODIFICATION OF SERVICES; DELAYS AND DAMAGES

In addition to the foregoing rights and options to terminate this Agreement, the CTRMA may elect to suspend any portion of the Services of the Contractor hereunder, but not terminate this Agreement, by providing the Contractor with prior written notice to that effect. Thereafter, the suspended Services may be reinstated and resumed in full force and effect upon receipt from the CTRMA of written notice requesting same.

Similarly, the CTRMA may expand, cancel (in whole or part), or otherwise modify any portion of the Services previously assigned to the Contractor in accordance with this Agreement. Such modification may include, but is not limited to, technological advances resulting in the development of equipment, software or any other aspect of the Services that would benefit the CTRMA and is not contemplated under this Agreement. In the event the Services are modified, the Parties shall agree to and execute a Work Authorization and Contractor's compensation shall be adjusted (up or down) based on the rates set forth in Appendices "D" or "E" as applicable. Without limiting the foregoing, the Contractor agrees that no claims for damages or other compensation shall be made by the Contractor for any delays, hindrances or modifications occurring during the progress of any portion of the Services specified in this Agreement as a result of any suspension or modifications occurring during the progress of any portion of the Services specified in this Agreement. Such delays or hindrances, if any, shall be provided for by an extension of time for such reasonable periods as the CTRMA may decide. It is acknowledged, however, that permitting the Contractor to proceed to complete any Services or any part of them after the originally specified date for completion, or after the date to which the time for completion may have been extended, shall in no way operate as a waiver on the part of the CTRMA or any of its rights herein.

ARTICLE 9

PERSONNEL, EQUIPMENT AND MATERIAL, GENERALLY

Contractor shall provide personnel and equipment as follows:

a. **ADEQUATE PERSONNEL, ETC.** The Contractor shall furnish and maintain, at its own expense, adequate and sufficient personnel (drawn from its own employees or from approved subcontractors) and equipment, in the reasonable opinion of the CTRMA, to perform the Services with due and reasonable diligence customary of a firm providing similar services and enjoying a favorable national reputation, and in all events without delays attributable to the Contractor which have a reasonable likelihood of adversely affecting the progress of others involved with one or more of the Projects. All persons, whether employees of the Contractor or of an approved subcontractor, providing the Services shall be fully licensed to the extent required by their professional discipline associations' codes or otherwise by law.

b. **REMOVAL OF PERSONNEL.** All persons providing the Services, whether employees of the Contractor or of an approved subcontractor, shall have such knowledge and experience as

will enable them, in the Contractor's reasonable belief, to perform the duties assigned to them. Any such person who, as determined by the CTRMA in its sole discretion, is incompetent or by his/her conduct becomes detrimental to the provision of the Services shall, upon request of the CTRMA, immediately be removed from the Services. The Contractor shall furnish the CTRMA with a fully qualified candidate for the removed person within thirty (30) days thereafter, provided, however, said candidate shall not begin work under this Agreement unless and until approved by the CTRMA.

c. **CONTRACTOR FURNISHES EQUIPMENT, ETC.** Except as otherwise specified or agreed to by the CTRMA, the Contractor shall furnish all equipment, transportation, supplies, and materials required for its performance of Services under this Agreement.

ARTICLE 10 **KEY PERSONNEL**

The Contractor acknowledges and agrees that the individual(s) identified on Appendix "G" attached hereto and incorporated herein are key and integral to the satisfactory performance of the Contractor under this Agreement. Throughout the term of this Agreement, the Contractor agrees that the identified individual(s) will remain in charge of the performance of the Services and they shall devote substantial and sufficient time and attention thereto. The death or disability of any such individual, his/her disassociation from the Contractor or the approved subcontractor, or his/her failure or inability to devote sufficient time and attention to the Services shall require the Contractor promptly to replace said individual with a person suitably qualified and otherwise acceptable to the CTRMA. If such individual has not been replaced by an individual approved by the CTRMA within thirty (30) days of the event requiring replacement, Contractor acknowledges that the CTRMA will suffer significant and substantial additional losses due to the unavailability of an approved individual and that it is impracticable and extremely difficult to ascertain and determine the actual losses which would accrue to the CTRMA in such event. Therefore, for each day that an individual identified on Appendix "G" is not filled by an approved individual, the CTRMA may require that the Contractor pay a daily liquidated amount with such amount calculated pursuant to the formula shown in Appendix "G".

ARTICLE 11 **BUSINESS OPPORTUNITY PROGRAM AND POLICY COMPLIANCE**

Contractor acknowledges that the CTRMA has a Business Opportunity Program and Policy ("BOPP") with which it requires contractors to comply in connection with Disadvantaged Business Enterprises. To the extent the Contractor utilizes third parties to provide the Services hereunder, Contractor agrees to comply with the BOPP and observe the guidelines set forth therein. Contractor shall provide annual reporting to the CTRMA (beginning one (1) year from the Effective Date) regarding its utilization of disadvantaged business enterprises ("DBEs") and the manner in which such utilization complies with, or deviates from, Contractor's commitment to DBE utilization as reflected in its response to the RFP attached as Appendix "H".

ARTICLE 12
PLANNING AND PERFORMANCE REVIEWS; INSPECTIONS

As directed by the CTRMA, key personnel shall meet with the CTRMA's Executive Director and/or his designee(s) upon request to: (a) assess the Contractor's performance of the Services; and (b) plan staffing levels to be provided by the Contractor to the CTRMA for the upcoming calendar quarter. The Contractor shall permit inspections of its Services and work by the CTRMA or its designated representative, when requested by the CTRMA. Nothing contained in this Agreement shall prevent the CTRMA from scheduling such other planning and performance reviews with the Contractor or inspections as the CTRMA determines necessary.

ARTICLE 13
OWNERSHIP OF REPORTS

Ownership of reports and related materials prepared by Contractor (or any subcontractor) at the direction of the CTRMA shall be as follows:

a. **GENERALLY.** Excluding Contractor's ownership rights as provided in Article 13.d., all of the documents, reports, plans, computer records, software maintenance records, discs and tapes, proposals, sketches, diagrams, charts, calculations, correspondence, memoranda, opinions, testing reports, photographs, drawings, analyses and other data and materials, and any part thereof, created, compiled or to be compiled by or on behalf of the Contractor solely under this Agreement ("work product"), including all information prepared for or posted on the CTRMA's website and together with all materials and data furnished to it by the CTRMA, shall at all times be and remain the property of the CTRMA and, for a period of four (4) years from completion of the Services or such period as is required by Texas law, whichever is longer, if at any time demand be made by the CTRMA for any of the above materials, records, and documents, whether after termination of this Agreement or otherwise, such shall be turned over to the CTRMA without delay. The CTRMA hereby grants the Contractor a revocable license to retain and utilize the foregoing materials, said license to terminate and expire upon the earlier to occur of (a) the completion of Services described in this Agreement or (b) the termination of this Agreement, at which time the Contractor shall deliver to the CTRMA all such materials and documents. If the Contractor or a subcontractor desires later to use any of the data generated or obtained by it in connection with the Projects or any other portion of the work product resulting from the Services, it shall secure the prior written approval of the CTRMA. Notwithstanding anything contained herein to the contrary, the Contractor shall have the right to retain a copy of the above materials, records, and documents for its archives.

b. **SEPARATE ASSIGNMENT.** If for any reason the agreement of the CTRMA and the Contractor set forth in subsection 13.a. above regarding the ownership of work product and other materials is determined to be unenforceable, either in whole or in part, the Contractor hereby assigns and agrees to assign to the CTRMA all right, title, and interest that Contractor may have or at any time acquire in said work product and other materials which are prepared for this Agreement, without royalty, fee or other consideration of any sort, and without regard to whether this Agreement has terminated or remains in force. The CTRMA hereby acknowledges, however, that all documents and other work product provided by the Contractor to the CTRMA and resulting from the Services performed under this Agreement are intended by the Contractor solely for the

use for which they were originally prepared. Notwithstanding anything contained herein to the contrary, the Contractor shall have no liability for the use by the CTRMA of any work product generated by the Contractor under this Agreement on any project other than for the specific purpose and Project for which the work product was prepared. Any other reuse of such work product without the prior written consent of the Contractor shall be at the sole risk of the CTRMA.

c. **DEVELOPMENT OF CONTRACTOR WORK PRODUCT.** The CTRMA acknowledges that the Contractor's work product will be developed using data that is available at the time of the execution of a given Work Authorization, and will not constitute any guarantee or other assurance of future events. The Contractor will prepare work product using practices that are standard procedures in the industry.

d. **OWNERSHIP OF MATERIALS, SOFTWARE AND LICENSES.** The CTRMA acknowledges and agrees that, the Contractor and/or its subcontractors or licensors of are the exclusive owners all copyrights, trade secret rights and related intellectual property rights (such rights together referred to herein as "Intellectual Property Rights") in all software and accompanying documentation developed, produced or implemented in connection with this Agreement by the Contractor, its officers, employees, subcontractors or agents (the "Software"). Except as expressly stated herein, this Agreement does not grant the CTRMA any rights in or to such Intellectual Property Rights. The Contractor reserves the right to grant licenses to use such Software to any other party or parties, provided that any such licenses do not affect the provision of any of the Services to the CTRMA pursuant to this Agreement.

i. The provisions of this subsection 13.d. shall be without prejudice to, and shall not interfere with the CTRMA's ownership of reports as provided for under subsections 13.a to 13.c. of this Agreement.

ii. The Contractor reserves all rights in Software and all Intellectual Property associated therewith that have not been expressly granted herein.

iii. For the duration of this Agreement, the Contractor hereby grants to the CTRMA a nonexclusive, non-sublicensable, non-transferable license to use the Software for such purposes and to the extent necessary to enable the CTRMA to receive the Contractor's Services under this Agreement. Notwithstanding anything to the contrary in this Agreement, the license referred to in this sub-clause (iii) shall not survive termination or expiration of this Agreement (except as required to facilitate succession to a new provider). Provided however that the license referred to in this sub-clause (iii) shall be extended for the limited purposes and term that may be necessary to give effect to any post termination or post expiration transition related obligations expressly undertaken by the Contractor under this Agreement, such that Contractor's Services shall remain continuous and uninterrupted for the duration of any post termination or post expiration transition period under this Agreement, with Contractor providing the CTRMA with all permissions and licenses necessary to enable the CTRMA to receive Contractor's Services throughout any such transition period, including permissions and licenses necessary for use of any third-party software implemented by Contractor under this Agreement.

iv. The CTRMA shall have no right to access or use the source code of the Software. Notwithstanding the foregoing, with respect to any contract between the Contractor and

any cloud service hosting provider related to the provision of the Services, the Contractor shall grant the CTRMA, upon termination or expiration of this Agreement, all of the rights and privileges of such contract, including but not limited to the CTRMA's right to secure the cloud service hosting services directly from the cloud service hosting provider.

v. The CTRMA shall not attempt to make any part of the Software or any accompanying documentation supplied by the Contractor along with the Software, available to any third party, or otherwise allow access to the same to any third party except as required by law.

vi. The CTRMA shall not attempt to reverse compile, decompile, disassemble or reverse engineer the Software, nor shall it amalgamate, amend, incorporate, modify, reproduce, translate or otherwise alter the same into or with any other software or use the same in conjunction with any third party's software.

vii. For purposes of this Agreement, the term Software shall mean any software used by the Contractor or any subcontractor of the Contractor to provide the Services to the CTRMA, including any software owned or provided by the Contractor or by a sub-consultant of the Contractor.

ARTICLE 14 **SUBLETTING OF WORK**

The Contractor shall not sublet, assign, or transfer any part of the work or obligations included in this Agreement without the prior written approval of the CTRMA. Responsibility for sublet, assigned or transferred work shall remain in all instances with the Contractor.

ARTICLE 15 **APPEARANCE AS WITNESS AND ATTENDANCE AT MEETINGS**

Contractor shall cooperate with the CTRMA and requests for attendance at meetings and in various types of proceedings as follows:

a. **WITNESS.** If requested by the CTRMA, the Contractor shall prepare such exhibits as may be requested for all hearings and trials related to any of the Services provided under this Agreement.

b. **MEETINGS.** At the request of the CTRMA, the Contractor shall provide appropriate personnel for conferences at its offices, or attend meetings and conferences at (a) the various offices of the CTRMA, (b) the offices of the CTRMA's legal counsel, bond counsel, and/or financial advisors, or (c) any reasonably convenient location.

ARTICLE 16 **COMPLIANCE WITH LAWS AND AUTHORITY POLICIES; PROTECTION OF DATA AND INFORMATION**

The Contractor shall comply with all federal, state, and local laws, statutes, ordinances, rules, regulations, codes and with the orders, judgements, and decrees of any courts or administrative bodies or tribunals in any matter affecting the performance under this Agreement,

including, without limitation, workers' compensation laws, antidiscrimination laws, environmental laws, minimum and maximum salary and wage statutes and regulations, health and safety codes, licensing laws and regulations, the CTRMA's enabling legislation (Chapter 370 of the Texas Transportation Code), other applicable portions of the Texas Transportation Code, and all amendments and modifications to any of the foregoing, if any. The Contractor shall also comply with the CTRMA's policies and procedures provided to the Contractor or which are generally available to the public related to operational and administrative matters, such as, but not limited to, security of and access to the CTRMA information and facilities. When requested, the Contractor shall furnish the CTRMA with satisfactory proof of compliance with said laws, statutes, ordinances, rules, regulations, codes, orders, judgements, and decrees above specified.

As part of their operations, the CTRMA, and other toll authorities to whom services may be provided collect and maintain information about individuals (including toll customers, vehicle owners, and employees) that may include data such as a license-plate number, geolocation or travel data, employment-related information, or login and password credentials (all such data pertaining to individuals, whether or not specifically listed, being "Personal Information"). As part of its performance of the Services, Contractor may have access to, handle, or receive Personal Information or other confidential or proprietary materials, information, or data maintained by or concerning the CTRMA, and other toll authorities to whom services may be provided (collectively with Personal Information, "RMA Information"). Contractor therefore agrees that:

a. Contractor is responsible for the security of RMA Information that it receives or accesses in performing Services, and Contractor shall at all times maintain appropriate information-security measures with respect to RMA Information in a manner consistent with applicable law.

b. Contractor must implement and maintain current and appropriate administrative, technical, and physical safeguards with respect to RMA Information in its possession, custody, or control, or to which it has access, to protect against unauthorized access or use of such RMA Information. At a minimum, such safeguards shall be consistent with generally-recognized best practices for information security in the handling of similar types of data. Without limiting the foregoing, Contractor must appropriately and effectively encrypt RMA Information (i) transmitted over the Internet, other public networks, or wireless networks, and (ii) stored on laptops, tablets, or any other removable or portable media or devices.

c. Contractor must identify to the CTRMA all subcontractors, consultants, and other persons who may have access to RMA Information in connection with the Services. Contractor must restrict the RMA Information to which a given employee or approved subcontractor has access to only that RMA Information which such employee or approved subcontractor needs to access in the course of such employee's or approved subcontractor's duties and responsibilities in connection with the Services.

d. Before granting access to RMA Information, Contractor must ensure that its employees and each approved subcontractor agrees to abide by these information security measures (or other applicable measures that are at least as protective of RMA Information).

e. Absent the CTRMA's advance written permission, RMA Information must not be stored, accessed, or processed at any location outside of the United States.

f. Contractor may use RMA Information only for performing the Services, and Contractor must ensure that its employees and approved subcontractor are restricted from any use of RMA Information other than for such purpose.

g. Except to the extent otherwise expressly permitted, Contractor may not disclose RMA Information except as required by law or a governmental authority having jurisdiction over Contractor. In the event of such required disclosure, Contractor must notify the CTRMA in advance (if legally permissible to do so) and reasonably cooperate with any decision by the CTRMA to seek to condition, minimize the extent of, or oppose such disclosure.

h. Contractor will immediately notify the CTRMA if Contractor discovers any actual or reasonably suspected breach of security or unauthorized use of RMA Information (i) in the possession, custody, or control of Contractor, its employees, or its subcontractors and/or (ii) effectuated using access permissions or credentials extended to an employee or subcontractor of Contractor (either of occurrences (i) or (ii) being referred to as a "Security Incident"). In no event shall Contractor's notification to the CTRMA be later than three (3) days after Contractor discovers the Security Incident; provided, however, that more immediate notification shall be given as the circumstances warrant or if more immediate notification is required by law. Contractor must provide all necessary and reasonable cooperation with respect to the investigation of such Security Incident, including the exchange of pertinent details (such as log files). In addition, Contractor must promptly undertake appropriate remediation measures and inform the CTRMA regarding the same.

i. Subject to requirements of data security or privacy laws, the CTRMA, in its sole discretion, will determine whether, and when to provide notice of a Security Incident to (a) any individuals whose personal information has been actually or potentially compromised; (b) any governmental authority; and/or (c) any other entity, including, but not limited to, consumer credit reporting agencies or the media. All notices must be approved by the CTRMA before they are distributed. Contractor must reimburse the CTRMA for costs or expenses the CTRMA incurs in connection with such notices (including the provision of credit monitoring or other identity protection services, to the extent the provision of such services is legally required or customary for similar data security incidents). Furthermore, and in addition to any other indemnification requirements under this Agreement, Contractor shall indemnify and hold the CTRMA harmless from all claims, costs, expenses, and damages (including reasonable attorneys' fees) that the CTRMA incurs in connection with any regulatory action or third-party claim arising from a Security Incident.

j. Contractor must cooperate and permit the CTRMA (and any governmental authorities with jurisdiction in connection with an audit requested by the CTRMA) reasonable access for on-site review of Contractor's data security systems and procedures to verify Contractor's compliance with its obligations under this Addendum.

k. Contractor must cooperate and permit the CTRMA's back office service provider reasonable access to all RMA Information in Contractor's possession, custody, or control

(including RMA Information in the possession, custody, or control of any of Contractor's subcontractors or consultants) in connection with any PCI DSS compliance audits.

ARTICLE 17
AUTHORITY INDEMNIFIED

THE CONTRACTOR SHALL INDEMNIFY AND SAVE HARMLESS THE CTRMA AND ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, AND CONTRACTORS FROM ANY CLAIMS, COSTS OR LIABILITIES OF ANY TYPE OR NATURE AND BY OR TO ANY PERSONS WHOMSOEVER, ARISING FROM THE CONTRACTOR'S ACTS, ERRORS OR OMISSIONS, OR THE ACTS, ERRORS OR OMISSIONS OF CONTRACTORS AGENTS, EMPLOYEES, SUBCONSULTANTS, OR OTHERS WORKING FOR OR ON BEHALF OF CONTRACTOR, WITH RESPECT TO PERFORMANCE OF THE WORK TO BE ACCOMPLISHED UNDER THIS AGREEMENT, WHETHER SUCH CLAIM OR LIABILITY IS BASED IN CONTRACT, TORT OR STRICT LIABILITY. IN SUCH EVENT, THE CONTRACTOR SHALL ALSO INDEMNIFY AND SAVE HARMLESS THE CTRMA, ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, AND CONTRACTORS (COLLECTIVELY THE "INDEMNIFIED PARTIES") FROM ANY AND ALL EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, INCURRED BY THE CTRMA OR ANY OF THE INDEMNIFIED PARTIES IN LITIGATING OR OTHERWISE RESISTING SAID CLAIMS, COSTS OR LIABILITIES. IN THE EVENT THE CTRMA, ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, OR CONTRACTORS IS/ARE FOUND TO BE PARTIALLY AT FAULT, THE CONTRACTOR SHALL, NEVERTHELESS, INDEMNIFY THE CTRMA OR ANY OF THE INDEMNIFIED PARTIES FROM AND AGAINST THE PERCENTAGE OF FAULT ATTRIBUTABLE TO THE CONTRACTOR, ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUB CONSULTANTS, AND CONTRACTORS OR TO THEIR CONDUCT.

ARTICLE 18
CONFLICTS OF INTEREST

The Contractor represents and warrants to the CTRMA, as of the effective date of this Agreement and throughout the term hereof, that it, its employees and subcontractors (a) have no financial or other beneficial interest in any contractor, engineer, product or service evaluated or recommended by the Contractor, except as expressly disclosed in writing to the CTRMA, (b) shall discharge their responsibilities under this Agreement professionally, impartially and independently, and (c) are under no contractual or other restriction or obligation, the compliance with which is inconsistent with the execution of this Agreement or the performance of their respective obligations hereunder. In the event that a firm (individually or as a member of a consortium) submits a proposal to work for the CTRMA, the Contractor shall comply with the CTRMA's conflict of interest policies and shall make disclosures as if it were one of the key personnel designated under such policies.

ARTICLE 19 INSURANCE

Prior to beginning the Services designated in this Agreement, the Contractor shall obtain and furnish certificates to the CTRMA for the following minimum amounts of insurance:

a. **WORKERS' COMPENSATION INSURANCE.** In accordance with the laws of the State of Texas covering all of Contractor's employees and employer's liability coverage with a limit of not less than \$1,000,000. A "Waiver of Subrogation" in favor of the CTRMA shall be provided.

b. **COMMERCIAL GENERAL LIABILITY INSURANCE.** On an "occurrence basis" with limit a limit of not less than \$1,000,000 combined single limit per occurrence for bodily injury, including those resulting in death; and property damage on an "occurrence basis" with an aggregate limit of not less than \$2,000,000. A "Waiver of Subrogation" in favor of the CTRMA shall be provided.

c. **BUSINESS AUTOMOBILE LIABILITY INSURANCE.** Applying to owned, non-owned, and hired automobiles in an amount not less than \$1,000,000 for bodily injury, including death, to anyone person, and for property damage on account of anyone occurrence. The policy shall insure any vehicle used in connection with the Contractor's obligations under this Agreement. A "Waiver of Subrogation" in favor of the CTRMA shall be provided.

d. **VALUABLE PAPERS INSURANCE.** With limits not less than \$500,000 to cover the full restoration of any records, information, logs, reports, diaries, or other similar data or materials of Contractor relating to the Services provided under this Agreement in the event of their loss or destruction, until such time as the work has been delivered to the CTRMA or otherwise completed.

e. **PROFESSIONAL/CYBERSECURITY INSURANCE.** Professional errors and omissions liability insurance, including liability for financial loss and/or business interruption suffered by the CTRMA, due to error, omission, negligence of employees and machine malfunction in connection with all Services provided by Contractor, in an amount of at least \$3,000,000;

Technology cyber liability insurance, including liability for financial loss and/or business interruption suffered by the CTRMA, due to cyber liability/network security/privacy coverage arising from errors, omission, negligence of employees and hardware malfunction, or causing electronic data to be inaccessible, computer viruses, denial of service, loss of service, network risks (such as data breaches, unauthorized access or use, identity theft, invasion of privacy, damage/loss/theft of data, degradation, downtime, etc.) in connection with all Services provided by Contractor, in an amount of at least three million dollars (\$3,000,000), and which has no exclusion or restriction for encrypted or unencrypted portable devices.

f. **EXCESS UMBRELLA LIABILITY.** With minimum limits of \$6,000,000 per claim and in the aggregate, annually, as applicable excess of the underlying policies required at a. - c. above. The Umbrella Policy shall contain the provision that it will continue in force as an underlying insurance in the event of exhaustion of underlying aggregate policy limits.

g. **EMPLOYEE DISHONESTY INSURANCE.** Coverage for employee dishonesty, loss of money and other property belonging to the CTRMA resulting directly from a fraudulent or

dishonest act by an agent or employee of the Contractor while performing the Services, with limits of not less than \$3,000,000 per claim.

h. **GENERAL FOR ALL INSURANCE.** The Contractor shall promptly, upon execution of this Agreement, furnish certificates of insurance to the CTRMA indicating compliance with the above requirements. Certificates shall indicate the name of the insured, the name of the insurance company, the name of the agency/agent, the policy number, the term of coverage, and the limits of coverage.

All policies are to be written through companies (a) registered to do business in the State of Texas; (b) rated: (i), with respect to the companies providing the insurance under subsections 19.a. through e. and 19.g., above, by A. M. Best Company as “A-X” or better (or the equivalent rating by another nationally recognized rating service) and (ii) with respect to the company providing the insurance under subsection 19.f., a rating by A. M. Best Company or similar rating service satisfactory to the CTRMA and/or its insurance consultant; and (c) otherwise acceptable to the CTRMA.

All policies are to be written through companies registered to do business in the State of Texas. Such insurance shall be maintained in full force and effect during the life of this Agreement or for a longer term as may be otherwise provided for hereunder. Insurance furnished under subsections 19.b., c., d., e. f, and g. above, shall name the CTRMA as additional insureds and shall protect the CTRMA, the Contractor, their officers, employees, directors, agents, and representatives from claims for damages for bodily injury and death and for damages to property arising in any manner from the negligent or willful wrongful acts or failures to act by the Contractor, its officers, employees, directors, agents, and representatives in the performance of the Services rendered under this Agreement. Applicable Certificates shall also indicate that the contractual liability assumed in Article 17, above, is included.

The insurance carrier shall include in each of the insurance policies required under subsections 19.a., b., c., d., e., f, and g. the following statement: “This policy will not be canceled or non-renewed during the period of coverage without at least thirty (30) days prior written notice addressed to the Central Texas Regional Mobility Authority, 3300 N. IH 35, Suite 300, Austin, TX 78705, Attention: Executive Director.”

ARTICLE 20 **COORDINATION OF CONTRACT DOCUMENTS**

The Proposal dated March 31, 2023, 2023 submitted by the Contractor in response to the RFP and Best and Final Offer, dated July 6, 2023 is attached hereto and incorporated herein as Appendix “H” for all purposes (the “Proposal”). In the event of a conflict, the order of prevailing precedence (a-highest order to d-lowest order of precedence) shall be as follows:

- (a) Any amendments to the Agreement.
- (b) The Agreement.
- (c) Appendices to the Agreement.

- (d) Work Authorizations Issued by the CTRMA
- (e) The Proposal.

However, if the Proposal can reasonably be interpreted as providing higher quality materials or services than those required by the other contract documents or otherwise contains offers, statements or terms more advantageous to the CTRMA, Contractor's obligations under the Agreement shall include compliance with all such statements, offers and terms contained in the Proposal

ARTICLE 21 **MAINTENANCE OF, ACCESS TO, AND AUDIT OF RECORDS**

a. **RETENTION AND AUDIT OF RECORDS.** Contractor shall maintain at its offices in Austin, Texas, a complete set of all books, records, electronic files and other documents prepared or employed by Contractor in its management, scheduling, cost accounting and other activities related to this Agreement. Contractor shall maintain all records and documents relating to this Agreement, including copies of all original documents, or electronic copies of such documents if approved by the CTRMA, delivered to the CTRMA until four (4) years after the date of the termination of this Agreement, or such period as is required by Texas law, whichever is longer. Contractor shall notify the CTRMA where such records and documents are kept. If approved by the CTRMA, photographs, microphotographs or other authentic reproductions may be maintained instead of original records and documents.

Contractor shall make these records and documents available for audit and inspection to the CTRMA, at the CTRMA's offices in Austin, Texas, at all reasonable times, without charge, and shall allow the CTRMA or its representatives to make copies of such documents. The CTRMA may direct its own auditors or representatives to perform such audits or reviews. Contractor shall cooperate fully with the entity performing the audit or review.

Notwithstanding the foregoing, the Contractor shall comply with all laws pertaining to the retention of records and the provision of access thereto. The Contractor shall maintain its books and records in accordance with generally accepted accounting principles in the United States, subject to any exceptions required by existing bond indentures of the CTRMA, and shall provide the CTRMA with a copy of any audit of those books and records as provided herein or otherwise requested by the CTRMA.

b. **PUBLIC INFORMATION ACT.** Contractor acknowledges and agrees that all records, documents, drawings, plans, specifications and other materials in the CTRMA's possession, including materials submitted by Contractor, are subject to the provisions of Chapter 552, Texas Government Code (the "Public Information Act"). Contractor shall be solely responsible for all determinations made by it under such law, and for clearly and prominently marking each and every page or sheet of materials with "Trade Secret" or "Confidential", as it determines to be appropriate. Contractor is advised to contact legal counsel concerning such law and its application to Contractor.

If any of the materials submitted by the Contractor to the CTRMA are clearly and prominently labeled "Trade Secret" or "Confidential" by Contractor, the CTRMA will endeavor

to advise Contractor of any request for the disclosure of such materials prior to making any such disclosure. Under no circumstances, however, will the CTRMA be responsible or liable to Contractor or any other person for the disclosure of any such labeled materials, whether the disclosure is required by law, or court order, or occurs through inadvertence, mistake or negligence on the part of the CTRMA.

In the event of litigation concerning the disclosure of any material marked by Contractor as “Trade Secret” or “Confidential,” the CTRMA’s sole obligation will be as a stakeholder retaining the material until otherwise ordered by a court, and Contractor shall be fully responsible for otherwise prosecuting or defending any action concerning the materials at its sole cost and risk; provided, however, that the CTRMA reserves the right, in its sole discretion, to intervene or participate in the litigation in such manner as it deems necessary or desirable. All costs and fees, including attorneys’ fees and costs, incurred by the CTRMA in connection with any litigation, proceeding or request for disclosure shall be reimbursed and paid by Contractor.

The requirements of Subchapter J of the Public Information Act may apply to this Agreement, and the Contractor agrees that the Agreement can be terminated if the Contractor knowingly or intentionally fails to comply with a requirement of that subchapter.

Notwithstanding any other provision of the Agreement, within five (5) business days of a request by the CTRMA, the Contractor shall provide any records related to this Agreement that are in the custody or possession of the Contractor that are subject to a pending request for information received by the CTRMA.

Not later than 180 days following the completion of the term of this Agreement the Contractor shall provide the CTRMA with all records related to this Agreement in the custody or possession of the Contractor. The cost of complying with Subchapter J of the Public Information Act is not subject to reimbursement by the CTRMA.

ARTICLE 22 **RELATIONSHIP BETWEEN THE PARTIES**

Notwithstanding the anticipated collaboration between the parties hereto, or any other circumstances, the relationship between the CTRMA and the Contractor shall be one of an independent contractor. The Contractor acknowledges and agrees that neither it nor any of its employees or subcontractors, shall be considered an employee of the CTRMA for any purpose. The Contractor shall have no authority to enter into any contract binding upon the CTRMA, or to create any obligation on behalf of the CTRMA. As an independent contractor, neither the Contractor nor its employees shall be entitled to any insurance, pension, or other benefits customarily afforded to employees of the CTRMA. Under no circumstances shall the Contractor, or its employees, or subcontractors, represent to suppliers, contractors or any other parties that it is employed by the CTRMA or serves the CTRMA in any capacity other than as an independent contractor. The Contractor shall clearly inform all suppliers, Contractors and others that it has no authority to bind the CTRMA. Nothing contained in this Agreement shall be deemed or construed to create a partnership or joint venture, to create the relationship of employee-employer or principal-agent, or to otherwise create any liability for the CTRMA whatsoever with respect to the liabilities, obligations or acts of the Contractor, its employees, subcontractors, or any other person.

ARTICLE 23
DELIVERY OF NOTICES, ETC.

In each instance under this Agreement in which one party is required or permitted to give notice to the other, such notice shall be deemed given either (a) when delivered by hand; (b) one (1) business day after being deposited with a reputable overnight air courier service; or (c) three (3) business days after being mailed by United States mail, registered or certified mail, return receipt requested, and postage prepaid. Any notices provided under this Agreement must be sent or delivered to:

In the case of the Contractor:

Kapsch TrafficCom USA, Inc.
2855 Premiere Parkway, Suite F
Duluth, GA 30097
Attn: Brooke Chaplain, Senior Legal Counsel

In the case of the CTRMA:

Central Texas Regional Mobility Authority
3300 N IH-35, Suite 300
Austin, TX 78705
Attn: Director of Information Technology

and:

Central Texas Regional Mobility Authority
3300 N IH-35, Suite 300
Austin, TX 78705
Attn: General Counsel

Either party hereto may from time to time change its address for notification purposes by giving the other party prior written notice of the new address and the date upon which it will become effective.

ARTICLE 24
REPORTING OF SUBPOENAS, NOTICES, ETC.

The Contractor shall immediately send the CTRMA a copy of any summons, subpoena, notice, or other documents served upon the Contractor, its agents, employees, subcontractors, or representatives, or received by it or them, in connection with any matter related to the Services under this Agreement.

ARTICLE 25
AUTHORITY'S ACTS

Anything to be done under this Agreement by the CTRMA may be done by such persons, corporations, firms, or other entities as the CTRMA may designate.

ARTICLE 26
LIMITATIONS

Notwithstanding anything herein to the contrary, all covenants and obligations of the CTRMA under this Agreement shall be deemed to be valid covenants and obligations only to the extent authorized by Chapter 370 of the Texas Transportation Code and permitted by the laws and the Constitution of the State of Texas, and no officer, director, or employee of the CTRMA shall have any personal obligations or liability thereunder or hereunder.

The Contractor is obligated to comply with applicable standards of professional care in the performance of the Services. The CTRMA shall have no obligation to verify any information provided to the Contractor by the CTRMA or any other person or entity.

ARTICLE 27
CAPTIONS NOT A PART HEREOF

The captions or subtitles of the several articles, subsections, and divisions of this Agreement are inserted only as a matter of convenience and for reference, and in no way define, limit or describe the scope of this Agreement or the scope or content of any of its articles, subsections, divisions, or other provisions.

ARTICLE 28
CONTROLLING LAW, VENUE

This Agreement shall be governed and construed in accordance with the laws of the State of Texas. The parties hereto acknowledge that venue is proper in Travis County, Texas, for all disputes arising hereunder and waive the right to sue and be sued elsewhere.

ARTICLE 29
COMPLETE AGREEMENT

This Agreement, including all Appendices attached hereto, sets forth the complete agreement between the parties with respect to the Services and supersedes all other agreements (oral or written) with respect thereto. Capitalized terms shall have the definitions provided herein. Any changes in the character, agreement, terms and/or responsibilities of the parties hereto must be enacted through a written amendment. No amendment to this Agreement shall be of any effect unless in writing and executed by the CTRMA and the Contractor. This Agreement may not be orally canceled, changed, modified or amended, and no cancellation, change, modification or amendment shall be effective or binding, unless in writing and signed by the parties to this Agreement. This provision cannot be waived orally by either party.

ARTICLE 30
TIME OF ESSENCE

With respect to any specific delivery or performance date or other deadline provided hereunder, time is of the essence in the performance of the provisions of this Agreement. The Contractor acknowledges the importance to the CTRMA of the timely provision of the Services and will perform its obligations under this Agreement with all due and reasonable care.

ARTICLE 31
SEVERABILITY

If any provision of this Agreement, or the application thereof to any person or circumstance, is rendered or declared illegal for any reason and shall be invalid or unenforceable, the remainder of this Agreement and the application of such provision to other persons or circumstances shall not be affected thereby but shall be enforced to the greatest extent permitted by applicable law.

ARTICLE 32
AUTHORIZATION

Each party to this Agreement represents to the other that it is fully authorized to enter into this Agreement and to perform its obligations hereunder, and that no waiver, consent, approval, or authorization from any third party is required to be obtained or made in connection with the execution, delivery, or performance of this Agreement.

ARTICLE 33
SUCCESSORS

This Agreement shall be binding upon and inure to the benefit of the CTRMA, the Contractor, and their respective heirs, executors, administrators, successors, and permitted assigns. The Contractor may not assign the Agreement or any portion thereof without the prior written consent of the CTRMA.

ARTICLE 34
INTERPRETATION

No provision of this Agreement shall be construed against or interpreted to the disadvantage of any party by any court, other governmental or judicial authority, or arbiter by reason of such party having or being deemed to have drafted, prepared, structured, or dictated such provision.

ARTICLE 35
BENEFITS INURED

This Agreement is solely for the benefit of the parties hereto and their permitted successors and assigns. Nothing contained in this Agreement is intended to, nor shall be deemed or construed to, create or confer any rights, remedies, or causes of action in or to any other persons or entities, including the public in general. Notwithstanding the foregoing, the Contractor acknowledges that the Services provided for hereunder may be made available to other toll authorities through agreements between the CTRMA and those entities, and that Contractor is required to perform for those entities in a manner which complies with the requirements and obligations of this Agreement. The CTRMA shall have the right to enforce this Agreement against Contractor on behalf of other entities to which the Services are being provided.

ARTICLE 36
SURVIVAL

The parties hereby agree that each of the provisions in the Agreement are important and material and significantly affect the successful conduct of the business of the CTRMA, as well as its reputation and goodwill. Any breach of the terms of this Agreement is a material breach of this Agreement, from which the Contractor may be enjoined and for which the Contractor also shall pay to the CTRMA all damages which arise from said breach. The Contractor understands and acknowledges that the Contractor's responsibilities under Articles 13, 16 and 17 of this Agreement shall continue in full force and effect after the Contractor's contractual relationship with the CTRMA ends for any reason.

ARTICLE 37
FORCE MAJEURE

If a Force Majeure Event occurs, the Nonperforming Party is excused from performance of its obligations under this Agreement but only for the time and to the extent that such performance is prevented by the Force Majeure Event. During a Force Majeure Event that prevents Contractor from delivering Services, Contractor's entitlement to compensation under this Agreement is suspended.

When the Nonperforming Party is able to resume performance of its obligations under this Agreement, it will immediately give the Performing Party (defined below) written notice to that effect and promptly resume performance under this Agreement.

The relief offered by this Force Majeure provision is the exclusive remedy available to the Nonperforming Party with respect to a Force Majeure Event.

The Performing Party may terminate this Agreement if:

- (a) the Nonperforming Party's failure to perform under this Agreement due to a Force Majeure Event impairs material benefits of this Agreement to the other party (the "Performing Party"); and
- (b) the Nonperforming Party does not resume performance in accordance with this Agreement within thirty (30) days following the giving of notice to the Nonperforming Party of the Performing Party's intent to terminate this Agreement.

In this Agreement, "Force Majeure Event" means any act, event, or condition not foreseeable by a party (the "Nonperforming Party") that: (A) prevents the Nonperforming Party from performing its obligations under this Agreement; (B) is beyond the control of, not caused in whole or in part by, and not otherwise the fault of the Nonperforming Party; and (C) is not able to be overcome or avoided by the Nonperforming Party's exercise of diligence or preventative measures. Notwithstanding the foregoing, Force Majeure Events shall be limited to the following: any earthquake, tornado, hurricane, flood or other natural disaster, fire, freight embargo, strike, blockade, rebellion, war, riot, act of sabotage or civil commotion. The following do not constitute a Force Majeure Event: economic hardship, changes in market conditions, or insufficiency of funds.

ARTICLE 38
DISPUTE RESOLUTION

The parties have established an issues resolution ladder in order to resolve disputes expeditiously and effectively at appropriate organizational levels of each party. In the event of any dispute whatsoever arising out of or relating to this Agreement, the disputing party must submit a written notice of the dispute to the Tier 1 designee of the other party shown in the issues resolution ladder below. The notice must state clearly, and in detail, the good faith basis for the dispute. Disputes shall be considered as quickly as possible, taking into consideration the particular circumstances and the time required to prepare detailed documentation. Steps may be omitted as agreed by both parties, and the time periods stated below may be shortened in order to hasten resolution.

Issues Resolution Ladder

<i>Tier</i>	<i>Contractor</i>		<i>CTRMA</i>	<i>Time Limit*</i>
1	Project Manager	and	CTRMA Assistant Director of Information Technology	10 days
2	Account Vice President	and	CTRMA Director of Operations	10 days
3	Chief Financial Officer	and	CTRMA Executive Director	10 days

** Time (in calendar days) in which dispute must be resolved or passed on to the next tier.*

If a dispute is processed under the issues resolution ladder and not resolved, the parties may attempt to resolve the dispute through mediation, using a mediator mutually agreed upon by the Contractor and the CTRMA, prior to initiating litigation.

At all times during this dispute resolution process or any subsequent administrative, mediation or court proceeding, the Contractor shall proceed with the provision of the Services, without delay, in accordance with this Agreement, and as directed by the CTRMA through a Work Authorization. The Contractor acknowledges that it shall be solely responsible for any delay that results from its actions or inactions during the dispute resolution process, even if the Contractor's position in connection with the dispute ultimately prevails.

ARTICLE 39
CONTRACTOR CERTIFICATIONS

a. **Entities that Boycott Israel.** The Contractor represents and warrants that (1) it does not, and shall not for the duration of this Agreement, boycott Israel or (2) the verification required by Section 2271.002 of the Texas Government Code does not apply to this Agreement. If circumstances relevant to this provision change during the course of the contract, the Contractor shall promptly notify the CTRMA.

b. **Entities that Boycott Energy Companies.** The Contractor represents and warrants that: (1) it does not, and will not for the duration of this Agreement, boycott energy companies or (2) the verification required by Section 2274.002 of the Texas Government Code does not apply to this Agreement. If circumstances relevant to this provision change during the course of this Agreement, the Contractor shall promptly notify the CTRMA.

c. **Entities that Discriminate Against Firearm Entities or Trade Associations.** The Contractor verifies that: (1) it does not, and will not for the duration of this Agreement, have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association or (2) the verification required by Section 2274.002 of the Texas Government Code does not apply to this Agreement. If circumstances relevant to this provision change during the course of this Agreement, the Contractor shall promptly notify the CTRMA.

[Remainder of Page Intentionally Left Blank]

IN WITNESS WHEREOF, the parties have executed this Agreement effective on the date and year first written above.

CONTRACTOR: **KAPSCH TRAFFICCOM USA, INC.**

By: _____
Name: JB Kendrick
Title: President

CTRMA: **CENTRAL TEXAS REGIONAL MOBILITY
AUTHORITY**

By: _____
Name: James Bass
Title: Executive Director

APPENDIX A
Scope of Services

Contents

1. Scope of Work.....	1
1.1 General.....	1
1.1.1 Item Additions and Deletions.....	2
1.1.2 Applicable Specifications and Standards.....	2
1.2 Approval of Products	3
1.3 Services To Be Provided	3
1.3.1 Maintenance Services	3
1.3.1.1 Scheduled and Preventive Maintenance Services	4
1.3.1.1.1 Scheduled and Preventive Maintenance Activities	4
1.3.1.1.2 Identified Deficiencies	5
1.3.1.1.3 Non-Scheduled Maintenance and Repairs	5
1.3.1.2 Diagnostic and Troubleshooting Services	6
1.3.1.3 Repair Services.....	6
1.3.1.3.1 On-Site Repairs	9
1.3.1.3.2 Equipment Replacement	10
1.3.1.4 Emergency Repair Services.....	10
1.3.1.5 Utility Locating Services.....	11
1.3.1.6 Equipment Logs	11
1.3.2 New Construction Services.....	12
1.3.3 Design Liaison and Support Services	20
1.3.4 Control of Materials	20
1.3.4.1 Device Inventory.....	21
1.3.4.1.1 Existing TIMC Device Inventory	21
1.3.4.1.2 Existing Field Device Inventory	21
1.3.4.1.3 Inventory Disposal	22
1.3.4.2 Inventory Management System	23
1.4 General Requirements for Execution of Work	23
1.4.1 Location of the Work.....	25
1.4.1.1 Traffic Incident Management Center (TIMC)	25
1.4.1.2 Field Sites.....	26
1.4.2 Scheduling and Execution of Work	26
1.4.3 Mobilization.....	27
1.4.4 Temporary Traffic Control.....	27
1.4.5 Warranty for Vendor Services and Materials.....	27
1.4.6 Lost, Stolen, or Damaged MOBILITY AUTHORITY Owned Resources	28

1.4.7	Materials to be Furnished	28
1.4.8	Software	29
1.4.9	Incidental Materials.....	29
1.4.10	Equipment, Machinery, Tools, and Vehicles.....	29
1.4.10.1	Control of Equipment	30
1.4.11	Working Hours, On-Call Responsibilities, and Response Times.....	31
1.4.11.1	Standard Hours of Operation	31
1.4.11.2	On-call Responsibilities.....	31
1.4.11.3	Response Times	31
1.4.11.3.1	Repair Services Response Time	31
1.4.11.3.2	Emergency Repair Response Time	32
1.4.12	Security and Safety Requirements	32
1.4.13	License and Insurance Qualifications	32
1.5	Required Qualifications of Vendor	33
1.5.1	Use of Subcontractor(s) or Subconsultant(s)	33
1.5.2	Staffing Requirements.....	33
1.5.3	Maintenance Staff Location and Availability.....	34
1.5.4	Vendor Facilities	34
1.5.5	Position Descriptions.....	35
1.5.6	General Appearance and Conduct	40
1.5.7	Training.....	40
1.5.8	Personnel Vetting.....	41
1.5.8.1	Background Check	41
1.5.8.2	Criminal Record Check.....	41
1.5.8.3	Drug-Free Workplace Certification.....	41
1.6	Criteria for Performance Measures and Evaluation	41
1.6.1	Staff Performance	42
1.6.2	Availability	42
1.6.2.1	Staff Availability.....	42
1.6.2.2	System and Device Uptime.....	42
1.6.2.3	Response and Repair Times.....	43
1.6.2.4	General Performance Measures	43
1.7	Services, Materials Provided by the Mobility Authority.....	44
1.7.1	Contract Management	44
1.7.2	Coordination.....	44
1.7.3	Access to Facilities.....	44
1.7.4	Technical Reviews	44

1.7.5 Existing Documentation	45
1.8 Contract Monitoring, Progress, Reporting and Coordination	45
1.8.1 Status Reports	45
1.8.1.1 Monthly Report	46
1.8.1.2 Annual Report.....	47
1.8.2 Meetings.....	48
1.8.3 Transition Plan.....	48
1.8.4 Project Management Plan.....	48
1.8.5 Preventative Maintenance Activities Plan	49
1.9 Submittals / Deliverables	49
1.9.1 Estimates	49
1.9.2 Equipment Submittal.....	49
1.9.3 Maintenance Documentation	49
1.9.3.1 Maintenance Checklists.....	49
1.9.3.2 Equipment Maintenance Logs.....	50
1.9.4 As-Built Plans.....	50
1.9.5 Status Reports	50
1.10 Preventative Maintenance Minimum Requirements	50
1.10.1 General	50
1.10.2 Minimum Requirements for Monthly Maintenance.....	50

List of Tables

Table 1: New construction services activities for Intelligent Transportation System (ITS) deployment.....	12
--	----

1. SCOPE OF WORK

1.1 GENERAL

The Central Texas Regional Mobility Authority (CTRMA) hereafter known as the MOBILITY AUTHORITY, requires maintenance and construction services by a qualified Intelligent Transportation Systems (ITS) device maintenance and construction firm, hereafter known as the VENDOR, for all work related to ITS devices, communications, electrification, and infrastructure, hereafter known as the SYSTEM, located in the counties of Hays, Travis, and Williamson. The SYSTEM consists of, but is not limited to, the following:

- Concrete encased conduit ductbank
- Conduit (laterals)
- Ground and junction boxes
- Underground cable vaults (UCV)
- Communications cable
- Electrical system and device grounding and surge suppression
- Electrical service wiring
- Electrical power service assemblies (i.e., electrical meter, service disconnect, step-up / step-down transformer, branch circuit disconnect)
- Pre-stressed concrete and steel device poles
- Field device equipment cabinets
- Communication equipment cabinets
- Network devices (e.g., aggregation/distribution, edge switches, terminal servers, Ethernet extenders, media converters)
- Wireless communication devices
- Remote Power Management Units (RPMU)
- Radar Vehicle Sensing Devices (RVSD)
- Bluetooth travel time reader units
- Video equipment (e.g., closed-circuit television (CCTV) cameras, video encoders/decoders, mounting hardware, video wall components, back-end software)
- Camera lowering systems
- Dynamic highway signing (e.g., dynamic message signs (DMS), LED highlighted signs, blankout signs, and electronic display signs, portable changeable message signs, sign support structures)
- Wrong way vehicle detection systems (WWVDS)
- Connected Vehicle (CV) technology (e.g., roadside units (RSU), edge-computer platforms, on-board units (OBU) within maintenance fleet vehicles)
- Road weather information systems (RWIS)
- Ancillary device equipment (e.g., power supplies, Power-over Ethernet (PoE) injectors)
- Portable and permanent emergency power generators

- Uninterruptable power supplies (UPS)
- Communications hubs and equipment shelters
- Ancillary facilities (e.g., central software servers, licensing, workstations)
- Environmental conditioning equipment
- Hardware, software, and firmware related to ITS equipment and other traffic control devices

The SYSTEM described in this Scope of Work (SOW) shall cover all existing and future ITS elements within the geographic coverage area and term defined in this agreement, hereafter known as the CONTRACT.

1.1.1 Item Additions and Deletions

During the Contract period and any renewal periods, the MOBILITY AUTHORITY shall have the right to add or delete items (services and/or commodities) to or from this agreement. Any new items added shall be at the requirements, specifications, terms, and conditions stated herein or as later stipulated by the MOBILITY AUTHORITY, and at mutually agreed pricing accepted, in writing, by both the VENDOR and the MOBILITY AUTHORITY. Items may be removed at the sole discretion of the MOBILITY AUTHORITY, per the requirements, terms, and conditions herein and/or as permitted by Texas Statutes or Texas Administrative Code.

Due to the changing dynamics within any ITS deployment, the VENDOR will be able, upon written authorization by the MOBILITY AUTHORITY and upon supplemental agreement to the CONTRACT as to compensation and time, to perform additional services pertaining to the support and/or maintenance of the ITS field devices and infrastructure not otherwise identified in this CONTRACT, as may be required by the MOBILITY AUTHORITY.

1.1.2 Applicable Specifications and Standards

All work shall be prepared using English units in accordance with the latest editions of standards and requirements utilized by the MOBILITY AUTHORITY, which include, but are not limited to, publications such as:

- 29 Code of Federal Regulations (CFR), Part 1910.1101 – Asbestos Standard for Industry, U.S. Occupational Safety and Health Administration (OSHA)
- 29 CFR, Part 1926, 1101 – Asbestos Standard for Construction, OSHA
- 40 CFR, Part 61, Subpart M - National Emission Standard for Hazardous Air Pollutants (NESHAP), Environmental Protection Agency (EPA)
- 40 CFR, Part 763, Subpart E – Asbestos-Containing Materials in Schools, EPA
- 40 CFR, Part 763, Subpart G – Asbestos Worker Protection, EPA
- Americans with Disabilities Act Accessibility Guidelines
- Manual on Uniform Traffic Control Devices (MUTCD), Federal Highway Administration
- Mobility Authority Policy Code
 - <https://www.mobilityauthority.com/about/policy-disclaimers/code>.

- National Electrical Safety Code (NESC)
- National Electrical Code (NEC)
- Standard Highway Signs Manual, Federal Highway Administration
- Texas Administrative Code
- Texas Department of Transportation Standard Specification for Construction and Maintenance of Highways, Streets, and Bridges
- Texas Department of Transportation CAD Standards
- Texas Department of Transportation Traffic Operations Division Standard Details
- Texas Department of Transportation Design Division Standard Details
- Texas Department of Transportation Design Maintenance Division Standard Details
- Texas Department of Transportation Bridge Division Standard Details
- Texas Department of Transportation Manual on Uniform Traffic Control Devices (TMUTCD)
- Texas Statutes

1.2 APPROVAL OF PRODUCTS

The VENDOR shall submit detailed technical product data sheets for all products for review and approval by the MOBILITY AUTHORITY prior to purchasing and installation of any field device, infrastructure, back-end hardware, or software. The VENDOR shall clearly identify the selected manufacturer and model number of each product submitted for approval. The VENDOR shall be responsible for providing product data sheets for all elements required for a complete installation—including but not limited to devices, communication equipment, mounting hardware, surge protection devices, power supplies, and cabling. The VENDOR shall provide a complete submittal package to the MOBILITY AUTHORITY a minimum of ten (10) business days prior to the scheduled work.

In the case of materials that have been previously approved, the MOBILITY AUTHORITY may elect to forego the review and approval process at the sole discretion of the MOBILITY AUTHORITY.

1.3 SERVICES TO BE PROVIDED

1.3.1 Maintenance Services

The objective of services required under this CONTRACT is to ensure continuous (24 hours/day, 7 days/week, 365 days/year) operation and functionality of all components of the SYSTEM and provide locate services for all ITS equipment. The MOBILITY AUTHORITY will assign a Project Manager responsible for oversight of this CONTRACT and assignment of tasks to the VENDOR. References to the MOBILITY AUTHORITY or the MOBILITY AUTHORITY'S Project Manager within this scope include the MOBILITY AUTHORITY'S Project Manager or designated representatives.

The VENDOR will be evaluated periodically based on SYSTEM uptime, this includes the use of automated performance monitoring software or periodic manual observation. The VENDOR will

be responsible for all SYSTEM support, including but not limited to scheduled, periodic, and routine maintenance; and replacement of failed or destroyed components. All preventative and routine maintenance services shall be performed as part of a recurring (e.g., annual) Work Authorization (WA); additional identified work—such as replacement of failed or destroyed infrastructure—will be assigned on a Work Authorization (WA) basis, as directed by the MOBILITY AUTHORITY'S Project Manager.

The VENDOR shall be on-call on a 24 X 7 X 365 basis for the duration of the CONTRACT to respond to emergency repair and/or replacement work, including but not limited to severe weather events and warnings. If a State of Emergency is declared by the Governor of Texas, the VENDOR may be called upon to provide repair and replacement services associated with disaster recovery. The VENDOR shall provide the MOBILITY AUTHORITY'S Project Manager with a list of at three (3) telephone numbers that will be answered at all times by the VENDOR'S personnel. The VENDOR shall maintain staffing levels required by this Scope of Work (SOW) at all times to ensure services required by the SOW under this CONTRACT are met.

Throughout the term of this CONTRACT, the MOBILITY AUTHORITY'S Project Manager will conduct reviews of the VENDOR'S work and daily operations. The VENDOR shall cooperate and assist the MOBILITY AUTHORITY'S Project Manager throughout the review process.

1.3.1.1 Scheduled and Preventive Maintenance Services

Coordinate the frequency of standard scheduled maintenance services with the MOBILITY AUTHORITY'S Project Manager, or as identified in the Work Authorization (WA). It shall be the VENDOR'S responsibility to respond to maintenance requests according to the priority assigned by the MOBILITY AUTHORITY. The definitions below shall be a baseline for this CONTRACT. At the discretion of the MOBILITY AUTHORITY, the VENDOR may be dispatched to any work priority deemed appropriate by the MOBILITY AUTHORITY.

1.3.1.1.1 Scheduled and Preventive Maintenance Activities

Typical scheduled maintenance includes SYSTEM inspection and other activities recommended by equipment manufacturers to be performed at periodic intervals. During the term of the CONTRACT, the VENDOR will perform scheduled, periodic preventive maintenance based upon manufacturer recommendations, budget limitations, and as general services are authorized by the MOBILITY AUTHORITY. If periodic maintenance intervals and activities are not specified by the equipment manufacturer, the VENDOR will develop periodic maintenance intervals and activities for approval by the MOBILITY AUTHORITY'S Project Manager. Scheduled preventive maintenance also includes periodic inspections and cleaning, as well as documentation of these actions. The MOBILITY AUTHORITY will work with the VENDOR to develop preventive maintenance checklists to ensure that consistent, comprehensive maintenance activities are executed correctly and documented. All work for scheduled and preventative maintenance shall be compensated by the monthly Maintenance Service Unit Price, unless otherwise noted.

1.3.1.1.2 Identified Deficiencies

In the event that the VENDOR encounters minor and/or major infrastructure (e.g., field device, equipment, hardware, cabling, wiring) deficiencies while performing preventive maintenance services as outlined above, the VENDOR shall correct such deficiencies during the preventive maintenance site visit, whenever possible.

The MOBILITY AUTHORITY considers minor repair to be the repair of minor deficiencies including, but not limited to, an unplugged device cable; tripped circuit breaker; loose connector; displaced or disorganized cabinet equipment; untidy or unlabeled cabling; debris, trash, dirt, or vermin droppings in cabinets or enclosures; and more. Additionally, minor repairs include the replacement of ancillary system components and hardware the VENDOR is reasonably expected to have on-hand spares including, but not limited to, surge protection devices, relays, power supplies, media converters, transceivers, patch cables, jumpers, mounting brackets, and more.

The MOBILITY AUTHORITY considers major repair to be the repair of major deficiencies including, but not limited to, a non-functional field device, physically damaged equipment, components exposed to weather, exposed power cabling, or items constituting a safety hazard. The VENDOR shall immediately contact the MOBILITY AUTHORITY'S Project Manager to report major deficiencies. The MOBILITY AUTHORITY will issue Work Authorizations (WA) to complete the necessary repair activities. The VENDOR shall identify all materials and labor necessary to complete the work and provide a price proposal, in accordance with the pricing included in the CONTRACT.

1.3.1.1.3 Non-Scheduled Maintenance and Repairs

Non-scheduled maintenance includes reactive maintenance, replacements, and diagnostic work necessary to correct deficiencies and keep the SYSTEM operational. This work may not be scheduled but is often generated by failures caused by acts of nature, construction, or accidents. Non-scheduled maintenance may include, but is not limited to:

1. Field repair or replacement of ancillary parts or equipment for any ITS field device, equipment, or cabling
2. Resetting of field devices, including DMS displays, controllers, CCTV cameras, vehicle detection systems, etc.
3. Focusing and re-aiming of CCTV cameras, vehicle detection systems, and other field sensors
4. Configuring or repairing the communications network, including switches, media converters, wireless communication devices, and terminal servers
5. Configuring or repairing CCTV video transmission equipment, including, PoE injectors, encoders, and decoders
6. Testing fiber optic cable (FOC) for optical budget requirements
7. Repairing damage caused by vandalism, accidents, or weather

If the cause of a failure is unknown, the MOBILITY AUTHORITY may have the VENDOR perform diagnostic work as required to determine the cause of the failure. The VENDOR shall perform all work to repair and restore the failed systems while on-site. In the event the VENDOR is unable to correct the failed system, the MOBILITY AUTHORITY will issue Work Authorizations (WA) to complete the necessary repair activities. The VENDOR shall identify all materials and labor necessary to complete the work and provide a price proposal, in accordance with the unit costs in the CONTRACT.

1.3.1.2 Diagnostic and Troubleshooting Services

The VENDOR will be required to provide diagnostic and troubleshooting services when equipment is inoperable and field troubleshooting is needed to identify the problem. When possible, the VENDOR shall perform minor repairs following diagnosis. The VENDOR must document troubleshooting and repair activities and services performed at the site. Major repairs require approval by the MOBILITY AUTHORITY before additional service can be performed.

If the VENDOR detects a device that exhibits frequent failures or requires an “on-off-on” power cycle in order to maintain operation, it shall be the responsibility of the VENDOR to notify the MOBILITY AUTHORITY, contact the equipment manufacturer, and recommend corrective action to the MOBILITY AUTHORITY. It is the responsibility of the VENDOR to service equipment and restore SYSTEM components to a 100-percent functional status and ensure all field devices and equipment are online. The VENDOR is responsible for all troubleshooting and repair of SYSTEM devices. The MOBILITY AUTHORITY Project Manager may provide MOBILITY AUTHORITY staff and resources to assist the VENDOR with troubleshooting and repair.

Should a particular device continue to fail, and the issue cannot be resolved by repair or replacement, the MOBILITY AUTHORITY, at its sole discretion, may remove the device from the VENDOR’S responsibility.

The VENDOR, through diagnostic service, shall investigate the cause for the failure of equipment and determine if the failure is related to a severe weather event, materials, or workmanship, supplied power, leased communications, electrical and/or mechanical components, hardware or software, or other failures. The diagnostic results shall define the type of repair needed to restore the device(s) to 100-percent functional status. The VENDOR shall investigate whether or not failures are covered under existing equipment warranties. If the diagnosis indicates the need for repairs or parts replacement, the VENDOR shall follow the procedures established between the VENDOR and the MOBILITY AUTHORITY’S Project Manager under this CONTRACT.

1.3.1.3 Repair Services

Repairs and/or parts replacement will be covered under Work Authorizations (WA) on an as-needed basis dependent upon the categorization of the repair (e.g., minor, major, warranty). The VENDOR shall identify all materials and labor necessary to complete the work and provide a

price proposal, in accordance with the unit costs the CONTRACT. Descriptions of labor, materials, and equipment shall be included as part of a work request as well as a justification for the work. The VENDOR shall submit written request(s) to the MOBILITY AUTHORITY for approval of any additional labor usage and expenditures that are not covered under a Work Authorization (WA).

- **Minor Repair**

Minor repairs for this CONTRACT are repairs/replacement of components due to equipment malfunction or end of service life. The MOBILITY AUTHORITY considers minor repair to be the repair of minor deficiencies including, but not limited to, an unplugged device cable; tripped circuit breaker; loose connector; displaced or disorganized cabinet equipment; untidy or unlabeled cabling; debris, trash, dirt, or vermin droppings in cabinets or enclosures; and more. Additionally, minor repairs include the replacement of ancillary system components and hardware the VENDOR is reasonably expected to have on-hand spares including, but not limited to, surge protection devices, relays, power supplies, media converters, transceivers, patch cables, jumpers, mounting brackets, and more. The VENDOR shall perform the necessary repair/replacement work, which includes diagnostic services.

Minor repairs are generally considered to be repairs that require less than four (4) hours of labor and can be completed on-site utilizing available materials and/or spare parts. Minor repairs shall be compensated by the monthly Maintenance Service Unit Price.

- **Major Repair**

Major repairs for this CONTRACT are defined as non-typical repairs that need diagnostic services to identify the problem, extensive repair services, temporary traffic control (TTC) and lane closures, utility coordination, or other regional agency coordination, such as damage caused by crashes, vandalism, theft, weather events, fiber cuts, power loss from the utility service point, and construction activity. The MOBILITY AUTHORITY considers major repair to be the repair of major deficiencies including, but not limited to, a non-functional field device, physically damaged equipment, components exposed to weather, exposed power cabling, or items constituting a safety hazard. Typical major repairs and parts replacement consist of, but are not limited to, repair or replacement of damaged, missing, or malfunctioning equipment in order to maintain the ITS operation and functionality.

For all major repairs, the VENDOR shall contact the MOBILITY AUTHORITY'S Project Manager to report field findings and receive instruction and authorization for related work. The MOBILITY AUTHORITY will issue Work Authorizations (WA) to complete the necessary repair activities. The VENDOR shall identify all materials and labor necessary to complete the work and provide a price proposal, in accordance with the unit costs in the CONTRACT. The VENDOR shall prepare and submit a diagnostic report, including

damage assessment, cost estimates, and recommendations for repair. The VENDOR shall not make major repairs prior to issuance of the WA covering specific corrective actions necessary for restoration.

Major repairs are generally considered to be repairs that require more than four (4) hours of labor and cannot be completed on-site utilizing on-hand materials and/or spare parts.

- **Warranty Repair**

The VENDOR shall act on behalf of the MOBILITY AUTHORITY to track manufacturer warranties and pursue warranty repairs from device manufacturers when failures are covered by the manufacturer's warranty. The VENDOR is responsible for coordinating warranty repairs with the MOBILITY AUTHORITY'S Project Manager and the device manufacturer/reseller. In the event warranty or insurance coverage is applicable, the VENDOR shall identify the proper procedure for contacting the entity responsible for coverage, secure the proper forms used for claim notification, and coordinate the repair, return, and disposition of equipment. Repaired MOBILITY AUTHORITY equipment returned from the manufacturer shall be held in inventory as spare parts if it is not to be immediately reinstalled.

The VENDOR shall support the MOBILITY AUTHORITY in pursuing claims until each claim is resolved to the satisfaction of the DEPARTMENT.

Repairs that require expertise and/or specialized equipment of the manufacturer shall be considered original equipment manufacturer (OEM) repairs. OEM repairs are specialized repairs that cannot be made by the VENDOR and must be made by the manufacturer or vendor of the equipment/component. On an as-needed basis, the VENDOR shall notify the MOBILITY AUTHORITY'S Project Manager of OEM repairs necessary for the continued safe and efficient operation of the SYSTEM. Accompanying notification, the VENDOR shall submit an OEM repair request to the MOBILITY AUTHORITY'S Project Manager for review. Approval of this request is required in order to proceed with the repair. If a device manufacturer is no longer producing, selling, or repairing a specific device, the VENDOR shall research, price, and present an alternate product to the MOBILITY AUTHORITY.

The VENDOR is required to assure the MOBILITY AUTHORITY that warranties are not voided by VENDOR repair services or other actions of the VENDOR at any point during the contract. If a device warranty expires, the VENDOR shall notify the MOBILITY AUTHORITY for the option to renew and/or replace the device if the unit is non-operational within 60 days of the warranty's expiration.

The VENDOR shall have the necessary equipment and personnel capable of maintaining and repairing the field equipment and infrastructure deployed throughout the geographic coverage area within the MOBILITY AUTHORITY's geographic boundaries. This includes a variety of

devices and communications infrastructure. Field site repair includes, but is not limited to, device replacement, electrical service work and repair, optical fiber cable splicing and troubleshooting, optical time domain reflectometer (OTDR) testing, fiber enclosure/fiber distribution panel installations, and terminations. The VENDOR shall have the capability to install and repair concrete encased conduit ductbank. The VENDOR shall have the capability to install and repair open trench, directional bored, and above ground lateral conduit. It shall be the responsibility of the VENDOR to perform all subsurface utility engineering (SUE) and obtain any permits required by the MOBILITY AUTHORITY and third-party entities before the VENDOR commences any work. After completion of device and/or communications infrastructure work by the VENDOR, documentation shall be presented to the MOBILITY AUTHORITY for record keeping of changes made to the fiber communication infrastructure and other components of the SYSTEM. At a minimum documentation must include repair notes; material quantities; and marked-up as-built construction plans and/or schematics that reflect post-repair conditions. No fiber related work shall be started by the VENDOR without written authorization and approval by the MOBILITY AUTHORITY.

1.3.1.3.1 On-Site Repairs

This work includes on-site repairs of devices and systems using readily available spare and component parts. New replacement parts for repairs are to be used unless otherwise directed by the MOBILITY AUTHORITY. If the existing component is to be replaced by a part that is not the same, the VENDOR shall not purchase or install the spare part until it has been approved by the MOBILITY AUTHORITY. The VENDOR shall be responsible for inventory control of all parts held in inventory for repair of devices that they have responsibility to maintain. Parts commonly used for shop and field repairs include, but are not limited to:

- Pan-tilt-zoom (PTZ) camera modules
- DMS LED display modules
- Vehicle Detectors
- Network Switches
- Power supplies
- Batteries
- UPS
- Media Converters
- PoE Injectors
- Terminal Blocks
- Surge Protection Devices
- Cabling and cabling connectors

The VENDOR shall submit requests to purchase spare parts including manufacturer, model, quantity, and unit cost to the MOBILITY AUTHORITY for review and approval prior to purchasing. The VENDOR shall notify the MOBILITY AUTHORITY of any part or component of the SYSTEM moved from its original location for the purpose of inventory control. The VENDOR

shall ensure all spare equipment is available in a timely manner and all inventory control records will be updated within seventy-two (72) hours.

1.3.1.3.2 Equipment Replacement

This work includes furnishing replacement devices needed for maintenance of the SYSTEM. Technical product data sheets for all new replacement parts must be submitted and approved by the MOBILITY AUTHORITY, in accordance with **Section 1.2 - Approval of Products**. The VENDOR shall not purchase or install equipment that has not been approved by the MOBILITY AUTHORITY. Proposed replacement parts shall be procured at the unit costs identified in the CONTRACT. The Vendor shall ensure the latest compatible technology, equal to or better in function and quality to existing SYSTEM components or equipment is provided for all replacement parts. Provide the specific manufacturer and model identified in the CONTRACT, where applicable. The VENDOR shall be responsible for inventory control of all equipment that they have responsibility to maintain within the SYSTEM and all devices, parts, and materials used to perform work.

When the MOBILITY AUTHORITY determines that additional parts are to be provided by the VENDOR as spares, the VENDOR shall procure and maintain the parts in MOBILITY AUTHORITY designated or approved location(s). The VENDOR shall notify the MOBILITY AUTHORITY of any part or component of the SYSTEM moved from its original location for the purpose of inventory control.

1.3.1.4 Emergency Repair Services

Emergency services consist of the restoration of components resulting from any malfunction or damage that creates a safety hazard or severely reduces the operational effectiveness of the overall SYSTEM. The VENDOR shall immediately correct any safety hazards discovered in the SYSTEM. Failures tend to be caused by severe and unusual forces of nature, crashes and collisions, vandalism, theft, fire, erosion, and extreme exposure to chemicals or pollutants. Communication and electrical cable cuts and loss of communications between the Traffic Incident Management Center (TIMC) and multiple field sites can warrant emergency repair services, as determined by the MOBILITY AUTHORITY.

The VENDOR will be required to supply substitute devices approved by the MOBILITY AUTHORITY to immediately restore normal operations during emergency repair services, when directed. Failure to restore normal operations in a timely manner may result in deductions of monies due or which may become due the VENDOR. If a structural failure causes a safety hazard or obstructs a roadway or waterway, the VENDOR will be required to remove the structure immediately.

The VENDOR must document malfunction and damage that necessitates emergency repair services. At a minimum, documentation shall include:

1. Device location, type, model, and serial and control number
2. Date and time of incident

3. Cause of failure and name of person reporting failure
4. Site needs analysis and digital photo documentation
5. Immediate repairs and corrective actions taken, including temporary repairs and repair cost breakdown
6. Corrective actions necessary for permanent repairs to be performed, including parts list, schedule, and estimated cost
7. Date, time, equipment, and personnel utilized for all corrective actions taken, temporary and permanent

The MOBILITY AUTHORITY will issue Work Authorizations (WA) to complete the necessary emergency repair activities. The VENDOR shall identify all materials and labor necessary to complete the work and provide a price proposal, in accordance with the unit costs in the CONTRACT. If an immediate repair order is needed, the MOBILITY AUTHORITY may issue a pre-approved, limited-amount WA to start the work. The VENDOR must receive approval prior to executing this WA. The VENDOR must document any verbal approvals issued for service/repair orders including the date, time, reason, and the name of the MOBILITY AUTHORITY Project Manager who issued and approved the WA.

1.3.1.5 Utility Locating Services

The VENDOR shall be responsible for locating and designating existing and future subsurface utilities associated with the SYSTEM. Cost to repair or replace underground facilities damaged as a result of incorrect locates shall be the responsibility of the VENDOR. The VENDOR must register with the Texas811 system within thirty (30) days of CONTRACT execution. The VENDOR shall be responsible for evaluating all locate tickets within the geographic area defined in this CONTRACT and shall be responsible for locating all MOBILITY AUTHORITY owned communications infrastructure (e.g., fiber optic communications) and electrical conductors within the SYSTEM. The MOBILITY AUTHORITY will issue Work Authorizations (WA) to complete necessary locates. The VENDOR shall identify all materials and labor necessary to complete the work and provide a price proposal, in accordance with the labor and material costs in the CONTRACT. All footages shall be validated by the original locate ticket and field photos when location of facilities is completed, and the ticket has been closed as “clear or flagged.” The VENDOR will be required to locate specific ITS facilities and document their findings within plan sets or another method approved by the MOBILITY AUTHORITY.

1.3.1.6 Equipment Logs

The VENDOR is required to document equipment and activities performed at each ITS device location. The VENDOR must maintain an equipment log documenting preventive scheduled maintenance and repair services, including repair logs, parts replacement, special notes, recommendations, and equipment warranty records. Device records must include, but are not limited to:

1. Device location, number, and type
2. Model and serial number

3. Firmware version
4. Manufacturer
5. Date, time, and description of failure
6. Report of failure source
7. Response details including arrival time, site conditions, and actions taken
8. Resolution details with documentation including date, time, equipment, and personnel utilized
9. Spare part(s) used, including type, model, serial, and control number
10. Replacement part notes and repair actions
11. Digital photo documentation before and after repair

1.3.2 New Construction Services

At the request of the MOBILITY AUTHORITY, the VENDOR shall perform all work for the installation of new infrastructure, facilities, and equipment related to the overall Intelligent Transportation System (ITS). This work may include, but is not limited to, the installation or retrofit of existing conduit ductbank, underground cable vaults, ground boxes, electrical power services, device poles, equipment cabinets, networking hardware, power service equipment, field devices (e.g., CCTV cameras, radar vehicle sensing devices (RVSD), dynamic message signs (DMS), wrong way vehicle detection systems (WWVDS), Connected Vehicle (CV) roadside units (RSU)), power and communications cabling, grounding arrays, and more. The VENDOR shall be responsible for furnishing all hardware, materials, and tools necessary to provide complete installations. Additionally, the VENDOR shall be responsible for the installation, configuration, licensing, and support of any associated software packages and/or backend support equipment (e.g., servers), as necessary.

The MOBILITY AUTHORITY will issue Work Authorizations (WA) for all new construction services activities. The VENDOR shall identify all materials and labor necessary to complete the work and provide a price proposal, in accordance with the unit costs in the CONTRACT. Refer to Table 1 for additional information regarding the proposed new construction services anticipated as part of the CONTRACT.

Table 1: New construction services activities for Intelligent Transportation System (ITS) deployment

ITS Field Devices
<p>CCTV Camera, Pan-Tilt- Zoom (PTZ) – installation includes all work to attach device to device pole or structure, route cabling between cabinet and device, install in-cabinet equipment, properly ground system, integrate system into Mobility Authority network and systems, testing; does <u>not</u> include device pole installation.</p> <p>Furnish one (1) Cohu 4261HD camera, or equivalent, and include all necessary components for a complete installation, including camera unit, power-over Ethernet (POE) injector, power</p>

supply, in-line surge protection device (SPD), camera mounting hardware, outdoor-rated CAT-6 Ethernet cabling, power cabling, and ground wire. All cameras shall be capable of H.264 and H.265 video streams and compliant with applicable National Transportation Communications for Intelligent Transportation System Protocol (NTCIP) and Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

CCTV Camera, Fixed – installation includes all work to attach device to device pole or structure, route cabling between cabinet and device, install in-cabinet equipment, properly ground system, integrate system into Mobility Authority network and systems, testing; does not include device pole installation.

Furnish one (1) Cohu 3430HD camera, or equivalent, and include all necessary components for a complete installation, including camera unit, power-over Ethernet (POE) injector, power supply, in-line surge protection device (SPD), camera mounting hardware, outdoor-rated CAT-6 Ethernet cabling (device), power cabling, and ground wire. All cameras shall be capable of H.264 and H.265 video streams and compliant with applicable NTCIP and Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Radar Vehicle Sensing Device (RVSD) – installation includes all work to attach device to device pole or structure, route cabling between cabinet and device, install in-cabinet equipment, properly ground system, integrate system into Mobility Authority network and systems, testing; does not include device pole installation.

Furnish one (1) Wavetronix SmartSensor HD sensor including all necessary components for a complete installation, including radar unit, serial-to-Ethernet media converter (CLICK! series), in-line surge protection device (SPD) (CLICK! series), power supply (CLICK! series), radar unit mounting hardware, proprietary composite cabling (device), power cabling, and ground wire. Ensure all necessary licenses with proprietary vendor software are included, as appropriate. All radar units shall be compliant with applicable NTCIP and Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Dynamic Message Sign (DMS) – installation includes all work to attach device to butterfly, cantilever, or overhead sign structure, route cabling between cabinet and device, install in-cabinet equipment, properly ground system, integrate system into Mobility Authority network and systems, testing; does not include structure installation.

Furnish one (1) Daktronics VF-2420-80-352-20-RGB front-access, full matrix color display including all necessary components for a complete installation, including front-access sign housing, in-cabinet rack-mounted controller unit (Vanguard VFC series), in-sign auxiliary controller panel, twelve-count fiber optic patch panel with matching connector panel, proprietary composite cabling (device), power cabling, and ground wire. Ensure all necessary licenses with proprietary vendor software (e.g., Vanguard) are included, as appropriate. All DMS shall be compliant with applicable NTCIP, Manual on Uniform Traffic Control Devices

(MUTCD), and Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Wrong Way Vehicle Detection System (WWVDS) - installation includes all work to install complete pole assemblies (4X) for with concrete foundation, reinforcement, conduit sweeps, and transformer bases; attach all system componentry to pole assemblies, route cabling between cabinet and device, install in-cabinet equipment, properly ground system, integrate system into Mobility Authority network and systems, testing.

Furnish one (1) complete ramp assembly system, including all necessary components for a complete installation with two (2) sets of signs on both sides of the ramps for a total of four sites per ramp, including aluminum pole assemblies with transformer base, "WRONG WAY" (R5-1a) sign panels, red rectangular rapid flashing beacon (RRFB) light bars, thermal imaging sensors, high-definition verification cameras, LED illuminators, controller cabinet assembly, proprietary cabling (device), power cabling, and ground wire. Ensure all necessary licenses with proprietary vendor software (e.g., Blinkerbeam) are included, as appropriate. All WWVDS shall be compliant with applicable NTCIP, Manual on Uniform Traffic Control Devices (MUTCD), and Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Connected Vehicle to Everything (C-V2X) Roadside Unit - installation includes all work to attach device to device pole or structure, route cabling between cabinet and device, install in-cabinet equipment, properly ground system, integrate system into Mobility Authority network and systems, testing; does not include device pole installation.

Furnish one (1) C-V2X RSU including all necessary components for a complete installation, including roadside unit (RSU), power-over Ethernet (POE) injector, power supply, in-line surge protection device (SPD), radio mounting hardware, outdoor-rated CAT-6 Ethernet cabling (device), power cabling, and ground wire. Ensure all necessary licenses with proprietary vendor software are included, as appropriate. All RSU shall be compliant with applicable Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Physical Infrastructure

Underground Conduit (2-2") – installation includes all work to install conduit run with two (2) two-inch conduits, including open trench and/or directional bore installation methods, conduit coupling, horizontal-to-vertical sweeps, warning tape, pulling, and grounding tone wire, and conduit fittings to boxes, cabinets, or enclosures.

Furnish underground conduit including all necessary components for a complete installation, including high-density polyethylene (HDPE), and polyvinyl chloride (PVC) conduits of two-inch nominal size, conduit couplers, horizontal-to-vertical sweeps, warning tape, stainless steel conduit straps, weatherheads, pull strings, tone wire with grounding unit, and conduit fittings for box and cabinet entrances. All conduits shall meet the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

Aboveground Conduit – installation includes all work to install two (2) conduits, including underground to aboveground transitions, stainless steel conduit straps, conduit fittings to boxes, cabinets, or enclosures, and weatherheads. Conduit diameter may vary.

Furnish aboveground conduit including all necessary components for a complete installation, including galvanized rigid-metallic conduits, conduit couplers, horizontal-to-vertical sweeps, warning tape, stainless steel conduit straps, weatherheads, pull strings, tone wire with grounding unit, and conduit fittings for box and cabinet entrances. All conduits shall meet the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

Conduit Ductbank (16-2") - installation includes all work to install a concrete encased ductbank with sixteen (16) two-inch conduits, including opening of trench, forming and reinforcement of ductbank, concrete encasement, installation of pull tapes in each conduit, conduit connections to UCVs, sealing of unused conduit knockouts, backfilling trench, and grounding.

Furnish conduit ductbank including all necessary components for a complete installation, including sixteen (16) two-inch concrete encased conduits, warning table, pull strings, tone wire with grounding unit, and conduit fittings for box and cabinet entrances. All conduit ductbank shall meet TxDOT Special Specification 6129 – Concrete Encased Duct Bank and any other applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

Conduit Ductbank is not included in the CONTRACT pricing. Material and installation costs associated with conduit ductbank shall be determined at the time of a Work Authorization.

Underground Cable Vault (UCV) – installation includes all work to install a custom 5 ft x 5 ft concrete UCV meeting TxDOT Special Specification 6130 – Underground Cable Vault and any other applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

Provide a 5 ft x 5 ft precast concrete UCV with a minimum depth of 4 ft and a maximum depth of 5 ft. Each vault wall shall have sixteen (16) conduit knock outs with 2" duct terminators in each knock out. Duct terminators shall be Carlon E297JN, Condux, or equivalent. Vault walls must be compatible with existing concrete ductbank.

Provide UCV with a self-draining bolting system that will secure cover positively in place. Provide double hinged cover with hinges operating freely for 180 degrees. Provide cover with drop handles and torsion assisted opening mechanism. Cover shall be grounded and permanently stamped "Communication". The cover and its frame shall be Vulcan V-6875, Neenah R-6663, or equivalent.

Provide frame with a Neoprene seal measuring 3/4" wide and 3/16" thick. Provide a bonded seal the entire length of each side of the frame contacting cover.

Provide UCV with a graded sump bottom with a minimum 4" weep hole. Provide UCV with heavy duty, non-metallic, and non-corrosive cable racks.

Install vault level and orient the frame normal to surrounding slopes. Slopes may require modification.

UCV is not included in the CONTRACT pricing. Material and installation costs associated with UCV's shall be determined at the time of a Work Authorization.

Ground Box – installation includes all work to install a ground box with an appropriately stamped lid, including finished grade, concrete apron with reinforcement, crushed aggregate subbase, connection of conduits to knockouts, installation of grounding array. Ground box material, type, and size may vary.

Furnish one (1) ground box including all necessary components for a complete installation, including pre-cast polymer concrete box, stamped lid with pull slots and security fastener holes, conduit knockouts, and grounding array. All ground boxes shall meet the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

ITS Device Pole, 40' (8-sided) – installation includes all work to install steel device pole, including concrete foundation with reinforcement, anchor bolts, and conduit sweeps, concrete apron, grounding array.

Furnish one (1) steel device pole including all necessary components for a complete installation, including octagonal (8-sided) steel pole, stiffeners, two-inch threaded cabling entrance nipples, handholes, air terminal, top-mount plate, base plate, anchor bolts, and concrete foundation with reinforcement and conduit sweeps. All steel device poles shall meet the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

ITS Device Pole, 60' (12-sided) with Lowering Device - installation includes all work to install steel device pole, including concrete foundation with reinforcement, anchor bolts, and conduit sweeps, concrete apron, grounding array, lowering device with internal winch.

Furnish one (1) steel device pole including all necessary components for a complete installation, including dodecahedral (12-sided) steel pole, stiffeners, two-inch threaded cabling entrance nipples, handholes, air terminal, base plate, anchor bolts, lowering device with included winch and quick disconnect junction box, and concrete foundation with reinforcement and conduit sweeps. All steel device poles shall meet the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

Cabinet Assembly, Pole Mount – installation includes all work attach cabinet assembly to device pole or structure, including physically securing of cabinet to the structure, attachment

of conduits and cabling entrances, grounding array, terminating wiring and cabling, testing; does not include installation of the pole.

Furnish one (1) Type 336S cabinet assembly (*TxDOT Type 3*) including all necessary components for a complete installation, including aluminum cabinet assembly with 19" EIA/TIA rack, front and rear doors, sunshields (top, sides, and doors), two (2) adjustable shelves, complete power distribution assembly, mounting brackets, and stainless-steel banding. Cabinet shall be provided with a minimum of two (2) standard Type 2 keys. All cabinet assemblies shall meet the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Cabinet Assembly, Ground Mount – installation includes all work attach cabinet assembly concrete foundation, including installation of concrete foundation with reinforcement, conduit sweeps, and anchor bolts, grounding array, terminating wiring and cabling, testing.

Furnish one (1) Type 332/334 cabinet assembly (*TxDOT Type 4*) including all necessary components for a complete installation, including aluminum cabinet assembly with 19" EIA/TIA rack, front and rear doors, sunshields (top, sides, and doors), two (2) adjustable shelves, complete power distribution assembly, and concrete foundation with technician pad. Cabinet shall be provided with a minimum of two (2) standard Type 2 keys. All cabinet assemblies shall meet the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Fiber Optic Communications

Fiber Optic Cabling, 12-Count, Single-Mode - installation includes all work to install fiber optic cabling through conduit pathways, coil minimum 200' slack in vaults and 50' in boxes.

Furnish fiber optic cabling meeting the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

Fiber Optic Cabling, 48-Count Single-Mode – installation includes all work to install fiber optic cabling through conduit pathways, coil minimum 200' slack in vaults and 50' in boxes.

Furnish fiber optic cabling meeting the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

Fiber Optic Cabling, 96-Count Single-Mode – installation includes all work to install fiber optic cabling through conduit pathways, coil minimum 200' slack in vaults and 50' in boxes.

Furnish fiber optic cabling meeting the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.

Fiber Optic Cabling, 144-Count Single-Mode – installation includes all work to install fiber optic cabling through conduit pathways, coil minimum 200' slack in vaults and 50' in boxes.

<p>Furnish fiber optic cabling meeting the applicable requirements of the Texas Department of Transportation (TxDOT) specifications and Traffic Standards.</p>
<p>Fiber Optic Patch Panel, 24-fiber capacity – installation includes all work to install fiber optic patch panel in cabinet with a minimum of one (1) 12-count ST-connector panels, splice trays, connection pigtails to cable with fusion splices (color-to-color), terminate all pigtail fibers.</p> <p>Furnish one (1) fiber optic patch panel including all necessary components for a complete installation, including 19" EIA/TIA rack-mounted enclosure unit (minimum capacity of 24 fibers), singlet ST-connector panels, splice trays, and buffer tube fan-out kits. All fiber optic patch panels shall meet the applicable Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.</p>
<p>Fiber Optic Patch Panel, 96-fiber capacity – installation includes all work to install fiber optic patch panel in cabinet with a minimum of four (4) 12-count ST-connector panels, splice trays, connection pigtails to cable with fusion splices (color-to-color), terminate all pigtail fibers.</p> <p>Furnish one (1) fiber optic patch panel including all necessary components for a complete installation, including 19" EIA/TIA rack-mounted enclosure unit (minimum capacity of 96 fibers), singlet ST-connector panels, splice trays, and buffer tube fan-out kits. All fiber optic patch panels shall meet the applicable Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.</p>
<p>Fiber Optic Connection, Fusion Splice</p>
<p>Fiber Optic Connection, Connectorized Termination</p>
<p>Fiber Optic Splice Enclosure – Furnish one (1) splice enclosure including all necessary components for a complete installation, including hardened underground splice enclosure with a minimum of four (4) cabling entry ports capable of accommodating a 144-count fiber optic cable and four (4) splice trays. Provide minimum of two (2) splice trays with each enclosure. All fiber optic splice enclosures shall be compliant with applicable Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.</p>
<p>In-Cabinet Equipment</p>
<p>Managed Field Ethernet Switch – installation includes all work to install the switch, including configuration of network parameters (e.g., IP addressing, routing tables, VLAN settings, etc.), SFP transceivers, power supply, and end-to-end network connectivity testing.</p> <p>Furnish one (1) Cisco IE 4000 series switch including all necessary components for a complete installation, including network switch with a minimum of twelve (12) RJ-45 copper ports and two (2) fiber optic ports, minimum of two (2) small-form factor pluggable (SFP) transceivers compatible with Cisco products, power supply (Cisco model), and DIN-rail mounting assembly unit. Ensure all necessary licenses with proprietary vendor software are included, as</p>

appropriate. All managed field Ethernet switches shall be compliant with NTCIP and Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Uninterruptible Power Supply (UPS) with Battery Backup System - installation includes all work to install the UPS head unit, automatic transfer switch (ATS), battery array with wiring harness; ground the system, configure equipment to the network, and perform testing.

Furnish one (1) UPS including all necessary components for a complete installation, including outdoor-rated UPS head unit with network connectivity via RJ-45 (10/100) Ethernet port and SNMP enabled, four (4) 12V 100 Ah batteries, wiring harness, automatic transfer switch (ATS), and mounting hardware for 19" EIA/TIA rack. All UPS shall meet the applicable Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Remote Power Management Unit (RPMU) – installation includes all work to install the RPMU, ground the system, configure equipment to the network, and perform testing.

Furnish one (1) RPMU including all necessary components for a complete installation, including RPMU with a minimum of eight (8) standard NEMA 5-15 120V plugs and network connectivity via RJ-45 (10/100) Ethernet port and SNMP enabled. Ensure the RPMU is capable of being mounted in a 19" EIA/TIA rack and each individual plug is isolated to allow for remote cycling of power. All RPMU shall meet the applicable Texas Department of Transportation (TxDOT) specifications and TxDOT Traffic Standards.

Electrical Power Service

Electrical Power Service - includes all work to establish a new electrical power service, including installation of service disconnect, utility service meter, transformer (step-down, step-up), and distribution panel board, and all associated infrastructure; coordination with the utility service provider; wiring connections, terminations, grounding, and testing.

Furnish one (1) Type D electrical service including all necessary components for a complete installation. At a minimum, the electrical service shall have the following characteristics: a service voltage of 120/240V; a stainless-steel enclosure; a steel pole service support.

Electrical Service Wire - includes all work to install electrical wires through conduit pathways in a manner which will ensure that damage to the installation will not occur. Ensure wire is of sufficient length after installation in the conduit to provide for attachment to the power company service and for termination within the cabinet for which power is required. This shall also include termination of wiring where necessary.

Furnish electrical wire to meet the applicable requirements of the Texas Department of Transportation (TxDOT) Specifications and Traffic Standards.

1.3.3 Design Liaison and Support Services

The VENDOR shall provide technical design review and coordination services, as requested by the MOBILITY AUTHORITY. This work may include, but is not limited to, participation in design workshops, construction plans review, on-site field meetings with stakeholders (e.g., utility service providers, Contractors, TxDOT), document development, and more.

The MOBILITY AUTHORITY will issue Work Authorizations (WA) for all design liaison and support services activities. The VENDOR shall identify all labor necessary to complete the work and provide a price proposal, in accordance with the unit costs in the CONTRACT.

1.3.4 Control of Materials

The VENDOR shall maintain and store all SYSTEM equipment and spare parts at a storage facility provided by the VENDOR. Storage of parts or equipment outside the MOBILITY AUTHORITY'S designated storage area(s) must be approved by the MOBILITY AUTHORITY.

Any equipment purchased by the VENDOR on behalf of the MOBILITY AUTHORITY, using MOBILITY AUTHORITY funds, belongs to the MOBILITY AUTHORITY, and shall be entered into the inventory system maintained by the VENDOR. Upon termination or ending date of the CONTRACT, all MOBILITY AUTHORITY property shall be transferred to the responsibility of the MOBILITY AUTHORITY.

By default, all spare parts or equipment not installed, and operating will be stored at the VENDOR'S facility dedicated to this project. However, the MOBILITY AUTHORITY reserves the right to store devices and/or parts at an independent storage area of its choosing within thirty (30) miles of the TIMC located at 104 N Lynnwood Trail, Cedar Park, TX 78613. The VENDOR is responsible for picking up parts as needed from MOBILITY AUTHORITY storage area(s) under the terms of this CONTRACT.

The VENDOR will maintain and have readily available an up-to-date inventory of all equipment and/or parts that are under the VENDOR'S supervision. Upon request, the VENDOR must be able to produce individual devices shown on the inventory within twenty-four (24) hours of request or replace with a new device at no cost to the MOBILITY AUTHORITY. If the MOBILITY AUTHORITY chooses to do so, it will be the responsibility of the VENDOR to pick up parts as needed under the terms of this CONTRACT and adhere to the response times as listed in this CONTRACT.

Upon request, the VENDOR shall provide an up-to-date inventory report to the MOBILITY AUTHORITY within seventy-two (72) hours of receiving a request. The inventory report must contain, but not be limited to, at a minimum:

1. Manufacturer
2. Model number
3. Descriptive name
4. Quantity
5. Manufacturer serial number

6. Purchase date
7. Current storage location
8. Condition (new, used, damaged, or available for parts)

1.3.4.1 Device Inventory

The VENDOR shall maintain and have readily available an up-to-date inventory of all the MOBILITY AUTHORITY'S equipment that the VENDOR is responsible to maintain and all spare parts and devices in the VENDOR'S or MOBILITY AUTHORITY'S possession. The VENDOR shall provide an inventory management system in accordance with the requirements of **Section 1.3.4 – Control of Materials**. The VENDOR shall be responsible for the procurement, configuration, maintenance, development, and updating of the inventory management system.

1.3.4.1.1 Existing TIMC Device Inventory

The VENDOR shall maintain and have readily available an up-to-date inventory of all the MOBILITY AUTHORITY'S equipment and/or parts within the TIMC and under the VENDOR'S supervision. The inventory shall contain, but not be limited to:

1. Asset ID No. (MOBILITY AUTHORITY)
2. Manufacturer
3. Model number
4. Descriptive name
5. Manufacturer serial number
6. Current location (e.g., server room, operational floor)
7. Current function and/or utilization
8. Condition (new, used, damaged, or available for parts)
9. Equipment status (spare or in-use)
10. Date of purchase
11. Date(s) of repair
12. Date when scrapped (as applicable)
13. Warranty status

1.3.4.1.2 Existing Field Device Inventory

The VENDOR shall maintain and have readily available an up-to-date inventory of all the MOBILITY AUTHORITY'S field devices, equipment, infrastructure, and/or parts that are under the VENDOR'S supervision. The inventory shall contain, but not be limited to:

1. Asset ID No. (MOBILITY AUTHORITY)
2. Manufacturer
3. Model number
4. Descriptive name
5. Manufacturer serial number,
6. Current site location (corridor, milepost, and side of the road)

7. Position (latitude, longitude)
8. Condition (new, used, or damaged), including contextual photos from the latest site visit
9. Equipment status (spare or in-use)
10. Site where equipment belongs and type of site (e.g., CCTV camera, DMS, etc.)
11. Date of purchase
12. Date(s) of repair
13. Date when scrapped (as applicable), and
14. Warranty status

1.3.4.1.3 Inventory Disposal

The VENDOR shall be responsible for monitoring the viability and usefulness of MOBILITY AUTHORITY inventory. When inventory (e.g., field devices, equipment, infrastructure, and/or parts) under the VENDOR'S supervision is determined to have no value, is beyond repair, out of warranty, or beyond useful service life the VENDOR shall label the inventory, physically and in the IMS, as "Disposable". The VENDOR shall dispose of equipment identified within the IMS as disposable at a standard frequency agreed upon by the MOBILITY AUTHORITY no greater than six (6) months. An inventory disposal list must be approved by the MOBILITY AUTHORITY prior to disposal. Recycling shall be the primary method of disposal.

Items with resale or trade-in value that are of no use to the MOBILITY AUTHORITY shall be labeled, physically and in the IMS, as "Commodity". The Vendor shall deliver an annual commodities report detailing the inventory commodities to the MOBILITY AUTHORITY. The report shall include:

1. Manufacturer
2. Model number
3. Descriptive name
4. Quantity
5. Manufacturer serial number
6. Purchase date
7. Current storage location
8. Condition (new, used, damaged, or available for parts)
9. Warranty Status
10. Estimated resale value
11. Potential trade-in options

At the request of the MOBILITY AUTHORITY the VENDOR may be asked to sell or trade-in inventory. All sales must be by competitive bid or auction. All trade-ins must be for new property of a similar type.

All disposal, sale, and trade-in of MOBILITY AUTHORITY inventory must abide by Article 23 of the Mobility Authority Policy Code.

1.3.4.2 Inventory Management System

The VENDOR shall furnish, maintain, configure, support, and populate a full-scale Inventory Management System (IMS) to support the long-term ITS asset and configuration management needs of the MOBILITY AUTHORITY. The IMS shall include configurable databases and a web-accessible user interface to allow users to access the system remotely. Access to the IMS shall be restricted to pre-approved users via username and password. All users shall be vetted by both the MOBILITY AUTHORITY and VENDOR prior to receiving access to the system. The MOBILITY AUTHORITY'S Project Manager shall remain a pre-approved user with full access to the IMS for the duration of this CONTRACT.

The VENDOR shall use the IMS for inventory and facilities management purposes. The VENDOR will be responsible for the operations and maintenance of all data used to inventory the SYSTEM field equipment and parts including, but not limited to, ITS devices; enclosures, cabinets, communication hubs, and the devices within; network equipment; electrical service equipment; communication cabling; ductbank; conduit; underground boxes and UCVs; communication connection points (e.g., splice, terminations); connection hardware; and other field installed assets. The VENDOR shall document as-built information about the SYSTEM and work performed under this CONTRACT which shall be made available to the MOBILITY AUTHORITY at all times.

The information contained within the IMS is confidential material; therefore, the VENDOR must ensure that VENDOR staff working under this CONTRACT have been pre-approved. The VENDOR shall be responsible for providing user training on the IMS and assign appropriate login credentials to VENDOR staff and MOBILITY AUTHORITY staff and designees that successfully complete training.

The VENDOR shall provide an IMS that is accessible from the field. The VENDOR shall provide field staff with a compatible laptop computer with direct Internet access from anywhere within the MOBILITY AUTHORITY system. Asset changes to the system shall be updated to the IMS database in real-time or as otherwise directed by the MOBILITY AUTHORITY. The VENDOR will be responsible for recurring usage cost including computer hardware, software licenses, data usages for connection to the Internet, etc.

The VENDOR shall include all necessary resources required to populate the database and routinely update the database as maintenance work changes the inventory and configuration. Information populated in the IMS shall meet the positional accuracy requirements of differential global positioning systems (D-GPS).

1.4 GENERAL REQUIREMENTS FOR EXECUTION OF WORK

The VENDOR is responsible for all labor, materials, and incidentals required to execute and complete the requirements of this CONTRACT including, but not limited to, the following:

1. Project management and contract administration

2. Communications and coordination between the MOBILITY AUTHORITY and the VENDOR
3. Communications and coordination with other MOBILITY AUTHORITY maintenance providers (e.g., performance-based roadway maintenance contractor, Toll Systems Integrator (TSI))
4. Communications and coordination with other stakeholder(s) (e.g., TxDOT, City of Austin, CapMetro, third-party contractors and vendors)
5. Personnel requirements
6. Project recordkeeping
7. Device availability matrices
8. WA requirements for payment of services
9. Status meetings, including meeting minutes and agendas
10. Utility locate administration
11. Scheduled and preventive maintenance
12. Minor and major repairs and parts replacement (including warranties and replacement parts)
13. New construction and installations
14. Design support services
15. Material and equipment requirements
16. Utility coordination for network and utility services
17. Emergency power, and
18. Disaster reporting

The VENDOR shall be responsible for obtaining any and all necessary subconsultants to perform specialty work (e.g., geotechnical boring), as necessary.

The VENDOR shall fully cooperate with all utility owners during activities such as, but not limited to, construction, installation, or repair associated with this CONTRACT. The VENDOR shall call Texas811 a minimum of forty-eight (48) hours and a maximum of ninety-six (96) hours before any excavation work requiring locate services from member operators of Texas811.

The VENDOR shall furnish and install all equipment and materials and perform all work in accordance with all applicable standards and procedures (refer to **Section 1.1.2 – Applicable Specifications and Standards**). The VENDOR is responsible for ascertaining the exact location of all utilities prior to beginning work in an area. Utility locations as shown on plans are approximate and may not include all utilities. If any utility damages are incurred as a result of VENDOR'S operations, it shall be the VENDOR'S sole responsibility to repair such damages or bear the cost of repairs performed by others.

The VENDOR shall be responsible for coordinating all scheduled and preventative maintenance, repairs, and emergency maintenance activities with the Toll Systems Integrator (TSI) where equipment or infrastructure is collocated, or existing tolling equipment is in the immediate proximity and may be impacted. The VENDOR may be required to have a representative of the TSI on-site during maintenance activities, at the discretion of the MOBILITY AUTHORITY. Communication between parties shall be coordinated through the Project Manager.

The VENDOR shall be responsible for coordinating and meeting with all utility companies having overhead or underground facilities in proximity with work performed under this CONTRACT. The VENDOR shall be responsible for determining and performing any needed subsurface utility exploration (SUE) work.

The VENDOR shall be responsible for providing the MOBILITY AUTHORITY with a detailed damage report after the occurrence of a disaster, natural or otherwise (e.g., vehicle collision). This report shall include an individual site analysis including, but not limited to, the following information:

- Field device or equipment location
- Date and time of visit
- Description of failure or issue and system impacts
- Site conditions noted (e.g., submerged, structure down, no power)
- Digital photo documentation
- Damaged parts list: type, model, and serial and control numbers
- Needed parts list, including reference to needed parts/devices currently in inventory
- Repair cost breakdown
- General notes, and
- Schedule of repair duration

The damage report by the VENDOR shall be per site and include all devices connected to the cabinet location. The VENDOR'S report shall include an Executive Summary and a Cost Summary including all parts necessary to re-establish the system in working order. In the event the damage requires the services of a subcontractor, the VENDOR shall include a short-list of quotes from at least three (3) different subcontractors, subconsultants, or sub-vendors. The MOBILITY AUTHORITY shall establish time frames for damage reports to be delivered to the MOBILITY AUTHORITY depending on the severity of the disaster.

1.4.1 Location of the Work

The VENDOR shall be responsible for maintenance of all existing, under-construction, and future MOBILITY AUTHORITY owned and operated SYSTEMS located in the following counties:

- Hays, Travis, and Williamson Counties

1.4.1.1 Traffic Incident Management Center (TIMC)

The VENDOR is to provide scheduled and preventative, repair, and emergency maintenance services for applicable components of the SYSTEM located within the TIMC. The VENDOR shall not be responsible or attempt to perform maintenance on any collocated electronic tolling or revenue generating equipment within the TIMC, including the server room unless otherwise approved by the MOBILITY AUTHORITY. The VENDOR shall coordinate with the MOBILITY AUTHORITY and Toll Systems Integrator (TSI) to determine specific requirements for equipment located within the TIMC and schedule maintenance periods.

Example work to be performed by the VENDOR within the TIMC includes, but is not limited to:

- Parts-only replacement warranty from the manufacturer registered in the MOBILITY AUTHORITY'S name
- Diagnostic and/or troubleshooting maintenance visits (e.g., video wall alignment, configuration, and color balance)
- Scheduled preventative maintenance visits (e.g., clean or replace air filters, clean screens)
- Repair service for video wall, servers, and operator workstation components. Repair work is to be coordinated with the MOBILITY AUTHORITY to determine the level of response/repair needed and scheduled downtime
- Video wall controller, software, and firmware upgrades
- Video wall servers
- Video wall displays (e.g., televisions, monitors)
- Workstation computer, monitor, software, and firmware upgrades
- Central servers

1.4.1.2 Field Sites

The VENDOR is to provide preventative and scheduled maintenance, emergency maintenance, and repair services for components of the SYSTEM located at existing and future field sites throughout the geographic coverage area of the CONTRACT.

1.4.2 Scheduling and Execution of Work

All work shall be scheduled with and approved by the MOBILITY AUTHORITY, including schedule and preventative maintenance, repairs, emergency maintenance, and new construction activities. The VENDOR shall work with the MOBILITY AUTHORITY'S Project Manager under this CONTRACT to establish recurring scheduled activities (e.g., preventative maintenance) and timelines. Additional work not covered under the Scope of Work (SOW) must be reviewed, approved, and authorized by the MOBILITY AUTHORITY.

The VENDOR will perform all SYSTEM support, including routine and preventative maintenance; repairs; utility locate services; and failed or destroyed component replacement, as needed by the MOBILITY AUTHORITY. The VENDOR may be required to perform new field device, equipment, and infrastructure installations; and design liaison and support services, as needed. All services will be performed on a WA basis.

The MOBILITY AUTHORITY will issue WAs to approve the VENDOR to work on any and all services on the SYSTEM directed by the MOBILITY AUTHORITY. Work estimates will be prepared by the VENDOR for all WAs, in accordance with the CONTRACT, and submitted to the MOBILITY AUTHORITY for review and approval. The work estimates will include, at a minimum, personnel, labor rates, materials, equipment and/or resources; documentation of proposed work to be performed; potential impacts to tolling systems and revenue, roadway, and users; travel requirements if outside the contract area; itemized cost breakdown; and proposed work

schedule. No work will be undertaken by the VENDOR unless it has been authorized in writing from the MOBILITY AUTHORITY. Each Work Authorization issued by the MOBILITY AUTHORITY will serve as a formal notice-to-proceed (NTP) and may include an effective time period for the particular Work Authorization being issued.

1.4.3 Mobilization

Work under this contract will require movement of personnel, equipment, supplies, and incidentals. All preparatory work and operations for beginning work, including movement of personnel, equipment, supplies, and other incidentals for a project (one Work Authorization), must be authorized by the MOBILITY AUTHORITY. Mobilization shall be compensated as five percent (5%) of the total proposed installation unit costs. Due to the unique nature of the CONTRACT and the work specified herein, mobilization may be adjusted by the MOBILITY AUTHORITY as needed on a case-by-case basis.

1.4.4 Temporary Traffic Control

Temporary Traffic Control (TTC) shall include the planning, furnishing, installing, maintaining, and removing of traffic control and safety devices. The need for lane closures shall be determined on a case-by-case basis as requested by the VENDOR. Any request for a planned lane closure(s) shall be submitted to the MOBILITY AUTHORITY a minimum of two (2) weeks in advance of the proposed lane(s) closure and coordinated with the Toll Systems Integrator (TSI), as appropriate. The VENDOR will be given a notification list by the MOBILITY AUTHORITY containing all contacts that shall be notified of the lane(s) closure by the VENDOR. The VENDOR shall coordinate TTC activities with traffic incident management center (TIMC) operations personnel and any other governing operations center that may be impacted (e.g., City of Austin, TxDOT).

The VENDOR shall have at least one (1) individual on its staff throughout the term of this CONTRACT with the appropriate Texas Department of Transportation (TxDOT) approved training, as outlined in TxDOT Standard Specifications, Item 7.

All system maintenance related TTC activities shall be compensated by the monthly Maintenance Service Unit Price, refer to the CONTRACT. All Work Authorization related TTC activities shall be compensated on an as needed basis. Under a Work Authorization, the VENDOR shall identify all materials and labor necessary to complete the work and provide a price proposal to the MOBILITY AUTHORITY for review and approval.

1.4.5 Warranty for Vendor Services and Materials

The VENDOR warrants to the MOBILITY AUTHORITY that all services, materials, parts, and supplies furnished under this CONTRACT shall be free from defects in material or workmanship and in accordance with good trade practices and local, state, and federal codes.

The VENDOR guarantees that upon completion of the services required by the CONTRACT, the work areas shall be left in a clean, sanitary, and safe condition.

The VENDOR agrees that each job assignment performed will be reviewed and approved by the VENDOR'S Project Manager before the MOBILITY AUTHORITY is requested to approve and process invoices for payment.

The VENDOR will correct deficient work and replace defective material provided and supplied, or credit the MOBILITY AUTHORITY for the inadequate services and materials. The MOBILITY AUTHORITY shall have the right to determine which course of correction must be taken.

Upon completion of a repair, the VENDOR shall warranty their work for a period of ninety (90) calendar days from the date of acceptance by the MOBILITY AUTHORITY. The VENDOR shall transfer manufacturer's warranties for parts and materials to the MOBILITY AUTHORITY upon completion of the necessary repairs and acceptance by the MOBILITY AUTHORITY.

1.4.6 Lost, Stolen, or Damaged MOBILITY AUTHORITY Owned Resources

The MOBILITY AUTHORITY'S Project Manager will provide a list of MOBILITY AUTHORITY owned resources for the VENDOR. The VENDOR shall acknowledge receipt and responsibility of the MOBILITY AUTHORITY owned resources by executing a Property Transfer Receipt form (<https://fmx.cpa.texas.gov/fmx/forms/spa/spaprotransrcpt.pdf>).

The VENDOR will inventory all MOBILITY AUTHORITY owned resources annually and provide the data to the MOBILITY AUTHORITY in a pre-approved format for review and record retention. The MOBILITY AUTHORITY may audit the inventory data at their own discretion. In the event MOBILITY AUTHORITY owned resources have been lost, stolen, or damaged, and had been in exclusive possession and control of the VENDOR, the VENDOR will replace the MOBILITY AUTHORITY owned resources before the end of the calendar year when the item(s) was known to be lost, stolen, or damaged. If the item(s) is not directly replaceable due to non-availability of identical models, the VENDOR will replace the item(s) with a functionally equal or better item or directly compensate the MOBILITY AUTHORITY. The risk of loss to any equipment being repaired or replaced shall be the responsibility of the VENDOR having possession or control of the equipment at the time of the loss.

1.4.7 Materials to be Furnished

All equipment and component parts that are furnished will be new, unused, will meet all requirements of this CONTRACT, and will be in operable condition at the time of delivery. All parts will be of high-quality workmanship and no part or attachment will be applied contrary to the manufacturer's recommendations or standard practice. If authorized by the MOBILITY AUTHORITY, cannibalized parts from damaged MOBILITY AUTHORITY equipment may be used if it does not affect a warranty.

1.4.8 Software

The VENDOR is expected to use, purchase, or provide the following software available for the performance of work described in the contract: inventory management system (IMS) software, network management system (NMS) software, proprietary software for field devices (as necessary), video management software, database management software, as well as Rekor One and SWRI Lonestar proprietary central management software(s).

1.4.9 Incidental Materials

The VENDOR shall be responsible for providing incidental materials that are necessary to perform the general nature of work described in this CONTRACT.

1.4.10 Equipment, Machinery, Tools, and Vehicles

The VENDOR shall provide on-site equipment including, but not limited to, bucket trucks, cranes, inspection/maintenance vehicles, field engineering equipment, air compressor, machinery, tools, materials, cellular phones, laptops, and other equipment necessary to perform the service required under this CONTRACT.

The VENDOR shall provide a bucket truck capable of reaching a minimum height of 40 feet for regular use under this CONTRACT. In addition, the VENDOR shall be able to provide a bucket truck capable of reaching 55 feet within twenty-four (24) hours of request by the MOBILITY AUTHORITY.

The VENDOR shall provide maintenance and inspection vehicles for the ITS Project Manager, ITS Maintenance Technician(s), Electrical Technician(s), and Utility Technician(s). The VENDOR shall provide the availability of an environmentally controlled van or trailer accustomed for conducting fiber optic fusing splicing and other similar type of work inside the van or trailer, within forty-eight (48) hours of the request of the MOBILITY AUTHORITY. All vehicle(s) shall have sufficient towing and hauling capabilities to carry out the tasks specified in this CONTRACT.

VENDOR logos shall be required on vehicles and equipment dedicated for use and performance of work under this CONTRACT. VENDOR vehicles that are regularly used to perform work under the CONTRACT must have the following markings: VENDOR logo and any other safety messages required for vehicles stopping on limited-access facilities to conform to all safety agency regulations. Vehicles shall be outfitted with the appropriate strobe and safety lights required to perform their field duties.

The VENDOR shall be responsible to provide a laptop computer with docking station and off-site internet access for each primary maintenance staff member. The laptop shall be compatible with the MOBILITY AUTHORITY'S network and include all appropriate software(s) to configure, monitor, and manage the SYSTEM. Computers and individuals using MOBILITY AUTHORITY technology resources shall comply all cyber-security, data privacy, and use of information and technology resources policies of the MOBILITY AUTHORITY.

The VENDOR shall be responsible to provide smartphones to field personnel in order for the MOBILITY AUTHORITY to immediately reach staff in the field. The VENDOR shall provide the MOBILITY AUTHORITY with a complete contact list of all key personnel including mobile phone numbers for all field staff. Smartphones provided to VENDOR field personnel shall be capable of capturing and transmitting high-resolution photographs (e.g., 300 pixels per inch).

The cost of the machinery, equipment tools, and vehicles including, but not limited to pliers, multi-meters, crimp tools, screwdrivers, crowbars, ground box pull hooks, conduit snakes, ratchets, hammers, shovels, battery or electrical power tools, Ethernet packet sniffers, laptop computers, smartphones, video monitors, vehicles, etc., shall be the VENDOR'S responsibility. The VENDOR shall be responsible for maintaining their equipment, machinery, tools, and vehicles, and all fixed and recurring costs for these items throughout the term of this CONTRACT.

VENDOR shall be responsible to provide suitable equipment (e.g., pull box hook, manhole cover hook) to field personnel for the opening of UCVs. Under no circumstances shall anyone attempt to open a UCV by hand or with the use of wire.

All measurement equipment and tools shall be calibrated by the manufacturer's certified calibrator and be calibrated on the frequency required by the manufacturer. These equipment and tools include, but are not limited to:

- Maintenance trucks with oscillating buckets
- OTDR
- Oscilloscopes
- Waveform and video generators
- Multi-meters, and
- Earth ground testers

The MOBILITY AUTHORITY may, at its sole discretion, provide certain maintenance and measurement tools/equipment for the VENDOR to use under this CONTRACT.

The VENDOR shall maintain and inventory all equipment and tools associated with this CONTRACT, including items provided by the MOBILITY AUTHORITY. The VENDOR shall ensure that all warranties remain valid on all equipment and that they are properly calibrated for the duration of the CONTRACT.

1.4.10.1 Control of Equipment

The VENDOR shall maintain and store equipment associated with this CONTRACT at the VENDOR's facility or other location(s) approved by the MOBILITY AUTHORITY. Storage locations shall be marked specifically for this CONTRACT and shall not be used for any other purposes. Parts or equipment to be stored outside the MOBILITY AUTHORITY storage area shall be authorized by the MOBILITY AUTHORITY'S Project Manager; by default, all spare parts or equipment not installed and operating shall be stored at the storage area dedicated to this project as approved by the MOBILITY AUTHORITY.

The VENDOR shall secure a new storage container(s), as necessary, under this CONTRACT to store spare parts at the location(s) approved by the MOBILITY AUTHORITY. The MOBILITY AUTHORITY may elect for the VENDOR to pick-up and deliver parts as needed to locations in the geographic coverage area of this CONTRACT.

1.4.11 Working Hours, On-Call Responsibilities, and Response Times

1.4.11.1 Standard Hours of Operation

The VENDOR shall have maintenance personnel available at all times including nights, weekends, and holidays. However, standard hours of operation are Monday through Friday from 6:00 a.m. – 7:30 p.m.

1.4.11.2 On-call Responsibilities

The VENDOR shall provide on-call staff at all times. On-call staff assignments shall be coordinated with the MOBILITY AUTHORITY and clearly communicated to staff responsible for TIMC operation. Qualified maintenance staff shall be on-call during weekends and statutory state holidays and at all times for the term of this CONTRACT to respond to calls and issues, as needed. The VENDOR may be required to perform repairs and emergency maintenance outside of normal business hours.

1.4.11.3 Response Times

The response times below require that qualified VENDOR staff with appropriate equipment, tools, and available parts be on-site and ready to perform work for repair services and emergency maintenance, as necessary. Response times are intended to identify the maximum allowable time for VENDOR personnel to acknowledge the maintenance need, mobilize staff on-site to assess the issue(s), perform diagnostic and/or troubleshooting efforts, perform corrective action for minor repairs or identify proposed work strategies to correct the issues for major repairs, and communicate the current situation with the MOBILITY AUTHORITY.

The VENDOR is expected to be readily available and responsive throughout the duration of the CONTRACT. The VENDOR shall respond to communications and requests from the MOBILITY AUTHORITY for non-critical activities (e.g., troubleshooting, diagnostics, general communications) no later than one (1) business day (state holidays excluded), unless otherwise deemed necessary by the MOBILITY AUTHORITY.

1.4.11.3.1 Repair Services Response Time

Response times for repair services, as identified in **Section 1.3.1.3 – Repair Services**, shall be no later than seventy-two (72) hours to the site, unless otherwise deemed necessary by the MOBILITY AUTHORITY.

1.4.11.3.2 Emergency Repair Response Time

Response times for emergency maintenance, as identified in **Section 1.3.1.4 – Emergency Repair Services**, shall be no later than four (4) hours to the site 24 X 7 X 365, unless otherwise deemed necessary by the MOBILITY AUTHORITY.

1.4.12 Security and Safety Requirements

The VENDOR shall utilize proper safety measures to ensure the proper protection for persons and property at all times.

The VENDOR shall be responsible for ensuring that all equipment used is maintained in a safe and efficient manner in accordance with all local, state, and federal laws, safety organizations, regulations, and guidelines pertaining to providing the required services.

The VENDOR shall follow all safety requirements outlined in the National Electric Safety Code (NESC), Occupational Safety and Health Administration (OSHA), and any standards or practices for safe installation or maintenance of required equipment per this CONTRACT.

The VENDOR shall be responsible for any injury to person(s) or damage to property that occurs as a result of VENDOR activities under this CONTRACT. The VENDOR shall notify the MOBILITY AUTHORITY immediately after any injury incurred by person(s) working under this CONTRACT.

At the conclusion of a workday, the VENDOR'S personnel must leave the work area free of safety hazards. The VENDOR shall remove all trash, personal belongings, debris, and unwanted items from the site at the end of each workday. The MOBILITY AUTHORITY assumes no liability for any equipment, personal belongings, or effects left unattended on MOBILITY AUTHORITY property.

The VENDOR shall be solely responsible for the safety of all its personnel.

The VENDOR shall be solely responsible for maintaining the safety required and providing safety equipment and procedures for the protection of employees and the public throughout the area(s) where work is performed under this CONTRACT.

If any deficiency may cause harm to life or property, or violate any rules or regulations such as, but not limited to, Americans with Disabilities Act (ADA), OSHA, or otherwise contained herein, the MOBILITY AUTHORITY may take immediate corrective action(s), and the VENDOR shall be responsible for the burden of any associated direct and/or indirect costs.

1.4.13 License and Insurance Qualifications

The VENDOR shall hold the licenses and certifications necessary to provide the services described in this CONTRACT in the counties specified and be required to submit proof of licenses and certifications prior to work being performed.

The VENDOR shall certify that skilled employees and/or subcontractor(s), who possess the necessary specialty licenses, as required by law to perform the work, shall provide the services being performed and provided by the VENDOR as described in this CONTRACT.

All records, insurance, and licenses must be current. The VENDOR must provide the MOBILITY AUTHORITY with evidence of current records, insurance, and licenses and copies must be kept on file for the duration of this CONTRACT and all renewals.

1.5 REQUIRED QUALIFICATIONS OF VENDOR

1.5.1 Use of Subcontractor(s) or Subconsultant(s)

The support of the SYSTEM may require a multi-disciplinary team made up of a prime VENDOR and subcontractors to successfully fulfill the obligations of this CONTRACT. The VENDOR must provide contact information for all subcontractors and indicate their areas of expertise and responsibility. Use of subcontractors must be coordinated with, and approved by, the MOBILITY AUTHORITY's Project Manager.

1.5.2 Staffing Requirements

Support of the SYSTEM will require a multi-disciplinary team. The following areas of expertise are considered to be the minimum necessary to successfully fulfill the obligations of this CONTRACT. Subcontractors submitted with the response are allowed.

- Project management / administration
- Electrical trades
- Electronic and electro-mechanical component diagnostics, troubleshooting, and repair
- Computer hardware troubleshooting and repair
- Layer 2/3 local area network (LAN) and wide area network (WAN) design, operation, and maintenance
- Ethernet, serial, and wireless communications
- Networking and network protocols, including switching, routing, VLANs, OSPF, PIM, SNMP, IGMP, IGRP, DVMRP, DNS, etc.
- Computer applications / database management
- Cyber-security
- Digital video transmission
- Fiber optic network configuration and administration
- Fiber optic cabling termination, splicing, testing, and management
- Installation, configuration, troubleshooting, and maintenance of digital video equipment (e.g., CCTV), network communication devices, DMS, RVSD, WWVDS, RWIS, Connected Vehicle (CV) technology, and vehicle detection systems (VDS)
- ITS design and plans production
- Review of civil construction plans

- Grounding and surge protection systems and related equipment
- Configuration management
- Database management
- Security devices for SYSTEM installations
- Installation of ITS device poles and structural supports
- Installation and maintenance of roadside infrastructure including cabinets, conduit, and ground boxes
- Temporary Traffic Control (TTC)

The VENDOR shall keep a staff of the required levels to respond to all requirements of this CONTRACT at all times during the term of the CONTRACT. The VENDOR shall have the option to provide the same dedicated maintenance staff on-site full-time in the MOBILITY AUTHORITY'S designated location(s). The VENDOR shall develop a staffing plan indicating how absences and vacations will be covered, and the expected activities of each proposed staff member. The VENDOR shall provide suitable replacement staff during vacations or sick periods of primary staff.

The MOBILITY AUTHORITY will conduct VENDOR performance reviews on an annual basis. When deficiencies are identified with VENDOR employees assigned to the CONTRACT, the VENDOR will immediately implement remedial action. Remedial actions may include further training of the employee, subdivision or reassignment of the employee, addition of staff, and removal of the employee from the CONTRACT. All VENDOR employees working on this CONTRACT are understood to be working under the direction and at the will of the MOBILITY AUTHORITY Project Manager.

1.5.3 Maintenance Staff Location and Availability

VENDOR staff whose primary function is performing work associated with this CONTRACT shall be located within the geographic coverage area designated by the MOBILITY AUTHORITY. The VENDOR may supply additional skilled staff from other locations, as requested by the MOBILITY AUTHORITY. The MOBILITY AUTHORITY may provide workspace at MOBILITY AUTHORITY locations within the geographic coverage area at no cost, at the direct discretion of the MOBILITY AUTHORITY. The VENDOR must coordinate staff locations and schedules with the MOBILITY AUTHORITY'S Project Manager and provide updates within five (5) business days, as necessary.

1.5.4 Vendor Facilities

The VENDOR shall provide a facility in order to maintain and store the MOBILITY AUTHORITY'S SYSTEM equipment or spare parts, in a location approved by the MOBILITY AUTHORITY. The facility must be located within thirty (30) miles of the TIMC located at 104 N Lynnwood Trail, Cedar Park, TX 78613. This location shall be marked specifically for this CONTRACT and shall not be used for any other purposes, unless otherwise approved by the MOBILITY AUTHORITY. This location will be temperature and humidity controlled, provide restricted access (log in/out of personnel), require logging in and out of parts and equipment by an individual, and be separate

from any other general use warehouse area(s). A copy of the checkout procedures and security system is required to be presented to the MOBILITY AUTHORITY for approval.

1.5.5 Position Descriptions

The VENDOR-provided key personnel roles are listed below and shall collectively have the areas of expertise mentioned above in **Section 1.5.2 – Staffing Requirements**. The final quantities of each position shall be determined during the CONTRACT negotiations and agreed upon by the VENDOR and the MOBILITY AUTHORITY. The VENDOR and/or MOBILITY AUTHORITY shall have the ability to add staff that is not defined herein, at any time under the term of this CONTRACT, as requested by the project requirement and staffing needs change.

The VENDOR must provide resumes for all key personnel proposed for this CONTRACT as part of the proposal package. Any changes to the key personnel identified in the proposal package submitted by the VENDOR shall be subject to review and approval by the MOBILITY AUTHORITY in writing before any billable services are authorized. Requests to add or change staff must be accompanied with accurate and current resumes for proposed individuals, including information on their licenses and certifications as well as a description of their expected duties.

ITS Project Manager

The VENDOR shall designate an ITS Project Manager who shall respond to all authorizations for services to the SYSTEM under this CONTRACT. The VENDOR'S ITS Project Manager shall be responsible for all work necessary to provide for the general management, oversight, quality control, and administration of all CONTRACT activities and support personnel. The VENDOR'S ITS Project Manager ensures that the requirements of the CONTRACT are met on a daily basis at all times. The ITS Project Manager is responsible for ensuring that maintenance activities supporting the SYSTEM are in accordance with this CONTRACT, Standard Operating Procedures (SOP), protocols, and policies.

The responsibilities include, but are not limited to, the following:

- Provide oversight of all work performed under this CONTRACT
- Follow direction set by the MOBILITY AUTHORITY'S Project Manager
- Perform project-related assignments to include the planning, organizing, and developing of complicated tasks as assigned by the MOBILITY AUTHORITY
- Direct oversight of project professionals and staff
- Direct training and indoctrination of workers to improve performance and acquaint workers with CONTRACT requirements, policies, and procedures
- Recommend changes, review progress, and approve work products for the maintenance program
- Recommend ITS equipment specifications and assist in developing operating procedures for ITS devices
- Represent the MOBILITY AUTHORITY in meetings for design and/or construction phases of projects, utility coordination, and others as directed

- Requisition tools, spare parts, equipment, and supplies required for maintenance operations
- Train assigned staff in proper work methods and techniques and in the set up and use of equipment
- Monitor allocated budget for spare parts and supplies and manage spare parts consumption and usage to ensure that budget levels are met
- Track project budget, inventory, and tasks assigned, and provide monthly updates, status of work, and cost summaries
- Prepare and submit monthly invoices, progress reports, and other documents within ten (10) business days of each month's end
- Provide sufficient staff and resources for all tasks and activities throughout the duration of the CONTRACT
- Ensure that maintenance staff have the required qualifications and background check documentation before being employed by the VENDOR
- Meet on a bi-weekly basis with the MOBILITY AUTHORITY'S Project Manager to review and discuss tasks completed during the previous week, task assignments for the current week, and two-week "look ahead" schedule
- Provide summary minutes within one (1) week after each meeting for review and approval by the MOBILITY AUTHORITY
- Coordinate activities of workers repairing, upgrading, modifying, or installing equipment or systems in order to improve existing equipment
- Interact with the MOBILITY AUTHORITY management, operations personnel, staff, and consultants to review issues pertaining to equipment or systems performance and status
- Perform other tasks as assigned by the MOBILITY AUTHORITY

Coordinator/Administrative Assistant

The Coordinator/Administrative Assistant position is responsible for supporting the VENDOR'S maintenance staff and MOBILITY AUTHORITY'S Project Manager on day-to-day business matters regarding maintenance services and utility locate coordination. The Coordinator/Administrative Assistant shall possess, but not be limited to, the following qualifications:

- Supplies administrative support services to the maintenance staff and assumes the role as an administrative liaison with internal and/or external sources
- Performs routine office or clerical support tasks according to well-established procedures. Examples of work performed may include scheduling of meetings; coordination between stakeholders; recording meeting minutes; establishing meeting agendas; control and organization of documentation; quality control and assurance; photocopying, filing, posting, or proofing data; or answering telephone calls
- Work performed may also include composing routine correspondence, preparing routine reports, scheduling appointments, screening and directing incoming calls, providing information, maintaining files, or transcribing dictation

- Prepares documents using Microsoft® applications; formats, proofs, edits for errors
- Assists ITS Project Manager on the data entry of the IMS
- Monitoring of scheduling, field activities, and all other deadlines and requirements of this CONTRACT
- Performs other tasks as assigned by the MOBILITY AUTHORITY

Technical Design Lead

The position will be responsible for representing the interests of the MOBILITY AUTHORITY for technical matters related to the SYSTEM, including the review and development of technical engineering and design documents. This individual shall be a subject-matter expert with related project experience in the design, installation, integration, testing, and maintenance of field devices, networking equipment, electrical systems, and associated infrastructure. The Technical Design Lead may be required to represent the MOBILITY AUTHORITY in meetings for ongoing or future construction projects, including on-site meetings, as necessary. This role shall be capable of developing technical design documents, including but not limited to, construction plans, technical specifications, as-built drawings, schematics, installation and maintenance documentation, testing plans, and Systems Engineering documents.

The responsibilities and duties may include, but are not limited to, the following:

- Represents the MOBILITY AUTHORITY in design, construction, integration, testing, utility, and other technical focused meetings
- Reads diagrams, plan sets, manuals, and specifications for new installations and continued maintenance of SYSTEM devices; makes corrections to schematics and plan sets, as necessary
- Designs elements of the SYSTEM, including field devices, networking equipment, electrical systems, and associated infrastructure and provides experience in the design and deployment of fiber optic and wireless communication technology, CCTV cameras, Dynamic Message Signs (DMS), Wrong Way Vehicle Detection Systems (WWVDS), and vehicle detection sensor technology
- Develops technical documents, including but not limited to Systems Engineering, technical specifications, construction plans, as-built drawings, installation schematics, testing plans, design standards, minimum technical requirements
- Performs technical plans and document reviews on behalf of the MOBILITY AUTHORITY
- Updates existing conditions information as SYSTEM
- Documents work performed on all SYSTEM devices, including real-time updates to the IMS
- Evaluates new technology and introduces creative solutions for the SYSTEM
- Interacts with the MOBILITY AUTHORITY management, operations personnel, staff, and consultants to review issues pertaining to equipment or systems performance and status

ITS Maintenance Technician(s)

The ITS Maintenance Technician shall be responsible for installing, maintaining, and repairing ITS devices; assisting in the ITS design review and the development of SOP; and performing a variety of technical tasks related to their assigned area of responsibility. The ITS Maintenance Technician shall receive general supervision from the VENDOR'S ITS Project Manager and MOBILITY AUTHORITY'S Project Manager. The technician shall document all work performed on all site conditions and daily activities.

The responsibilities and duties may include, but are not limited to, the following:

- Installs and maintains a wide variety of SYSTEM devices
- Troubleshoots malfunctions; isolates defects and repairs devices and equipment using above ground equipment on high-speed, high-volume roads and freeways
- Verifies proper device and system operation; conducts inspections and periodic preventive maintenance
- Monitors ITS device operation through the use of a laptop computer; uses SYSTEM software, both proprietary and nonproprietary; recommends and safely completes appropriate changes for effective SYSTEM operation
- Performs repair, removal, and replacement of poles, cabinets, controllers, and other equipment; repairs conduit and pull wires and cable, as needed; performs emergency repairs as needed
- Modifies or updates existing SYSTEM devices and equipment
- Reads diagrams, plan sets, manuals, and specifications for new installations and continual maintenance of SYSTEM devices; makes corrections to schematics and plan sets
- Performs field and bench testing procedures on a variety of SYSTEM equipment; tests, troubleshoots, and repairs SYSTEM equipment to component level of micro processing systems; maintains and services a variety of test and repair equipment
- Assists network administrator with repairs and connection of intercommunication cable and related equipment, as necessary
- Documents work performed on all SYSTEM devices and daily activities, including real-time updates to the IMS
- Performs other tasks as assigned by the MOBILITY AUTHORITY

Electrical Technician(s)

The Electrical Technician shall be responsible for installing, maintaining, and repairing electrical SYSTEM devices; assisting in SYSTEM design review and the development of SOPs; and performing a variety of technical tasks related to their assigned area of responsibility. The Electrical Technician shall receive general supervision from the VENDOR'S ITS Project Manager and MOBILITY AUTHORITY'S Project Manager. The Electrical Technician shall document and photograph the work performed on all site conditions and daily activities.

The responsibilities and duties may include, but are not limited to, the following:

- Directs and participates in a wide range of functional electrical tasks on SYSTEM components; isolates prime power malfunctions and coordinates repairs with power company; replaces power service points, as needed
- Performs field and bench testing procedures on a variety of SYSTEM and power equipment, such as UPS, automatic transfer switches, generators, load switches, power service assemblies, CCTV cameras, VDS, DMS, wireless communication facilities, WWVDS, RWIS, Connected Vehicle technology, and others; tests, troubleshoots, and repairs SYSTEM equipment to component level of micro-processing systems; maintains and services a variety of test and repair equipment
- Installs and maintains a wide variety of SYSTEM devices
- Troubleshoots malfunctions; isolates defects and repairs devices and equipment using a bucket truck on high-speed, high-volume roads and freeways; has exposure to electrical energy, high voltage, heat, cold, noise, dust, fumes, inclement weather conditions
- Verifies proper device and system operation; conducts inspections and periodic preventive maintenance
- Monitors SYSTEM device operation (e.g., UPS input/out) through the use of a laptop; uses sophisticated SYSTEM software, both proprietary and non-proprietary; recommends and safely completes appropriate changes for effective system operation
- Performs repair, removal, and replacement of poles, cabinets, controllers, and other equipment; repairs conduit and pulls wires and cable, as needed; performs emergency repairs as needed
- Reads diagrams, plan sets, manuals, and specifications for new installations and continual maintenance of SYSTEM devices; makes corrections to schematics and plan sets
- Documents work performed on all SYSTEM devices and daily activities, including real-time updates to the IMS
- Performs other tasks as assigned by the MOBILITY AUTHORITY

Utility Technician(s)

The Utility Technician shall be responsible for identifying the underground location, delineating, and marking on the ground of existing utilities, per requests from Texas811, the VENDOR'S ITS Project Manager, or MOBILITY AUTHORITY'S Project Manager. The utility locates shall include, but not be limited to, fiber optic communication backbone and drop cables, power cables, composite cables, UCV, and all ground boxes that constitute MOBILITY AUTHORITY owned underground utilities. The Utility Technician shall also meet with parties requesting utility locates as necessary in the field to supplement marking SYSTEM utilities. Whenever available, the Utility Technician shall assist with the installation, maintenance, and repair of SYSTEM devices. The Utility Technician shall be able to respond to emergency utility locate ticket(s) as requested by the VENDOR'S ITS Project Manager or the MOBILITY AUTHORITY'S Project

Manager. The Utility Technician shall document and photograph the work performed on all utility locating and daily activities.

Fiber Optic Technician(s)

The Fiber Technician shall be responsible for troubleshooting and repairing or replacing patch panels, fiber jumper cables, patch cables, splice enclosures, splice trays, splices, snowshoes, optics, terminations (e.g., pigtailed, buffer tube fan out kits), and any such items related to network and device connectivity.

Network Administrator

The Network Administrator shall be responsible for installing, configuring, maintaining, monitoring, diagnosing, troubleshooting, and repairing all networking equipment related to the SYSTEM; assisting in the design and modification of the MOBILITY AUTHORITY'S existing Layer 2/3 network; conducting technical design reviews for construction and maintenance projects; and performing a variety of technical tasks related to their assigned area of responsibility. The Network Administrator shall receive general supervision from the VENDOR'S ITS Project Manager and MOBILITY AUTHORITY'S Project Manager. The Network Administrator shall be responsible for maintaining a database of all pertinent configuration parameters for network equipment—including, but not limited to—IP addresses, default gateways, VLANs, port assignments, routing tables, and firewall rules. The Network Administrator shall also be responsible for all elements of the implementation and maintenance of the MOBILITY AUTHORITY'S cybersecurity features.

1.5.6 General Appearance and Conduct

VENDOR staff shall exercise good judgment in carrying out their duties and conduct themselves in such a manner that will reflect favorably upon the MOBILITY AUTHORITY. These requirements extend anywhere and anytime VENDOR staff represent the MOBILITY AUTHORITY, including in office buildings, on the roadside, and most importantly when travelling the roadways. MOBILITY AUTHORITY reserves the right to require removal of any VENDOR employee from this CONTRACT who cannot perform their duties to the satisfaction of the MOBILITY AUTHORITY or damages the reputation of the MOBILITY AUTHORITY and/or the VENDOR.

VENDOR staff shall be provided photo identification by the VENDOR and shall be able to present this identification at any time VENDOR staff are operating on MOBILITY AUTHORITY property.

1.5.7 Training

The VENDOR shall provide qualified instructors and all materials for training VENDOR staff in the maintenance, operation, and troubleshooting of equipment, hardware, software, and firmware for all SYSTEM devices. MOBILITY AUTHORITY staff may participate in training with

VENDOR staff. Training shall be conducted on an as-needed basis and shall consist of formal classroom lectures and online webinars, as well as “hands-on” training that consists of working with actual equipment and testing of SYSTEM devices and the entire SYSTEM.

1.5.8 Personnel Vetting

During the term of the CONTRACT, the VENDOR shall provide resumes of all proposed primary maintenance staff and all new hires along with certification or documentation of the following: drug test results, criminal background check, drivers’ licenses, and other information for approval prior to hiring.

1.5.8.1 Background Check

Each of the VENDOR’S staff assigned to service this CONTRACT and SYSTEM must pass a background check. The VENDOR shall provide the MOBILITY AUTHORITY’s Project Manager with proper documentation. It will be the responsibility of the VENDOR’S ITS Project Manager to ensure coordination of the background checks for the term of this CONTRACT.

The MOBILITY AUTHORITY reserves the right to reject any staff prior to being assigned duties.

1.5.8.2 Criminal Record Check

Individuals with felony conviction records shall not be hired. A criminal history record check shall be conducted by an approved MOBILITY AUTHORITY agency and shall be provided by the VENDOR to the MOBILITY AUTHORITY for each employee before hire. These criminal record checks shall go back as far as the employee’s birth. The VENDOR shall perform criminal checks annually for all VENDOR staff. Additionally, the MOBILITY AUTHORITY may elect to have VENDOR perform periodic criminal record checks on VENDOR staff.

1.5.8.3 Drug-Free Workplace Certification

The VENDOR shall provide proof, by a licensed medical practitioner or technician, that all VENDOR staff is drug-free in accordance with 37 Tex. Admin. Code 35.13, prior to beginning operations. The VENDOR shall submit the proof described above for staff every year thereafter.

1.6 CRITERIA FOR PERFORMANCE MEASURES AND EVALUATION

Throughout the term of the CONTRACT, the MOBILITY AUTHORITY will conduct reviews of various phases of the VENDOR’S operations to determine compliance with the CONTRACT and the sufficiency with which control procedures are applied to assure activities are in conformity with CONTRACT provisions and MOBILITY AUTHORITY procedures. Activities include staff performance and availability, system uptime, data management, and general performance measures.

Immediate remedial action is required for deficiencies to correct work that is not at the level of accepted performance. Failures to correct deficiencies shall result in assessment of liquidated damages.

1.6.1 Staff Performance

VENDOR staff performance will be reviewed with regard to work quality, professionalism, reliability, and punctuality, and other performance assessments consistent with MOBILITY AUTHORITY policy.

1.6.2 Availability

The VENDOR will be evaluated with respect to overall responsiveness to MOBILITY AUTHORITY requests. Response times longer than those agreed upon between the VENDOR and the MOBILITY AUTHORITY, or instances when the MOBILITY AUTHORITY is unable to reach the VENDOR to request services under this CONTRACT, will negatively impact evaluation of availability.

1.6.2.1 Staff Availability

VENDOR staff assigned to this CONTRACT will be evaluated with respect to availability of time, reliability, and prompt responsiveness.

1.6.2.2 System and Device Uptime

The VENDOR will be evaluated by the overall uptime of the SYSTEM—including field devices, equipment, and backend software—as CONTRACT performance indicators. The VENDOR will implement and maintain tools that collect and report SYSTEM availability—including SYSTEM device and overall SYSTEM uptime percentages. Tools and network access used to determine device and system availability must be coordinated with, and approved by, the MOBILITY AUTHORITY. Uptime percentages must be monitored and reported for the following:

1. Network devices (e.g., Layer 2/3 Ethernet switches, wireless communication devices)
2. CCTV cameras
3. Vehicle detection systems (e.g., RVSD, Bluetooth travel time reader)
4. DMS (e.g., full-matrix display, embedded single-line)
5. WWVDS
6. Connected Vehicle technology (e.g., RSU)
7. TIMC equipment (e.g., video wall, servers, operator workstation, central computer system)

Any field device or equipment within the SYSTEM shall be considered “down” if not 100-percent functional. The VENDOR shall be responsible for the operation and maintenance of a network monitoring system (NMS) software used to monitor and manage the SYSTEM communications network. The VENDOR shall configure the NMS to communicate with ITS field

network devices via simple network management protocol (SNMP), allowing field devices to be auto-discovered, monitored, and controlled. The NMS shall determine and display physical and logical connectivity in networks, as well as information pertaining to protocols running over the network. The VENDOR shall expand the NMS as the growth of the SYSTEM network warrants. The VENDOR shall utilize the NMS to run diagnostics of the SYSTEM and provide the report to the MOBILITY AUTHORITY within twenty-four (24) hours of being requested. The VENDOR shall provide remote access to the NMS software to the MOBILITY AUTHORITY, including MOBILITY AUTHORITY personnel and designated representatives.

The VENDOR shall be responsible for developing an availability report and submitting it for approval to the MOBILITY AUTHORITY. Availability reports using a tabular format with graphical charts that display historical device system availability carried forward for the duration of the CONTRACT are acceptable. Coordinate the final format of reports with the MOBILITY AUTHORITY. The VENDOR shall develop the report using data recorded in the NMS and in conjunction with information collected through TIMC operations and the MOBILITY AUTHORITY.

The report shall include the uptime of all field devices, networking equipment, subsystems, and systems, including but not limited to, CCTV cameras, network devices, vehicle detection systems, DMS, WWVDS, Connected Vehicle technology, and TIMC equipment. This information shall be included within a monthly report and an aggregated annual report documenting the total downtime and percentage available (e.g., 99.999 percent/year for each device), with a weighted average for the total equipment percentage reported submitted to the MOBILITY AUTHORITY. Downtime related to incidents or natural disasters shall be recorded separately from all other SYSTEM failures and will be excluded from the downtime percentages at the discretion of the MOBILITY AUTHORITY.

1.6.2.3 Response and Repair Times

The VENDOR will be evaluated by the overall responsiveness when notified of maintenance needs. Criteria for response and repair activities are defined in **Section 1.4.11.3 – Response Times**. The clock will begin at the time the VENDOR is notified of the maintenance need or identified issue.

1.6.2.4 General Performance Measures

General performance measures will be used to indicate how well the VENDOR is adhering to the submitted proposal for this CONTRACT. General performance measures include:

- Adherence to Proposed Staffing Levels – reporting of the number of working staff hours for the month versus the VENDOR’S proposed staffing hours
- Adherence to Operating Hours – reporting of the number of hours the SYSTEM was operational during the month versus the hours of operation established by the MOBILITY AUTHORITY, as well as the number of hours worked by the VENDOR’S

- assigned staff versus the hours of operation established by the MOBILITY AUTHORITY
- Other data as agreed to between the VENDOR and the MOBILITY AUTHORITY

1.7 SERVICES, MATERIALS PROVIDED BY THE MOBILITY AUTHORITY

As part of this CONTRACT, the following activities will be performed by the MOBILITY AUTHORITY, including contract management/payment, coordination, access to facilities, technical reviews, and providing existing documentation, including as-builts, studies, and reports, as necessary.

1.7.1 Contract Management

The MOBILITY AUTHORITY will assign a Project Manager to be responsible for coordination with the VENDOR and the direct management of personnel and tasked activities (e.g., Work Authorization) as required to perform work on behalf of the MOBILITY AUTHORITY under this CONTRACT.

1.7.2 Coordination

The MOBILITY AUTHORITY'S Project Manager will assist the VENDOR with coordination efforts for ongoing projects, maintenance activities, and with other stakeholders, as required to perform work on behalf of the MOBILITY AUTHORITY under this CONTRACT. This does not alleviate the VENDOR for being responsible for coordination efforts with third-party contractors, stakeholders, VENDOR personnel, and MOBILITY AUTHORITY staff.

1.7.3 Access to Facilities

The MOBILITY AUTHORITY will provide access to any and all MOBILITY AUTHORITY facilities and resources in accordance as necessary by the VENDOR and approved by the MOBILITY AUTHORITY. THE MOBILITY AUTHORITY reserves the right to reject any and all requests for facility access into MOBILITY AUTHORITY facilities made by the VENDOR. The VENDOR shall be responsible for strict adherence to all MOBILITY AUTHORITY policies and procedures while on the property and inside of MOBILITY AUTHORITY facilities.

1.7.4 Technical Reviews

The MOBILITY AUTHORITY will perform technical peer reviews for plans, schematics, bill of materials, product data sheets, reports, and other documentation submitted by the VENDOR as a deliverable. The MOBILITY AUTHORITY reserves the right to review and provide comments to the VENDOR to be addressed and revise the submittal, as appropriate, prior to approval. All deliverables from the VENDOR to the MOBILITY AUTHORITY require approval prior to notice to proceed on construction or closeout of the Work Authorization. The VENDOR is responsible for the documentation of all comments received, as well as recording VENDOR responses,

disposition (e.g., agree, disagree, more clarification needed), and status (e.g., complete, incomplete, address in future submittal) for each comment received. The MOBILITY AUTHORITY will perform reviews and provide feedback/comments within fifteen (15) days of the submittal unless an extension is otherwise requested by the MOBILITY AUTHORITY.

1.7.5 Existing Documentation

To the best of its abilities, the MOBILITY AUTHORITY will provide the VENDOR will all relevant documentation on the existing SYSTEM. This includes, but may not be limited to, as-built plan sets, existing conditions reports, bill of materials, asset inventory, studies, research findings, technical product data sheets, and more.

1.8 CONTRACT MONITORING, PROGRESS, REPORTING AND COORDINATION

The MOBILITY AUTHORITY will use VENDOR reports and periodic contact with the VENDOR to monitor the contract and VENDOR compliance with agreement terms and conditions, applicable laws, and regulations. Contract monitoring will also be used to verify that activities are being or have been performed in accordance with this agreement, that deliverables have been completed, that funds have been accounted for and used appropriately, and that the goals and objectives of this CONTRACT are being met by the VENDOR. The VENDOR is required to develop and maintain a two-week “look ahead” schedule to assist with coordination and monitoring of work performed under the CONTRACT. The VENDOR shall coordinate the format of the schedule and the frequency of updates with the MOBILITY AUTHORITY.

1.8.1 Status Reports

The VENDOR shall maintain complete and accurate records, in hard copy and electronic file formats acceptable to and approved by the MOBILITY AUTHORITY for all SYSTEM maintenance activities and any other events relating to the CONTRACT. All documentation shall be stored in a SharePoint site (or equivalent) accessible by both the VENDOR and MOBILITY AUTHORITY. The MOBILITY AUTHORITY may elect to save copies of files onto a local hard drive at its own discretion.

All project records and files (e.g., as-built drawings, bill of materials), as well as any equipment owned by the MOBILITY AUTHORITY shall be delivered to the MOBILITY AUTHORITY within thirty (30) calendar days prior to submittal of the final invoice by the VENDOR. Final payment shall not be rendered by the MOBILITY AUTHORITY until all of the conditions of the CONTRACT have been met.

The VENDOR shall keep a documented log of each and every device location. Preventive and routine maintenance, repair logs, parts replacement, special notes, recommendations, and equipment warranty records (if available) shall be included as part of the device log. Multiple device logs can be compiled into a single site log if multiple devices are at a single location. This

log shall be presented to the MOBILITY AUTHORITY by the final working day of each month and shall be in an Excel file format. The Excel document shall include sortable columns and must be in a format approved by the MOBILITY AUTHORITY.

Device records, at a minimum, shall include, but not be limited, to the following:

- Asset ID No. (MOBILITY AUTHORITY)
- Device location (corridor, milepost, and side of the road)
- Date and time of failure(s) or preventative maintenance visit
- Description of failure(s) or issue(s) and impacts
- Report of failure source
- Technician responding
- Arrival time at device location
- Site conditions noted (e.g., weather, accident, fire)
- Action(s) taken and result (e.g., successful, otherwise)
- Date and time of resolution
- Spare parts used – type, manufacturer, model, serial number
- Photo documentation
- Replaced parts – type, manufacturer, model, serial number
- Action for replaced parts (e.g., in-house repair, return to manufacturer, scrap); and
- General notes.

It shall be the VENDOR'S responsibility to maintain complete and accurate records of all work activities and all other events relating to this CONTRACT. Project records shall include, but not be limited to, such items as status reports, meeting notes, cost proposals, invoices, current and historical inventory records, locate tickets and reports, updated as-built plans, time sheets, technical product data sheets, and VENDOR'S staff records. Project files shall contain all correspondence to and from the VENDOR and subcontractors, consultants, manufacturers, equipment vendors, local, state, and federal agencies, etc., as related to this CONTRACT. These files shall also include all materials information obtained by or given to the VENDOR. All records shall be categorized and organized by date, activity, and subject. Paper documentation shall be scanned into an electronic format and become part of an electronic document repository for the CONTRACT.

The project files shall be established such that they can be delivered to the MOBILITY AUTHORITY within forty-eight (48) hours of request.

1.8.1.1 Monthly Report

The VENDOR shall prepare and submit a monthly status report describing all activities to the MOBILITY AUTHORITY'S Project Manager. The purpose of the monthly report is to provide a summary of all work performed by the VENDOR and the status of that work over one (1) month's period. The VENDOR shall supply a monthly report within ten (10) business days of each month's end following the monthly report period of the CONTRACT. This report shall

include all information collected during the reporting period; device availability information; preventive maintenance plan update and progress; and a work breakdown listing the technician, equipment utilized, and repair procedure for each occurrence of work. The monthly status reports shall commence at CONTRACT Notice to Proceed (NTP) and shall continue for the duration of the CONTRACT. This report shall include descriptions of all services performed and results of testing conducted during the report period. The report format shall be coordinated with the MOBILITY AUTHORITY for approval prior to the submittal of the first report. The report shall be a collection of events, data, calculations, decisions, instructions, notifications, circumstances, photographs, and work performed each day during the CONTRACT period. The monthly status report shall include, but not be limited to, the following information:

- Overall System Uptime (summary)
- Emergency Maintenance Repairs Performed (each)
 - Location
 - Date and time
 - Description of event, including digital photo documentation
 - Contributing factors, cause of issue
 - Arrival time
 - Departure time
 - Action(s) taken
 - Result and status, including digital photo documentation
 - Next steps, as appropriate
- Preventative Maintenance Performed (summary)
- Completed/ongoing projects and efforts (e.g., previous month)
- Upcoming projects and efforts (e.g., next month)
- Status of purchase orders
- Status of Action Items (from bi-weekly coordination meetings)
- Staffing changes
- General Comments

1.8.1.2 Annual Report

The VENDOR shall develop and submit an annual report to the MOBILITY AUTHORITY to provide a summary of all work performed by the VENDOR and the status of ongoing/upcoming work over a twelve-month period, recurring every March 31.

The VENDOR shall supply the annual report on the final MOBILITY AUTHORITY each year for the twelve-month period duration between April 1 and March 31, beginning at the start of the CONTRACT. This report shall include all information from the monthly reports for the previous year, as well as overall device and system uptime percentage information. This report shall also document and certify that all work has been completed in accordance with manufacturer's recommendations and the requirements of this CONTRACT. This report shall include an assessment by the VENDOR of equipment failures and their causes, such as design/construction

errors, aging, environmental problems (such as lightning/surge/power issues), etc., as well as maintenance recommendations for the upcoming twelve-month period.

1.8.2 Meetings

The VENDOR will be required to participate in bi-weekly status meetings relating to SYSTEM maintenance, ongoing project/effort status, and upcoming projects/efforts, as scheduled by the MOBILITY AUTHORITY or its representatives. The VENDOR shall ensure that key personnel is available and prepared for the bi-weekly status meetings. The VENDOR is required to provide meeting minutes within two (2) working days of each meeting, unless otherwise directed by the MOBILITY AUTHORITY. The MOBILITY AUTHORITY will be provided one (1) week to review and comment.

The VENDOR will be required to participate in monthly status meetings coordinated by the MOBILITY AUTHORITY with the Toll Systems Integrator (TSI). The VENDOR shall ensure that key personnel is available and prepared for the monthly status meetings.

The MOBILITY AUTHORITY reserves the right to schedule additional as-needed meetings involving the VENDOR, including, but not limited to, design coordination, construction status, vendor presentations, in-house staffing meetings, stakeholder coordination, and budget planning meetings.

1.8.3 Transition Plan

The VENDOR shall be responsible for developing a Transition Plan and submitting it for approval to the MOBILITY AUTHORITY within thirty (30) days after the CONTRACT execution date. The Transition Plan shall detail how the VENDOR will work with the current service provider to ensure a seamless transfer of maintenance services and to ensure continuous (24 X 7 X 365) system operation and functionality of all components of the SYSTEM. The transition period will occur from the time of this CONTRACT execution until the time the previous contract expires, unless otherwise directed by the MOBILITY AUTHORITY.

1.8.4 Project Management Plan

The VENDOR shall be responsible for creating the Project Management Plan (PMP) and submitting it for review and approval by MOBILITY AUTHORITY within thirty (30) days after the CONTRACT Notice to Proceed (NTP). The Project Management Plan shall include, but not be limited to, the VENDOR'S staffing plan, hiring plan, tiered staff support plan, emergency response plan, vehicle and equipment maintenance plan, training and certification plan, communication protocols with MOBILITY AUTHORITY personnel, and any other items necessary to identify how the VENDOR intends on executing the CONTRACT.

1.8.5 Preventative Maintenance Activities Plan

The VENDOR shall be responsible for creating a Preventative Maintenance Activities Plan (PMAP) and submitting for review and approval by MOBILITY AUTHORITY within sixty (60) days after the CONTRACT Notice to Proceed (NTP). The Preventative Maintenance Activities Plan shall be a living document that details the evaluation criteria, procedures, and timelines for performing preventative maintenance on the SYSTEM components. The PMAP shall establish standard operating guidelines (SOP) and procedures for maintenance responsibilities, detail typical maintenance activities per device and equipment, identify intercommunication protocols, identify roles and responsibilities, and create an atmosphere conducive to teamwork, accuracy, consistency, and professionalism. At a minimum, the PMAP will be reviewed once a year, and recommended updates must be submitted to the MOBILITY AUTHORITY for review and approval. The VENDOR may be requested to revise this document earlier at the discretion of the MOBILITY AUTHORITY. Please refer to Section 3.10 for additional details on the minimum requirements for scheduled and preventative maintenance.

1.9 SUBMITTALS / DELIVERABLES

The executed Work Authorization (WA) will serve as official Notice to Proceed (NTP) for any and all work authorized and performed under this contract. The VENDOR will be required to provide the following submittals based on the work outlined in the WA.

1.9.1 Estimates

The VENDOR shall provide all cost estimates related to performing the work identified in the WA, including purchasing devices, equipment, and software; man-hours; rental equipment; and more. The VENDOR must receive MOBILITY AUTHORITY approval of the submitted estimate request prior to receiving begin work.

1.9.2 Equipment Submittal

The VENDOR shall provide detailed technical data sheets and unit costs for equipment to be purchased to complete the work identified in the WA. The VENDOR must receive MOBILITY AUTHORITY approval of the submitted equipment prior to ordering and purchasing.

1.9.3 Maintenance Documentation

The VENDOR shall develop and submit all documentation for maintenance efforts performed, including preventative and emergency as defined in the CONTRACT.

1.9.3.1 Maintenance Checklists

Preventative Maintenance Checklists will be submitted for approval by the MOBILITY AUTHORITY within thirty (30) days of Notice to Proceed (NTP). Completed checklists will be

maintained by the VENDOR and subject to review at the request of the MOBILITY AUTHORITY at any time.

1.9.3.2 Equipment Maintenance Logs

The VENDOR shall log all maintenance activities performed for repair and emergency maintenance efforts. Completed logs will be maintained by the VENDOR and included as part of the monthly and annual status reports and subject to review at the request of the MOBILITY AUTHORITY at any time.

1.9.4 As-Built Plans

The VENDOR shall develop as-built plans for all new and/or revised infrastructure, field devices, and equipment removed, replaced, modified, or installed under this CONTRACT. The VENDOR shall submit final as-built plans to the MOBILITY AUTHORITY within thirty (30) days of completing the work. The VENDOR shall be responsible for keeping the latest version of the as-built plans for the duration of the CONTRACT.

1.9.5 Status Reports

The VENDOR shall develop and submit monthly and annual status reports to the MOBILITY AUTHORITY for review and approval as defined in the CONTRACT.

1.10 PREVENTATIVE MAINTENANCE MINIMUM REQUIREMENTS

1.10.1 General

The following section details the minimum requirements expected by the MOBILITY AUTHORITY for scheduled and preventative maintenance activities only. These minimum requirements do not account for non-scheduled maintenance, minor repairs, diagnostics and troubleshooting, or any other services which are also compensated by the monthly Maintenance Service Unit Price. Maintenance procedures must fall within manufacturer recommendations and must not void equipment warranty.

1.10.2 Minimum Requirements for Monthly Maintenance

ITS Field Equipment Maintenance Minimum Requirements

CCTV Camera, Pan-Tilt-Zoom (PTZ) and Fixed – preventative maintenance of a CCTV camera includes, but is not limited to, the camera assembly and associated infrastructure located external to the device’s cabinet or enclosure. The camera assembly includes the lens, housing and all internal components, mounting hardware, communication and power cabling, air terminals and grounding array, power supplies, PoE injectors, and any other in-cabinet

ITS Field Equipment Maintenance Minimum Requirements

equipment exclusive to the CCTV assembly. Associated infrastructure includes any non-structural infrastructure related to the camera system including any ground boxes and conduit containing camera communication and/or power cabling.

The following scheduled maintenance for CCTV cameras shall occur a minimum of **1 time per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

- Assessing structural integrity and alignment of the camera assembly
- Inspecting camera assembly for physical damage and degraded conditions (e.g., cracks, rust, loose connections)
- Operational maintenance of mechanical components, including removal of sediment and lubrication of pan-tilt-zoom (PTZ) tracking components
- Physical opening and cleaning of any aerially mounted junction boxes (if applicable)
- Physically testing and inspecting grounding system(s), surge protective devices, PoE injectors, connections, cable assemblies, and other related hardware. Inspecting cabling for kinks, damage to outer jacket, and other irregularities
- Physically opening ground boxes to remove dirt, debris, vegetation, and standing water; cleaning bolt holes and threads; Replace missing or damaged bolts, as necessary; Inspecting condition of ground box lids and replacing, as necessary. Inspecting cabling for kinks, damage to outer jacket, and other irregularities
- Providing weed, grass, and erosion control around devices, above-ground conduit, ground boxes, etc.

The following scheduled maintenance for CCTV cameras shall occur a minimum of **4 times per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

- Cleaning of housing and lens, including application of rain repellent to the lens and video feed quality verification

Radar Vehicle Sensing Device (RVSD) – preventative maintenance of a RVSD includes, but is not limited to, the RVSD assembly and associated infrastructure located external to the device’s cabinet or enclosure. The RVSD assembly includes the device, mounting assembly, communication and power cabling, grounding array, wireless communication device(s) (if applicable), power supplies, media converters, and any other in-cabinet equipment exclusive to the RVSD assembly. Associated infrastructure includes any non-structural infrastructure related to the RVSD system including ground boxes and conduit containing RVSD communication and/or power cabling. If the RVSD is mounted to a device pole without a cabinet, the device pole shall be considered as associated infrastructure.

Scheduled maintenance for RVSDs shall occur a minimum of **1 time per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

ITS Field Equipment Maintenance Minimum Requirements

- Validating operation and physical positioning of RVSD to collect accurate vehicle detection data on a per lane basis; adjusting as necessary
- Assessing structural integrity and alignment of the RVSD assembly and device pole (if applicable)
- Inspecting RVSD assembly for physical damage and degraded conditions (e.g., cracks, rust, loose connections)
- Cleaning of the device housing
- Physically opening and cleaning of any aerially mounted junction boxes (if applicable)
- Physically testing and inspecting grounding system(s), surge protective devices, media converters, connections, cable assemblies, and other related hardware. Inspecting cabling for kinks, damage to outer jacket, and other irregularities
- Physically opening ground boxes to remove dirt, debris, vegetation, and standing water; cleaning bolt holes and threads; Replace missing or damaged bolts, as necessary; Inspecting condition of ground box lids and replacing, as necessary. Inspecting cabling for kinks, damage to outer jacket, and other irregularities
- Providing weed, grass, and erosion control around devices, above-ground conduit, ground boxes, poles, etc.

Dynamic Message Sign (DMS) – preventative maintenance of a DMS includes, but is not limited to, the sign assembly and associated infrastructure located external to the device’s cabinet or enclosure. The sign assembly includes the housing, LED modules, internal electronics and all miscellaneous hardware within the sign, power supplies, and any mounting connections to the sign structure. Infrastructure associated with the DMS includes the sign structure, foundation, cabling providing power and/or communications¹, and ground boxes and conduit containing DMS cabling.

The following scheduled maintenance for DMS shall occur a minimum of **1 time per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

- Inspecting the field controller for proper operation (e.g., error codes, alarms), damage, and degraded conditions; performing diagnostics as necessary
- Inspecting, testing, and cleaning fan blades, bearings, and air filters inside sign housing
- Visually inspecting equipment status LED modules, light fixtures, light bulbs, and all wiring for proper function, damage, and degraded conditions
- Inspecting the mounting structure for corrosion, loose bolts, and overall stability (e.g., rust, cracks, foundation or structure settling, off-plumb positioning)
- General cleaning inside sign housing including debris and dust removal
- Performing pest control as necessary, including placement of barriers to prevent rodent or insect entry
- Cleaning the external sign panel of dirt, dust, and debris

ITS Field Equipment Maintenance Minimum Requirements

- Physically opening and cleaning of any aerial mounted junction boxes (if applicable)
- Physically testing and inspecting of grounding system(s), surge protective devices, connections, and cable assemblies. Inspecting cabling for kinks, damage to outer jacket, and other irregularities
- Physically opening ground boxes to remove dirt, debris, vegetation, and standing water; cleaning bolt holes and threads; Replace missing or damaged bolts, as necessary; Inspecting condition of ground box lids and replacing, as necessary; Inspecting cabling for kinks, damage to outer jacket, and other irregularities¹
- Providing weed, grass, and erosion control around devices, above-ground conduit, ground boxes, poles, etc.

¹Includes communication cabling from the DMS to its termination point (i.e., fiber splice vault, patch panel, network switch) and power cabling from the DMS to its termination point (i.e., electrical service, toll facility breaker panel, ITS cabinet)

Wrong Way Vehicle Detection System (WWVDS) – preventative maintenance of a WWVDS includes, but is not limited to, the WWVDS assembly and associated infrastructure. The WWVDS assembly includes CCTV cameras, thermal cameras, “Wrong Way” signs, Retro-reflective Flashing Beacons (RRFB’s), device poles and foundations, mounting assemblies, pole-mounted cabinets and internal components, cabling, grounding array, wireless communication devices. Associated infrastructure includes cabling providing power and/or communications¹ and ground boxes and conduit containing WWVDS communication and/or power cabling.

The following scheduled maintenance for WWVDS shall occur a minimum of **1 time per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

- Conducting a standard test procedure to test and document functionality of the detection system
- Testing wireless connectivity
- Assessing structural integrity and alignment of cameras, wireless communication devices, and mounting hardware
- Inspecting the structure for corrosion, loose bolts, and overall stability
- Physically testing and inspecting of grounding system(s), surge protective devices, connections, and cable assemblies. Inspecting cabling for kinks, damage to outer jacket, and other irregularities.
- Physically opening ground boxes to remove dirt, debris, vegetation, and standing water; cleaning bolt holes and threads; Replace missing or damaged bolts, as necessary; Inspecting condition of ground box lids and replacing, as necessary; Inspecting cabling for kinks, damage to outer jacket, and other irregularities¹
- Providing weed, grass, and erosion control around devices, above-ground conduit, ground boxes, poles, etc.

ITS Field Equipment Maintenance Minimum Requirements

- General cleaning, including debris and dust removal from equipment, cabinets enclosures, sign panels, Retro-reflective Flashing Beacons (RRFB's) and associated junction boxes; replacing of air filter(s); checking general operation of internal lights, fans, outlets, and other system components
- Checking cabinet door locks, opening mechanisms, and entry detection sensors, for proper function, damage, and degraded conditions (e.g., corrosion, wear and tear); lubricating locks and other mechanisms and replacing as necessary
- Physically testing and inspection of in-cabinet equipment, including the power array, media converters, power supplies, ethernet switches, patch panels, grounding system(s), surge protective devices, cable connections, and cable assemblies
- Visually inspecting devices, cabinets, enclosure exteriors, and checking for corrosion, punctures, graffiti, and vandalism
- Performing pest control as necessary, including placement of barriers to prevent rodent or insect entry.

The following scheduled maintenance for CCTV camera and thermal detection cameras within the WWVDS assembly shall occur a minimum of **4 times per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

- Cleaning of housing and lens, including application of rain repellent to the lens and video feed quality verification

¹Includes communication cabling from the WWVDS cabinet to its termination point (i.e., fiber splice vault) and power cabling from the WWVDS cabinet to its termination point (i.e., electrical service)

Connected Vehicle to Everything (C-V2X) Roadside Unit (RSU) – preventative maintenance of a RSU includes, but is not limited to, the RSU assembly and associated infrastructure located external to the device's cabinet or enclosure. The RSU assembly includes the device, antennas, mounting assembly, communication/power cabling, grounding wires, power supplies, PoE injectors, and any other in-cabinet equipment exclusive to the RSU assembly. Associated infrastructure includes any non-structural infrastructure related to the RSU system including ground boxes and conduit containing RSU communication and/or power cabling.

Scheduled maintenance for RSUs shall occur a minimum of **1 time per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

- Validating RSU broadcasts, including verification of all enabled TIM messages, CV applications, MAP messages, etc.; adjusting as necessary
- Checking RSU assembly for structural integrity and alignment
- Cleaning of the device housing and antennas to remove dust and dirt
- Physically opening and cleaning any junction boxes (if applicable)

ITS Field Equipment Maintenance Minimum Requirements

- Physically testing and inspecting grounding system(s), surge protective devices, PoE injectors, connections, cable assemblies, and other related hardware. Inspecting cabling for kinks, damage to outer jacket, and other irregularities
- Physically opening ground boxes to remove dirt, debris, vegetation, and standing water; cleaning bolt holes and threads; Inspecting condition of ground box lids and replace as necessary; Inspecting cabling for kinks, damage to outer jacket, and other irregularities.
- Providing weed, grass, and erosion control around devices, above-ground conduit, ground boxes, poles, etc.

ITS Cabinets – preventative maintenance of ITS cabinets¹ includes, but is not limited to, the cabinet and infrastructure associated with the cabinet. The ITS cabinet includes the shell, opening mechanisms, and assembly located within (e.g., power array, ethernet switches, patch panels). Infrastructure associated with the ITS cabinet includes above-ground conduit, junction boxes, cabling providing power and/or communications², any ground boxes or conduit containing cabinet communication and/or power cabling, mounting assembly, and the pole structure and foundation the cabinet is mounted to, provided it is not a sign structure or tolling gantry. In cabinets, enclosures, or buildings where the co-location of tolling and ITS equipment exists, preventative maintenance on the cabinet and associated infrastructure shall be the responsibility of the Toll Systems Integrator.

The following scheduled maintenance for ITS cabinets shall occur a minimum of **1 time per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

- General cleaning including debris and dust removal from equipment, cabinets, enclosures, and associated junction boxes; replacing of air filter(s); checking general operation of internal lights, fans, outlets, and other system components
- Checking cabinet door locks, opening mechanisms, and entry detection sensors, for proper function, damage, and degraded conditions (e.g., corrosion, wear and tear); lubricating locks and other mechanisms and replacing as necessary
- Physically testing and inspecting in-cabinet equipment, including the power array, power supplies, ethernet switches, patch panels, grounding system(s), surge protective devices, cable connections, and cable assemblies
- Physically opening ground boxes to remove dirt, debris, vegetation, and standing water; cleaning bolt holes and threads; Replace missing or damaged bolts, as necessary; Inspecting condition of ground box lids and replacing, as necessary; Inspecting cabling for kinks, damage to outer jacket, and other irregularities
- Providing weed, grass, and erosion control around devices, above-ground conduit, ground boxes, poles, etc.

ITS Field Equipment Maintenance Minimum Requirements

- Checking mounting hardware and poles for structural integrity and alignment
- Visually inspecting devices, cabinets, enclosure exteriors, and checking for corrosion, punctures, graffiti, and vandalism
- Performing pest control as necessary, including placement of barriers to prevent rodent or insect entry

¹ Does not include WWVDS cabinets which shall be maintained as a part of the WWVDS System.

² Includes communication cabling from the ITS cabinet to its termination point (i.e., fiber splice vault, patch panel, network switch) and power cabling from the ITS cabinet to its termination point (i.e., electrical service, toll facility breaker panel)

Underground Cable Vault (UCV) – preventative maintenance of an UCV includes inspecting and providing maintenance to the entire UCV structure, including, but not limited to, the steel lid and its hinges, opening mechanism (if applicable), concrete apron, vault side-walls, conduit entry ports, cable rack system, and vault floor drain.

Scheduled maintenance for UCVs shall occur a minimum of **1 time per year**. At a minimum maintenance must include (pursuant to manufacturer recommendations):

- Physically opening UCV to remove dirt, debris, vegetation, and standing water
- Physically clearing the vault floor drain of all obstruction or potential obstruction (e.g., dirt, debris, mud)
- Lubricating the lid hinges and opening mechanism(s); Replacing as necessary
- Physically Inspecting UCV conditions for proper function, damage, and degraded conditions (e.g., corrosion, wear and tear), and replacing parts as necessary (e.g., duct terminators/caps in the conduit entry ports, cable rack system, concrete apron)
- Rearranging cables to utilize the cable rack system and prevent potential damage
- Physically testing and inspecting grounding system(s) to ensure steel lid is properly grounded
- Providing weed, grass, and erosion control around UCV apron, including filling in any missing earth material around and underneath the concrete apron
- Performing pest control as necessary

Electrical Service – preventative maintenance of electrical services includes the service assembly and infrastructure associated with the service assembly. The service assembly includes the pole, enclosure, all hardware within the enclosure, power meter, safety switch, mounting assembly, pole structure, and its foundation.

The following scheduled maintenance for electrical services shall occur a minimum of **1 time per year**. At a minimum maintenance must include (pursuant to the local utility company recommendations):

ITS Field Equipment Maintenance Minimum Requirements

- General cleaning, including debris and dust removal from within the enclosure and wiping of the external surface and panel labels. Replacing labels as necessary
- Checking enclosure locks and opening mechanisms, for proper function, damage, and degraded conditions (e.g., corrosion, wear and tear); lubricating locks and other mechanisms and replacing as necessary
- Physically testing and inspecting grounding system(s), disconnect, and safety switch(es) for proper function, exposed electrified wires, damage, and degraded conditions (e.g., corrosion, wear and tear)
- Providing weed, grass control, and around service pole, above-ground conduit, ground boxes, etc.

APPENDIX B
Form of Work Authorization

WORK AUTHORIZATION NO. ____

This Work Authorization is made as of this ____ day of _____, 202_, under the terms and conditions established in the AGREEMENT FOR INTELLIGENT TRANSPORTATION SYSTEM PERFORMANCE-BASED MAINTENANCE SERVICES, dated as of _____, 2023 (the “Agreement”), between the Central Texas Regional Mobility Authority (the “Authority”) and Kapsch TrafficCom USA, Inc. (“Contractor”). This Work Authorization is made for the following purpose, consistent with the services defined in the Agreement:

[Brief description of the Project elements to which this Work Authorization applies]

Section A. - Scope of Services

A.1. Contractor shall perform the following Services:

[Enter description of the Scope of Services here for which this Work Authorization applies, or make reference to an attached Appendix]

A.2. The following Services are not included in this Work Authorization but shall be provided as Additional Services if authorized or confirmed in writing by the Authority.
[optional]

A.3. In conjunction with the performance of the foregoing Services, Contractor shall provide the following submittals/deliverables (Documents) to the Authority:

Section B. - Schedule

This Work Authorization shall become effective on the date both parties have signed this Work Authorization No. ___. This Work Authorization No. ___ will terminate upon the Authority's final acceptance of the work described herein as determined by the Authority.

Contractor shall perform the Services and deliver the related Documents (if any) according to the following schedule:

[Insert description of proposed project schedule.]

Section C. - Compensation

C.1. In return for the performance of the foregoing obligations, the Authority shall pay to the Contractor the amount not to exceed \$ _____, based on the attached fee estimate. Compensation shall be in accordance with the Agreement.

C.2. Compensation for Additional Services (if any) shall be paid by the Authority to the Contractor according to the terms of a future Work Authorization.

Section D. - Authority's Responsibilities

The Authority shall perform and/or provide the following in a timely manner so as not to delay the Services of the Contractor. Unless otherwise provided in this Work Authorization, the Authority shall bear all costs incident to compliance with the following:

[Insert Authority's responsibilities, if any.]

Section E. - Other Provisions

The parties agree to the following provisions with respect to this specific Work Authorization:

Except to the extent expressly modified herein, all terms and conditions of the Agreement shall continue in full force and effect.

IN WITNESS WHEREOF, this Work Authorization No. [] is executed in duplicate counterparts and hereby accepted and acknowledged below.

CTRMA DIVISION DIRECTOR (*Requesting Work Authorization*)

Signature

Date

Typed/Printed Name and Title

CTRMA LEGAL (*Noting Legal Sufficiency*)

Signature

Date

Typed/Printed Name and Title

CTRMA FINANCE (*Noting Funds Availability*)

Signature

Date

Typed/Printed Name and Title

APPENDIX C
ITS Equipment Prices

APPENDIX D
Maintenance Services Unit Prices

APPENDIX E
Labor Rates

APPENDIX F
Service Level Agreements

CONTENTS

1. Service Level Agreements (SLA).....	1
1.1 General Provisions	1
1.2 Key Performance Requirements.....	2
1.2.1 Availability Requirements	2
1.2.2 Performance Reviews.....	2
1.2.3 Chargeable vs. Non-Chargeable Failures	2
1.2.3.1 Chargeable Failures	2
1.2.3.2 Non-Chargeable Failures	3
1.2.4 Accuracy Requirements.....	3
1.2.5 Time Constraint Requirements	3
1.2.6 Maintenance Service Level Requirements.....	4
1.2.6.1 Maintenance Support Requirements	4
1.2.6.2 Scheduled Preventative Maintenance Activities Requirements.....	4
1.2.6.3 Stop Clock Conditions.....	4
1.2.6.4 Help Desk Support Requirements	6
1.2.7 Miscellaneous.....	7
1.2.7.1 Single Event Causing Cumulative Liquidated Damages.....	7
1.2.7.2 Calculation of Damages	7
1.2.7.3 Calculation of Damages for Consecutive Failures	7
1.3 Service Level Agreement (SLA) Details	8

1. SERVICE LEVEL AGREEMENTS (SLA)

1.1 GENERAL PROVISIONS

The VENDOR shall meet defined levels of performance in the execution of the Scope of Work. **Appendix A – Scope of Work** describes the minimum performance requirements the VENDOR must meet. The VENDOR is responsible for demonstrating that the performance requirements described herein can be met or exceeded for all maintenance and installation activities before Final Acceptance. The measurement of these Service Level Agreements (SLA) shall be automated where possible and shall be straightforward and data-driven, as agreed to by the VENDOR and the MOBILITY AUTHORITY. The MOBILITY AUTHORITY, at their sole discretion, will periodically audit reports SLA results.

The VENDOR shall develop reports that compare actual, field-verified results to the requirements defined in this appendix and shall submit these reports to the MOBILITY AUTHORITY within ten (10) business days of each month's end. The VENDOR shall maintain all corresponding data in compliance with MOBILITY AUTHORITY Data Retention policies, and the data shall be made available to the MOBILITY AUTHORITY upon request. The methods and results of the measurement process shall be fully subject to independent audit and the results shall be utilized by the VENDOR to take corrective action to correct any deficiencies and failures to meet the required availability, accuracy, and performance requirements. The VENDOR shall be subject to liquidated damages as described in the SLA Table for failure to provide the required reports within the specified timeframe, or if reports are not accurate or complete.

Actual performance shall be defined and measured against the requirements and time periods in the SLA Table to assess the availability, accuracy, and performance of the delivered system. This appendix addresses these requirements for the following levels of service:

1. Accuracy
2. Availability
3. System Performance
4. Maintenance (response / repair timing)

The following sections provide general conditions that apply to the SLAs described herein. Should a specific SLA section define terms or conditions which appear contrary to these general provisions, the terms or conditions within the specific SLA section take precedence.

1.2 KEY PERFORMANCE REQUIREMENTS

1.2.1 Availability Requirements

The availability requirements, as specified in the SLA Table, shall be measured during monthly operations testing. The availability requirements will not include approved scheduled preventative maintenance activities.

For existing field devices, subsystems, and systems, the availability requirements shall begin immediately following the execution of this Contract (START DATE) as part of the maintenance phase. For newly installed systems, these requirements shall begin at the start of the warranty phase. The warranty phase shall conclude twelve (12) months after successful completion of Final Acceptance. Once the MOBILITY AUTHORITY has provided Final Acceptance and upon expiration of the warranty phase, the appropriate field device, subsystem, and system will transition in the maintenance period. The monthly warranty or maintenance fee, as applicable, shall be subject to the monthly assessment of availability and reliability measurements, as well as other criteria outlined in the SLA Table, and applicable damages for failure to meet such criteria.

1.2.2 Performance Reviews

The MOBILITY AUTHORITY will review the VENDOR's performance monthly using required system reports developed by the VENDOR in a format with content approved by the MOBILITY AUTHORITY. Performance reviews shall begin one (1) month following the execution of this Contract (START DATE) or one (1) month after the commencement of the warranty phase and shall include evaluation of the previous month of operation. The MOBILITY AUTHORITY may elect to waive or impose damages during the first four (4) months of the warranty phase for new installations.

The availability calculation will not include downtime during any period when the MOBILITY AUTHORITY does not allow the VENDOR to close a lane or otherwise work along the roadway, unless such failure to approve is the result of the VENDOR not following the MOBILITY AUTHORITY procedures in making the request.

1.2.3 Chargeable vs. Non-Chargeable Failures

For purposes of calculating availability performance requirements for testing and maintenance, performance chargeable and non-chargeable failures are defined as follows:

1.2.3.1 Chargeable Failures

Chargeable failures include any failures that are not specifically identified as non-chargeable in **Section 1.2.3.2 – Non-Chargeable Failures**, including but not limited to:

1. Malfunction that prevents Intelligent Transportation System (ITS) field devices, subsystems, or systems whether hardware or software from performing their designated function, when used and operated under the intended operational and environmental conditions
2. Malfunction that poses a threat to the safety of the general motoring public, maintenance personnel, employees, other roadway users, or the functionality of existing MOBILITY AUTHORITY systems (e.g., ITS, electronic toll collection systems)
3. Occurrence where data is not successfully transmitted between the field devices and the associated subsystems and systems unless the failure is already accounted for as a separate performance failure. For example, if video streams from a CCTV camera are not reaching the video wall within the Traffic Incident Management Center (TIMC) due to a physical fiber cut on the roadside, the failure would be charged to the fiber cut, but the camera would not be cited as a failure
4. Any failure of equipment or software—including ransomware, bugs—that result in failure of revenue-generating systems for the MOBILITY AUTHORITY (e.g., electronic toll collection systems)
5. Shutdown or unavailability of field devices, subsystems, or systems, unless otherwise specifically directed
6. Failure to properly record and transmit accurate data (e.g., vehicle data) from field devices to various associated subsystems and systems
7. Loss of data including failure to meet data retention requirements
8. Failure to generate the reports required to reconcile and audit the overall system and performance

1.2.3.2 Non-Chargeable Failures

Non-chargeable failures include events that fall outside of the direct control of the VENDOR, including but not limited to:

1. Force majeure event, as defined in the Contract
2. Vandalism
3. System component failures caused by environmental or operating conditions outside the design standards of the equipment
4. Customer or user induced failures

1.2.4 Accuracy Requirements

Accuracy requirements are specified in the SLA Table.

1.2.5 Time Constraint Requirements

Time constraint requirements are specific in the SLA Table.

1.2.6 Maintenance Service Level Requirements

The VENDOR shall provide sufficient personnel, tools, and other necessary resources to meet the service level requirements defined in the SLA Table.

1.2.6.1 Maintenance Support Requirements

Response times shall be measured from the time the overall system generates a fault/alert, the VENDOR is notified an event requiring maintenance or a failure event has occurred, or a maintenance ticket has been generated, and end when the VENDOR acknowledges the alert, ticket, and/or event via an approved communication method approved by the MOBILITY AUTHORITY.

Repair times shall be measured from the time the VENDOR acknowledges the maintenance ticket for the event and ends when the failure condition is corrected, and the system is returned to regular operation. If access to the equipment in question or associated equipment necessary to complete the repair is denied by the MOBILITY AUTHORITY, the repair time shall be measured beginning when the VENDOR is permitted to access the relevant equipment.

Both the response time and the repair time shall be registered in the maintenance ticketing systems provided by the VENDOR with access provided to the MOBILITY AUTHORITY upon request. Failure to meet the required response and repair times shall be monitored through performance reports provided by the VENDOR.

1.2.6.2 Scheduled Preventative Maintenance Activities Requirements

The VENDOR shall perform scheduled preventative maintenance activities per the provided maintenance schedule approved by the MOBILITY AUTHORITY.

1.2.6.3 Stop Clock Conditions

In specific circumstances, the VENDOR may be excused from its obligations to meet the performance and service level requirements set forth above under certain conditions agreed upon by the MOBILITY AUTHORITY, hereinafter referred to as STOP CLOCK CONDITIONS. Only the time during which these conditions are present shall be excluded from the timeframes used to measure the VENDOR's performance, as described below:

The VENDOR will exclude from the availability calculations the time arising from any of the following STOP CLOCK CONDITIONS:

1. Loss of connectivity to all of the MOBILITY AUTHORITY provisioned network and networking equipment if a third-party causes the loss of network connectivity, not under the direct or indirect control of the VENDOR and not reasonably preventable by the VENDOR, including, but not limited to, fiber optic cabling cuts not caused by the VENDOR. For purposes of this provision, the VENDOR's employees, subcontractors,

affiliates, subsidiaries, data service providers, agents, or suppliers shall be deemed to be under the control and responsibility of the VENDOR concerning equipment, services, or facilities to be provided under this Agreement.

2. The following MOBILITY AUTHORITY contact and/or access problems, provided that the VENDOR makes reasonable efforts to contact the MOBILITY AUTHORITY approved contacts immediately upon the commencement of the STOP CLOCK period:
 - a. Access necessary to correct the problem at a MOBILITY AUTHORITY owned site (e.g., TIMC) is not available because access is improperly denied or not arranged by the site contact or the MOBILITY AUTHORITY representative, provided that the VENDOR properly scheduled the visit or access beforehand, if advanced notice was required.
 - b. MOBILITY AUTHORITY construction activities prevent the VENDOR from performing scheduled maintenance or repair of field devices, subsystems, or systems.
 - c. Incorrect site contact information, which prevent access, provided that the VENDOR takes reasonable steps to notify the MOBILITY AUTHORITY of the improper contact information immediately and takes reasonable steps to obtain the correct information.
3. Scheduled Preventative Maintenance provided such schedule was provided to and approved by the MOBILITY AUTHORITY in advance and in writing; provided, however, that in no event shall the STOP CLOCK CONDITION time period be extended beyond the standard Scheduled Preventative Maintenance time period.
4. Force majeure events.

The VENDOR shall be required to submit the appropriate "Stop Clock Documentation" for each use of a STOP CLOCK CONDITION. The VENDOR shall submit documentation to the MOBILITY AUTHORITY as soon as the VENDOR is aware of a STOP CLOCK CONDITION occurring. Failure to provide the MOBILITY AUTHORITY with written notice when a STOP CLOCK CONDITION event arises waives the VENDOR's right to seek such amnesty. All "Stop Clock Documentation" must be included in the VENDOR's Monthly Report. The MOBILITY AUTHORITY may evaluate all "Stop Clock Documentation" and is entitled to request additional justification for each STOP CLOCK CONDITION identified. At the sole discretion of the MOBILITY AUTHORITY, use of STOP CLOCK CONDITIONS may be rejected, conditionally accepted, or accepted on a case-by-case basis. The VENDOR shall coordinate with the MOBILITY AUTHORITY to define all processes related to STOP CLOCK CONDITIONS, notification thereof, documentation requirements, and other relevant processes, as necessary, and document those processes in the VENDOR's Maintenance Plan submitted to the MOBILITY AUTHORITY for review, comment, and approval.

If it is determined during the review of a monthly maintenance invoice that the cause of the problem was not the fault or responsibility of the MOBILITY AUTHORITY, or in the event of denied access, if the reason was determined to be proper, then the STOP CLOCK CONDITION shall not apply. Further, if it is determined that the cause of the problem was not the fault or responsibility of the MOBILITY AUTHORITY, or in the event of denied access, if the reason was determined to be proper, after the MOBILITY AUTHORITY has paid the VENDOR the monthly

maintenance amount for the month in question, the MOBILITY AUTHORITY shall be able to deduct any penalties that should have been applied from a future monthly maintenance payment amount.

Notwithstanding any other provisions of the contract documents to the contrary, the following STOP CLOCK CONDITIONS do not apply to:

1. The VENDOR's response time performance requirements, as outlined in the Service Level Agreement.
2. Testing or maintenance initiated by the VENDOR outside of the Scheduled Preventative Maintenance windows.
3. Power fluctuations caused by electrical utility providers, common carriers, the VENDOR—including all subcontractors, affiliates, subsidiaries, data service providers, agents, or suppliers.
4. Time period during which the MOBILITY AUTHORITY has made reasonable efforts to notify the VENDOR of a problem, but the VENDOR was not available or unreachable.
5. Failure of the VENDOR to provide adequate facilities (including cabinets, sunshields, replacement field devices, networking equipment, power supplies, etc.) to ensure delivery of the contracted services will not be considered a valid STOP CLOCK CONDITION.
6. Any other reason or cause not expressly listed above for which the VENDOR is responsible.
7. If the VENDOR asserts force majeure or failure of the MOBILITY AUTHORITY provided equipment as an excuse to performance, the VENDOR shall have the burden of (i) providing sole proximate cause to the satisfaction of the MOBILITY AUTHORITY, (ii) that the VENDOR took reasonable steps to minimize the delay and damages caused by events when known or should have been known, and (iii) that the VENDOR timely notified the MOBILITY AUTHORITY of the actual occurrence which is claimed as grounds for a defense under this clause (if any).

1.2.6.4 Help Desk Support Requirements

The VENDOR shall supply personnel with direct expertise in support of the system hardware—including field devices, subsystems, and systems; software; networking equipment; and database management system(s) during the MOBILITY AUTHORITY normal operating hours to provide “help desk” support function for all VENDOR-supplied field devices, subsystems, and systems. The “help desk” is intended to act as a central point of contact for all technical support, including hardware and software questions; installation of updated versions of software and firmware; networking equipment; network connections; and general troubleshooting.

1.2.7 Miscellaneous

1.2.7.1 Single Event Causing Cumulative Liquidated Damages

If the VENDOR can prove to the reasonable satisfaction of MOBILITY AUTHORITY that a single event causes the VENDOR to fail to meet more than one Service Level Agreement (SLA), cumulative liquidated damages shall not be imposed. Instead, the highest applicable liquidated damages relative to such occurrence(s) shall apply.

If the VENDOR fails to complete the repair according to the services levels outlined in the SLAs, the VENDOR shall, in addition to the liquidated damages assessed for the single event, will be responsible for liquidated damages resulting from not meeting the repair time service levels for the impacted systems.

1.2.7.2 Calculation of Damages

To calculate liquidated damaged, all timeframes stated in the “Damages” column of the SLA Table shall be the time stated or any portion thereof.

Formulas for measuring each SLA have been provided for each SLA description below. While a measurement formula is provided, the VENDOR shall coordinate with the MOBILITY AUTHORITY to review, finalize, and agree upon all measurement formulas prior to execution of the Contract. The VENDOR shall document each approved, agreed upon measurement method within the Maintenance Plan for the MOBILITY AUTHORITY’s review and approval. The VENDOR shall be responsible for updating the Maintenance Plan to reflect the most current version of the measurement formula(s) upon request from or agreement between the MOBILITY AUTHORITY to modify any formulas(s) in the future.

1.2.7.3 Calculation of Damages for Consecutive Failures

Recurring and consecutive failure to comply with the SLAs provided in this Agreement may result in substantial harm to the MOBILITY AUTHORITY, but damages from such harm are difficult to quantify. Damages will increase for prolonged periods, and therefore for any SLA that is missed for three (3) consecutive months, the liquidated damages will be doubled for each subsequent month where the SLA is missed. The liquidated damages will revert to the original value upon the SLA being met for one (1) month.

1.3 SERVICE LEVEL AGREEMENT (SLA) DETAILS

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement				
RV1	RVSD – Volume Accuracy	Per lane volume provided by radar vehicle sensing devices (RVSD) shall be 95.00% accurate.	95.00%	For every 0.1% below the SLA, the VENDOR shall be subject to liquidated damages in the amount of 0.25% of the monthly maintenance fee. Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.	Every three (3) months, unless otherwise agreed upon by the MOBILITY AUTHORITY. VENDOR shall coordinate with the MOBILITY AUTHORITY monthly to determine a statistically significant sample size, as shown below, to show compliance with the SLA. VENDOR shall coordinate with the MOBILITY AUTHORITY to determine the specific RVSD(s) to be audited each period, minimum of three (3) average taken for all accuracy measurements. Accruing more errors than allowed, as indicated in the following table, shall result in an audit failure of SLA:				
					<table border="1"> <thead> <tr> <th>Sample Set</th> <th>Required Samples</th> <th>Allowable Errors</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>300</td> <td>15</td> </tr> <tr> <td>2</td> <td>250</td> <td>12</td> </tr> </tbody> </table>	Sample Set	Required Samples	Allowable Errors	1
Sample Set	Required Samples	Allowable Errors							
1	300	15							
2	250	12							
<p>Measurement Method:</p> $RVSD \text{ Volume Accuracy (\%)} = \left[1 - \left(\frac{Ground \ Truth \ Volume - RVSD \ Volume}{Ground \ Truth \ Volume} \right) \right] \times 100$ <p>Where,</p> <ul style="list-style-type: none"> RVSD Volume is the volume provided by the specific RVSD field device, subsystem, and system being measured Ground Truth Volume is the volume determined by manual means (e.g., recorded CCTV camera feeds) over the same time interval for which the specific RVSD is being measured. 									

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
RV2	RVSD – Availability	On average, each RVSD unit shall be available 99.50% of the time. Available is defined as functioning properly and recording accurate field conditions data.	99.50%	<p>For every 0.1% or portion thereof below the SLA, the VENDOR shall be subject to liquidated damages in the amount of 0.5% of the monthly maintenance fee.</p> <p>Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	Each month, as determined by the VENDOR provided monthly report(s), systemwide.
	<p>Measurement Method:</p> $RVSD \text{ Measured Availability } (\%) = \left[1 - \left(\frac{\text{Total Hours RVSD Downtime} - \text{Exclusions}}{\text{Total Expected Hours of Operation} - \text{Exclusions}} \right) \right] \times 100$ <p>Where,</p> <ul style="list-style-type: none"> ▪ The Expected Hours of Operation for each RVSD unit is 24 hours a day, seven (7) days a week. ▪ The <i>Total Expected Hours of Operation</i> is the sum of the Expected Hours of Operation for all deployed RVSD units in the SYSTEM. ▪ <i>Total Hours RVSD Downtime</i> is the sum of the down hours for all deployed RVSD units in the SYSTEM. 				

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
CC1	CCTV Camera – Availability	<p>On average, each CCTV camera shall be available 99.50% of the time. Available is defined as functioning properly, including responding to remote control functions (e.g., pan, tilt, zoom) and transmission of video streams without pixilation or dropped frames.</p> <p>This includes all camera models / types (e.g., dome enclosure and external positioner pan-tilt-zoom cameras; fixed or stationary cameras).</p>	99.50%	<p>For every 0.1% or portion thereof below the SLA, the VENDOR shall be subject to liquidated damages in the amount of 0.75% of the monthly maintenance fee.</p> <p>Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	Each month, as determined by the VENDOR provided monthly report(s), systemwide.
		<p>Measurement Method:</p> $CCTV \text{ Measured Availability } (\%) = \left[1 - \left(\frac{\text{Total Hours CCTV Camera Downtime} - \text{Exclusions}}{\text{Total Expected Hours of Operation} - \text{Exclusions}} \right) \right] \times 100$ <p>Where,</p> <ul style="list-style-type: none"> ▪ The Expected Hours of Operation for each CCTV Camera is 24 hours a day, seven (7) days a week. ▪ The <i>Total Expected Hours of Operation</i> is the sum of the Expected Hours of Operation for all deployed CCTV Cameras in the SYSTEM. ▪ <i>Total Hours CCTV Camera Downtime</i> is the sum of the down hours for all deployed CCTV Cameras in the SYSTEM. 			

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
DM1	DMS – Availability	<p>On average, each dynamic message sign (DMS) shall be available 99.50% of the time. Available is defined as functioning properly, including displaying proper messages / displays that are clearly legible and responding to remote control and diagnostic functions.</p>	99.50%	<p>For every 0.1% or portion thereof below the SLA, the VENDOR shall be subject to liquidated damages in the amount of 0.1% of the monthly maintenance fee.</p> <p>Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	Each month, as determined by the VENDOR provided monthly report(s).
		<p>Measurement Method:</p> $DMS \text{ Measured Availability } (\%) = \left[1 - \left(\frac{\text{Total Hours DMS Downtime} - \text{Exclusions}}{\text{Total Expected Hours of Operation} - \text{Exclusions}} \right) \right] \times 100$ <p>Where,</p> <ul style="list-style-type: none"> ▪ The Expected Hours of Operation for each DMS is 24 hours a day, seven (7) days a week. ▪ The <i>Total Expected Hours of Operation</i> is the sum of the Expected Hours of Operation for all deployed DMS in the SYSTEM. ▪ <i>Total Hours DMS Downtime</i> is the sum of the down hours for all deployed DMS in the SYSTEM. 			

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
CV1	Connected Vehicle RSU – Availability	<p>On average, each Connected Vehicle (CV) Roadside Unit (RSU) shall be available 95.00% of the time. Available is defined as functioning properly, including transmitting and receiving applicable messages as defined by the SAE J2735 standard.</p>	95.00%	<p>\$200 per each 1.0% below SLA threshold.</p> <p>Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	<p>Each month, as determined by the VENDOR provided monthly report(s).</p>
		<p>Measurement Method:</p> $RSU \text{ Measured Availability } (\%) = \left[1 - \left(\frac{\text{Total Hours RSU Downtime} - \text{Exclusions}}{\text{Total Expected Hours of Operation} - \text{Exclusions}} \right) \right] \times 100$ <p>Where,</p> <ul style="list-style-type: none"> ▪ The Expected Hours of Operation for each RSU is 24 hours a day, seven (7) days a week. ▪ The <i>Total Expected Hours of Operation</i> is the sum of the Expected Hours of Operation for all deployed RSU in the SYSTEM. ▪ <i>Total Hours DMS Downtime</i> is the sum of the down hours for all deployed RSU in the SYSTEM. 			

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement						
WW1	WWVDS – Event Accuracy	<p>Each vehicle traveling in the incorrect direction of an off-ramp shall be correctly identified and verified by the Wrong Way Vehicle Detection System (WWVDS) with 93.33% accuracy.</p> <p>Additionally, each WWVDS shall not produce significant false-positive events (e.g., greater than 5.00%).</p>	93.33%	<p>For every 3.33% below the SLA, the VENDOR shall be subject to liquidated damages in the amount of 1.5% of the monthly maintenance fee.</p> <p>Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	<p>Every six (6) months, as determined by the VENDOR audited sample WWVDS event detection data. This may be achieved by perform vendor testing runs to simulate wrong-way driving events.</p> <p>VENDOR shall coordinate with the MOBILITY AUTHORITY monthly to determine a statistically significant sample size, as shown below, to show compliance with the SLA.</p> <p>VENDOR shall coordinate with the MOBILITY AUTHORITY to determine the specific WWVDS site(s) to be audited each period.</p> <p>Accruing more errors (e.g., false-positives) than allowed, as indicated in the following table, shall result in an audit failure of SLA:</p> <table border="1" data-bbox="1255 919 1892 1094"> <thead> <tr> <th>Sample Set</th> <th>Required Samples</th> <th>Allowable Errors</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>30</td> <td>2</td> </tr> </tbody> </table>	Sample Set	Required Samples	Allowable Errors	1	30	2
					Sample Set	Required Samples	Allowable Errors				
1	30	2									
<p>Measurement Method:</p> $WWVDS \text{ Volume Accuracy (\%)} = \left[1 - \left(\frac{\text{Ground Truth Event Total} - WWVDS \text{ Events Detected}}{\text{Ground Truth Event Total}} \right) \right] \times 100$ <p>Where,</p> <ul style="list-style-type: none"> ▪ <i>WWVDS Events Detected</i> is the total number of events identified by the specific WWVDS being measured ▪ <i>Ground Truth Event Total</i> is the volume determined by manual means (e.g., recorded CCTV camera feeds, manual observation) over the same time interval for which the specific WWVDS is being measured. 											

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
WW2	WWVDS – Availability	Each Wrong Way Vehicle Detection Systems (WWVDS) shall be available 99% of the time. Available is defined as functioning properly, including properly identifying wrong-way driving vehicles, initiating a localized response (e.g., flashing signs), and alerting MOBILITY AUTHORITY personnel of confirmed wrong-way driving events.	99%	\$500 per each 1.0% below SLA threshold. Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.	Each month, as determined by the VENDOR provided monthly report(s).
	<p>Measurement Method:</p> $WWVDS \text{ Measured Availability } (\%) = \left[1 - \left(\frac{\text{Total Hours WWVDS Downtime} - \text{Exclusions}}{\text{Expected Hours of Operation} - \text{Exclusions}} \right) \right] \times 100$ <p>Where,</p> <ul style="list-style-type: none"> ▪ <i>Expected Hours of Operation</i> is 24 hours a day, seven (7) days a week ▪ <i>Total Hours WWVDS Downtime</i> is measured as the number of down hours for a single WWVDS. 				

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
VW1	Video Wall – Availability	<p>The video wall located in the TIMC shall be available 99.50% of the time. Available is defined as functioning properly, including properly displaying multiple live video feeds from CCTV cameras and allowing user-customizable display features.</p>	99.50%	<p>\$500 per each 0.5% below SLA threshold. Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	<p>Each month, as determined by the VENDOR provided monthly report(s).</p>
		<p>Measurement Method:</p> $\text{Video Wall Measured Availability (\%)} = \left[1 - \left(\frac{\text{Total Hours Video Wall Downtime} - \text{Exclusions}}{\text{Expected Hours of Operation} - \text{Exclusions}} \right) \right] \times 100$ <p>Where,</p> <ul style="list-style-type: none"> ▪ <i>Expected Hours of Operation</i> is 24 hours a day, seven (7) days a week 			

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
MM1	Monthly Maintenance Report – Processing Time	<p>The monthly report, accurately detailing system performance relative to the project SLAs, shall be submitted to the MOBILITY AUTHORITY within ten (10) business days of each month's end, commencing the first full month (Month 1) following Notice to Proceed.</p>	<p>Within ten (10) business days of each month's end.</p>	<p>For every one (1) calendar day outside the SLA, 0.5% of the monthly maintenance fee.</p> <p>Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	<p>Determined by the data Monthly Maintenance report received, measured by e-mail timestamp.</p>
		<p>Measurement Method:</p> $Report\ Tardiness\ (days) = Date_{Report\ Delivered} - Date_{Report\ Due}$			

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
AR1	Annual Report – Processing Time	<p>The VENDOR shall develop a comprehensive annual report accurately detailing the past year’s activities.</p> <p>The annual report, accurately detailing system performance relative to the project SLAs, shall be submitted to the MOBILITY AUTHORITY within ten (10) business days of the year’s end, measured twelve (12) full months following Notice to Proceed and each twelve (12) months following.</p>	<p>Within ten (10) business days of each year’s end.</p>	<p>For every one (1) calendar day outside the SLA, 0.1% of the monthly maintenance fee.</p> <p>Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	<p>Determined by the data Annual Report received, measured by e-mail timestamp.</p>
		<p>Measurement Method:</p> $Report\ Tardiness\ (days) = Date_{Report\ Delivered} - Date_{Report\ Due}$			

SLA ID	Name	Key Performance Indicator Description	Service Level Agreement	Damages	Measurement Requirement
RT1	Response Time	<p>Response times for repair services, as identified in Section Error! Reference source not found. – Error! Reference source not found., shall be no later than seventy-two (72) hours to the site, unless otherwise deemed necessary by the MOBILITY AUTHORITY.</p> <p>Response times for emergency maintenance, as identified in Section Error! Reference source not found. – Error! Reference source not found., shall be no later than four (4) hours to the site 24 X 7 X 365, unless otherwise deemed necessary by the MOBILITY AUTHORITY.</p>	<p>Repair Services: Respond within seventy-two (72) hours to the site</p> <p>Emergency Repair Services: Respond within four (4) hours to the site</p>	<p>For every response one (1) hour over the SLA, 0.1% of the monthly maintenance fee.</p> <p>For every response one (1) hour over the SLA, 0.5% of the monthly maintenance fee.</p> <p>Liquidated damages for the SLA are capped at a maximum of 25% of the monthly maintenance fee.</p>	Determined by repair documentation and/or audit by the MOBILITY AUTHORITY.
		<p>Measurement Method:</p> $Response\ Time(Hours) = Time_{Incident\ Reported} - Time_{On-Site\ Response}$			

APPENDIX G
Key Personnel

APPENDIX H
Contractor's Proposal

APPENDIX I-1
Form of Installation Performance Bond

FORM OF INSTALLATION PERFORMANCE BOND

AGREEMENT FOR INTELLIGENT TRANSPORTATION SYSTEM PERFORMANCE-BASED MAINTENANCE SERVICES

Bond No. _____

KNOW ALL PERSONS BY THESE PRESENTS, that that [_____], a [_____], as “Principal” and [_____], as “Surety” or as “Co-Sureties”, each a corporation duly organized under the laws of the State indicated on the attached page, having its principal place of business at the address listed on the attached page, in the State indicated on the attached page, and authorized as a surety in the State of Texas, are hereby jointly and severally held and firmly bound unto the CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY (the “Authority”), a political subdivision of the State of Texas, as “Obligee”, in the sum of [\$ _____] (the “Bonded Sum”), for the payment whereof Principal and Surety (or Co-Sureties), bind themselves, and their heirs, executors, administrators, representatives, successors, and assigns, jointly and severally, firmly by these presents.

WHEREAS, the Obligee, has awarded to Principal, the Agreement for Intelligent Transportation System Performance-Based Maintenance Services, duly executed and delivered as of [_____], 2023 (the “Agreement”), on the terms and conditions set forth therein; and

WHEREAS, upon the issuance of Work Authorization Number __, dated _____ pursuant to Article 2, subsection 2.1., Principal is required to furnish a bond guaranteeing the faithful performance of its obligations under the Agreement;

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION IS SUCH THAT, if Principal shall promptly and faithfully perform all of its obligations under the Agreement, including any and all amendments and supplements thereto, then this obligation shall be null and void; otherwise it shall remain in full force and effect. The Obligee shall release this bond upon the conclusion of the term of the Agreement as set forth in Article (7)(d)(ii) of the Agreement.

The following terms and conditions shall apply with respect to this bond:

1. The Agreement is incorporated by reference herein.
2. This bond specifically guarantees (1) the performance of each and every obligation of Principal under the Agreement, as it may be amended and supplemented, including but not limited to, its liability for liquidated damages as specified in the Agreement, but not to exceed the penal amount described in Article (7)(d)(ii).
3. Whenever Principal shall be, and is declared by the Obligee to be, in default under the Agreement and the Obligee has formally terminated the Principal’s right to complete the Services required under the Agreement, provided that the Obligee is not then in material default thereunder, Surety shall promptly take one of the following actions with the consent of the Obligee:
 - a. arrange for the Principal to perform and complete the Agreement;

b. complete the Services required under the Work Authorization then in effect in accordance with the terms and conditions of the Agreement then in effect, through its agents or through independent contractors;

c. obtain bids or negotiated proposals from qualified contractors acceptable to the Obligee for a contract for performance and completion of the Services required under the Work Authorization, arrange for a contract to be prepared for execution by the Obligee and the contractor selected with the Obligee's concurrence, to be secured with performance and payment bonds executed by a qualified surety equivalent to the bonds issued on the Agreement in an amount that corresponds to the amount of the Work Authorization to be completed, and pay to the Obligee the amount of damages as described in Article 7 of the Agreement; or

d. waive its right to perform and complete, arrange for completion, or obtain a new contractor and with reasonable promptness under the circumstances, (i) after investigation, determine the amount for which it may be liable to the Obligee and, as soon as practicable after the amount is determined, tender payment therefore to the Obligee, or (ii) deny liability in whole or in part and notify the Obligee citing reasons therefore.

5. If Surety does not proceed as provided in Paragraph 3 with reasonable promptness, Surety shall be deemed to be in default on this Bond fifteen (15) days after receipt of an additional written notice from the Obligee to Surety demanding that Surety perform its obligations under this Bond, and the Obligee shall be entitled to enforce any remedy available to the Obligee. If Surety proceeds as provided in Subparagraph 3.d, and the Obligee refuses the payment tendered or Surety has denied liability, in whole or in part, without further notice the Obligee shall be entitled to enforce any remedy available to the Obligee.

6. After the Obligee has terminated the Principal's right to complete the Agreement, and if Surety elects to act under Subparagraph 3.a, 3.b, or 3.c above, then the responsibilities of Surety to the Obligee shall not be greater than those of the Principal under the Agreement, and the responsibilities of the Obligee to Surety shall not be greater than those of the Obligee under the Agreement. To the limit of the Bonded Sum, Surety is obligated without duplication for:

a. the responsibilities of the Principal for correction of defective work and completion of the Services required under the Agreement;

b. additional legal and delay costs resulting from Principal's default, and resulting from the actions or failure to act of Surety under Paragraph 3; and

c. liquidated damages under the Agreement.

7. No alteration, modification or supplement to the Agreement or the nature of the work to be performed thereunder, including without limitation any extension of time for performance, shall in any way affect the obligations of Surety under this bond.

8. Correspondence or claims relating to this bond should be sent to Surety at the following address:

9. No right of action shall accrue on this bond to or for the use of any entity other than the Obligee or its successors and assigns.

10. If any legal action be filed on this bond, venue shall be in Travis County, Texas.

11. This bond is executed in accordance with the provisions of Chapter 2253 of the Texas Government Code, as amended.

12. Initially capitalized terms not otherwise defined herein shall have the definition set forth in the Agreement.

IN WITNESS WHEREOF, Principal and Surety have caused this bond to be executed and delivered as of [_____], 202[_____].

Principal:

By: _____
Its: _____
(Seal)

Surety:

By: _____
Its: _____
(Seal)

[ADD APPROPRIATE SURETY ACKNOWLEDGMENTS]

APPENDIX I-2
Form of Installation Payment Bond

FORM OF INSTALLATION PAYMENT BOND

AGREEMENT FOR INTELLIGENT TRANSPORTATION SYSTEM PERFORMANCE-BASED MAINTENANCE SERVICES

Bond No. _____

KNOW ALL PERSONS BY THESE PRESENTS, that that [_____], a [_____], as “Principal” and [_____], as “Surety” or as “Co-Sureties”, each a corporation duly organized under the laws of the State indicated on the attached page, having its principal place of business at the address listed on the attached page, in the State indicated on the attached page, and authorized as a surety in the State of Texas, are hereby jointly and severally held and firmly bound unto the CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY (the “Authority”), a political subdivision of the State of Texas, as “Obligee”, in the sum of [\$_____] (the “Bonded Sum”), for the payment whereof Principal and Surety (or Co-Sureties), bind themselves, and their heirs, executors, administrators, representatives, successors, and assigns, jointly and severally, firmly by these presents.

WHEREAS, the Obligee, has awarded to Principal, the Agreement for Intelligent Transportation System Performance-Based Maintenance Services, duly executed and delivered as of [_____], 2023 (the “Agreement”), on the terms and conditions set forth therein; and

WHEREAS, upon the issuance of Work Authorization Number __, dated _____ pursuant to Article 2, subsection 2.1., Principal is required to furnish a bond guaranteeing payment of claims, subcontractors, suppliers, materialmen and mechanics.

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION IS SUCH THAT, if Principal shall fail to pay any valid and timely claims of subcontractors, suppliers, materialmen and mechanics with respect to the Services, then Surety shall pay for the same in an amount not to exceed, in the aggregate, the Bonded Sum; otherwise this obligation shall be null and void upon the conclusion of the term of the Agreement as set forth in Article (7)(d)(ii) of the Agreement.

The following terms and conditions shall apply with respect to this bond:

1. The Agreement is incorporated by reference herein.
2. No alteration, modification or supplement to the Agreement or the nature of the work to be performed thereunder, including without limitation any extension of time for performance, shall in any way affect the obligations of Surety under this bond.
3. Correspondence or claims relating to this bond should be sent to Surety at the following address:

4. This bond shall inure to the benefit of the persons identified above so as to give a right of action to such persons and their assigns in any suit brought upon this bond.

5. To the extent permitted by law, the only permitted claimants under this Bond shall be those entities having a contract with Principal and those entities having a contract with an entity which has a contract with Principal.

6. If any legal action be filed on this bond, venue shall be in Travis County, Texas.

7. This bond is executed in accordance with the provisions of Chapter 2253 of the Texas Government Code, as amended.

8. Initially capitalized terms not otherwise defined herein shall have the definition set forth in the Agreement.

IN WITNESS WHEREOF, Principal and Surety have caused this bond to be executed and delivered as of [_____], 202[___].

Principal: _____

By: _____

Its: _____

(Seal)

Surety: _____

By: _____

Its: _____

(Seal)

[ADD APPROPRIATE SURETY ACKNOWLEDGMENTS]

APPENDIX J-1
Form of Maintenance Performance Bond

FORM OF MAINTENANCE PERFORMANCE BOND

AGREEMENT FOR INTELLIGENT TRANSPORTATION SYSTEM PERFORMANCE-BASED MAINTENANCE SERVICES

Bond No. _____

KNOW ALL PERSONS BY THESE PRESENTS, that that [_____], a [_____], as “Principal” and [_____], as “Surety” or as “Co-Sureties”, each a corporation duly organized under the laws of the State indicated on the attached page, having its principal place of business at the address listed on the attached page, in the State indicated on the attached page, and authorized as a surety in the State of Texas, are hereby jointly and severally held and firmly bound unto the CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY (the “Authority”), a political subdivision of the State of Texas, as “Obligee”, in the sum of [\$ _____] (the “Bonded Sum”), for the payment whereof Principal and Surety (or Co-Sureties), bind themselves, and their heirs, executors, administrators, representatives, successors, and assigns, jointly and severally, firmly by these presents.

WHEREAS, the Obligee, has awarded to Principal, the Agreement for Intelligent Transportation System Performance-Based Maintenance Services, duly executed and delivered as of [_____], 2023 (the “Agreement”), on the terms and conditions set forth therein; and

WHEREAS, as prior to the issuance of the Work Authorization under Article 2, subsection 2.2., Principal is required to furnish a bond guaranteeing the faithful performance of its obligations under the Agreement;

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION IS SUCH THAT, if Principal shall promptly and faithfully perform all of its obligations under the Agreement, including any and all amendments and supplements thereto, then this obligation shall be null and void; otherwise it shall remain in full force and effect. The Obligee shall release this bond upon the conclusion of the term of the Agreement as set forth in Article (7)(d)(iii) of the Agreement.

The following terms and conditions shall apply with respect to this bond:

1. The Agreement is incorporated by reference herein.
2. This bond specifically guarantees (1) the performance of each and every obligation of Principal under the Agreement, as it may be amended and supplemented, including but not limited to, its liability for liquidated damages as specified in the Agreement and loss of revenue incurred by the CTRMA under Article 7(b), but not to exceed the penal amount described in Article (7)(d)(iii).
3. Whenever Principal shall be, and is declared by the Obligee to be, in default under the Agreement and the Obligee has formally terminated the Principal’s right to complete the Services required under the Agreement, provided that the Obligee is not then in material default thereunder, Surety shall promptly take one of the following actions with the consent of the Obligee:

- a. arrange for the Principal to perform and complete the Agreement;
- b. complete the Services required under any Work Authorization(s) then in effect in accordance with the terms and conditions of the Agreement then in effect, through its agents or through independent contractors;
- c. obtain bids or negotiated proposals from qualified contractors acceptable to the Obligee for a contract for performance and completion of the Services required under any Work Authorization(s) then in effect, arrange for a contract to be prepared for execution by the Obligee and the contractor selected with the Obligee's concurrence, to be secured with performance and payment bonds executed by a qualified surety equivalent to the bonds issued on the Agreement in an amount that corresponds to the amount of Work Authorization(s) to be completed, and pay to the Obligee the amount of damages as described in Article 7 of the Agreement; or
- d. waive its right to perform and complete, arrange for completion, or obtain a new contractor and with reasonable promptness under the circumstances, (i) after investigation, determine the amount for which it may be liable to the Obligee and, as soon as practicable after the amount is determined, tender payment therefore to the Obligee, or (ii) deny liability in whole or in part and notify the Obligee citing reasons therefore.

5. If Surety does not proceed as provided in Paragraph 3 with reasonable promptness, Surety shall be deemed to be in default on this Bond fifteen (15) days after receipt of an additional written notice from the Obligee to Surety demanding that Surety perform its obligations under this Bond, and the Obligee shall be entitled to enforce any remedy available to the Obligee. If Surety proceeds as provided in Subparagraph 3.d, and the Obligee refuses the payment tendered or Surety has denied liability, in whole or in part, without further notice the Obligee shall be entitled to enforce any remedy available to the Obligee.

6. After the Obligee has terminated the Principal's right to complete the Agreement, and if Surety elects to act under Subparagraph 3.a, 3.b, or 3.c above, then the responsibilities of Surety to the Obligee shall not be greater than those of the Principal under the Agreement, and the responsibilities of the Obligee to Surety shall not be greater than those of the Obligee under the Agreement. To the limit of the Bonded Sum, Surety is obligated without duplication for:

- a. the responsibilities of the Principal for correction of defective work and completion of the Services required under the Agreement;
- b. additional legal and delay costs resulting from Principal's default, and resulting from the actions or failure to act of Surety under Paragraph 3; and
- c. liquidated damages under the Agreement.

7. No alteration, modification or supplement to the Agreement or the nature of the work to be performed thereunder, including without limitation any extension of time for performance, shall in any way affect the obligations of Surety under this bond.

8. Correspondence or claims relating to this bond should be sent to Surety at the following address:

9. No right of action shall accrue on this bond to or for the use of any entity other than the Obligee or its successors and assigns.

10. If any legal action be filed on this bond, venue shall be in Travis County, Texas.

11. This bond is executed in accordance with the provisions of Chapter 2253 of the Texas Government Code, as amended.

12. Initially capitalized terms not otherwise defined herein shall have the definition set forth in the Agreement.

IN WITNESS WHEREOF, Principal and Surety have caused this bond to be executed and delivered as of [____], 202[].

Principal:

By: _____

Its: _____

(Seal)

Surety:

By: _____

Its: _____

(Seal)

[ADD APPROPRIATE SURETY ACKNOWLEDGMENTS]

APPENDIX J-2
Form of Maintenance Payment Bond

FORM OF MAINTENANCE PAYMENT BOND

AGREEMENT FOR INTELLIGENT TRANSPORTATION SYSTEM PERFORMANCE-BASED MAINTENANCE SERVICES

Bond No. _____

KNOW ALL PERSONS BY THESE PRESENTS, that that [_____], a [_____], as “Principal” and [_____], as “Surety” or as “Co-Sureties”, each a corporation duly organized under the laws of the State indicated on the attached page, having its principal place of business at the address listed on the attached page, in the State indicated on the attached page, and authorized as a surety in the State of Texas, are hereby jointly and severally held and firmly bound unto the CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY (the “Authority”), a political subdivision of the State of Texas, as “Obligee”, in the sum of [\$_____] (the “Bonded Sum”), for the payment whereof Principal and Surety (or Co-Sureties), bind themselves, and their heirs, executors, administrators, representatives, successors, and assigns, jointly and severally, firmly by these presents.

WHEREAS, the Obligee, has awarded to Principal, the Agreement for Intelligent Transportation System Performance-Based Maintenance Services, duly executed and delivered as of [_____], 2023 (the “Agreement”), on the terms and conditions set forth therein; and

WHEREAS, prior to the issuance of the Work Authorization under Article 2, subsection 2.2., Principal is required to furnish a bond guaranteeing payment of claims, subcontractors, suppliers, materialmen and mechanics.

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION IS SUCH THAT, if Principal shall fail to pay any valid and timely claims of subcontractors, suppliers, materialmen and mechanics with respect to the Services, then Surety shall pay for the same in an amount not to exceed, in the aggregate, the Bonded Sum; otherwise this obligation shall be null and void upon the conclusion of the term of the Agreement as set forth in Article (7)(d)(iii) of the Agreement.

The following terms and conditions shall apply with respect to this bond:

1. The Agreement is incorporated by reference herein.
2. No alteration, modification or supplement to the Agreement or the nature of the work to be performed thereunder, including without limitation any extension of time for performance, shall in any way affect the obligations of Surety under this bond.
3. Correspondence or claims relating to this bond should be sent to Surety at the following address:

4. This bond shall inure to the benefit of the persons identified above so as to give a right of action to such persons and their assigns in any suit brought upon this bond.

5. To the extent permitted by law, the only permitted claimants under this Bond shall be those entities having a contract with Principal and those entities having a contract with an entity which has a contract with Principal.

6. If any legal action be filed on this bond, venue shall be in Travis County, Texas.

7. This bond is executed in accordance with the provisions of Chapter 2253 of the Texas Government Code, as amended.

8. Initially capitalized terms not otherwise defined herein shall have the definition set forth in the Agreement.

IN WITNESS WHEREOF, Principal and Surety have caused this bond to be executed and delivered as of [____], 202[___].

Principal: _____

By: _____

Its: _____

(Seal)

Surety: _____

By: _____

Its: _____

(Seal)

[ADD APPROPRIATE SURETY ACKNOWLEDGMENTS]



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #11

Discuss and consider approving an agreement with Deloitte Consulting LLP for enhancement development of the Mobility Authority's Data Platform System

Strategic Plan Relevance:	Innovation
Department:	Operations
Contact:	Greg Mack, Director of Information Technology
Associated Costs:	Not to exceed \$500,000
Funding Source:	FY24 Capital Budget
Action Requested:	Consider and act on draft resolution

Project Description/Background: To provide more flexibility in the future, in March 2021, the Mobility Authority awarded a contract to Deloitte Consulting LLP (Deloitte) to develop a system wherein all toll transaction processing and data management capabilities after the point of transaction creation are advanced to a Mobility Authority-managed solution. The Data Platform System (DPS) is the next step in the agency's evolution to a mature toll entity that controls transaction pricing and revenue recognition timing. The DPS will also provide the Authority with more insight into its transactional data, providing the ability to make better informed decisions regarding collection initiatives, transportation improvements, and other planning efforts.

The objective of the DPS is to transition all toll transaction data processing and data management capabilities after the point of transaction creation to a Mobility Authority-managed solution. Kapsch and ETC, the Authority's lane vendors, will collect the toll transaction at the roadside and forward the transaction and vehicle images to the DPS. Business logic will then consume the transaction and route the data to either the Central United States Interoperability (CUSIOP) Hub or the Pay by Mail (PBM) vendor for payment. The payment status is ultimately passed back to the DPS allowing complete reconciliation of all the Authority's toll transactions.

Development for the first two project releases was completed September 2021 on schedule. These releases created the base code as well as the routing and exchange processes. Release 3 supports development for pricing and billing transactions, defining how data governance is handled in the new processing schema, and identifying the suite of reports necessary to account for the agency's revenue and monitor performance. Release 3 is anticipated to be completed this month. The DPS went live in August 2023, and has been running in parallel to the current system since that time.

The Mobility Authority desires additional development services as the system matures. Enhancements to DPS would include new functionality that is not covered in the Operations and Maintenance scope of work. Today's action is directly related to the engagement of resources for such development.

Previous Actions & Brief History of the Program/Project: An initial contract for the development of DPS Releases 1 & 2 was awarded to Deloitte in February 2021; the contract was subsequently approved in March 2021. A contract for the development of Release 3 was awarded to Deloitte in September 2021. The initial one-year O&M contract was awarded to Deloitte in June 2022; three amendments to that contract have been issued to provide services through September 2023.

Financing: FY24 Capital Budget

Action requested/Staff Recommendation: Staff recommends approving an agreement with Deloitte Consulting LLP for consulting services for enhancement development of the Mobility Authority's Data Platform System.

Backup provided:

- Draft Resolution
- CTRMA TOMS Enhancements Statement of Work (dated 9/15/23)
- DIR Public Records Act Agreement – Deloitte Consulting Enhancements Statement of Work
- DIR Vendor Agreement – Deloitte Consulting O&M Enhancements

**GENERAL MEETING OF THE BOARD OF DIRECTORS
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**

RESOLUTION NO. 23-0XX

**APPROVING AN AGREEMENT WITH DELOITTE CONSULTING LLP FOR
ENHANCEMENT DEVELOPMENT OF THE MOBILITY AUTHORITY'S DATA PLATFORM
SYSTEM**

WHEREAS, as of August 1, 2023, the Mobility Authority has been utilizing its own data platform for all toll transaction data processing and data management capabilities after the point of transaction creation (the "Data Platform System"); and

WHEREAS, the Data Platform System also supports new business capabilities such as external reporting, data analytics and a connection to the Texas Department of Motor Vehicles' datasets to allow better informed agency decision making; and

WHEREAS, the Mobility Authority staff desires additional enhancements to the Data Platform System to add new capabilities and improve functionality; and

WHEREAS, the Executive Director has negotiated a scope of work with Deloitte Consulting LLP in an amount not to exceed \$500,000 for additional development services and enhancements to the Data Platform System which is attached hereto as Exhibit A; and

WHEREAS, pursuant to Texas Government Code Section 2054.0565 and Mobility Authority Policy Code Section 401.008, the Mobility Authority may utilize procedures established by the Texas Department of Information Resources (DIR) to procure goods and services through DIR cooperative contracts; and

WHEREAS, the Executive Director recommends entering into an agreement with Deloitte Consulting LLP for additional development services and enhancements to the Data Platform System in an amount not to exceed \$500,000 through their DIR cooperative contract.

NOW THEREFORE BE IT RESOLVED that the Board of Directors hereby approves the scope of work for additional development services and enhancements to the Data Platform System which is attached hereto as Exhibit A; and

BE IT FURTHER RESOLVED, that the Executive Director is authorized to enter into an agreement with Deloitte Consulting LLP in an amount not to exceed \$500,000 through their cooperative contract with the Texas Department of Information Resources for additional development services and enhancements to the Data Platform System.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

Robert W. Jenkins, Jr.
Chairman, Board of Directors

Exhibit A



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

Statement of Work

Tolling Operations Management Solution (TOMS)

2023 – 2024 Enhancements

October 25, 2023

Contents

1.	Statement of Work Purpose and Overview.....	3
1.1.	Term.....	3
2.	Scope of Services	3
2.1.	Requirements Services	3
2.2.	Design Services	4
2.3.	Development Services	4
2.4.	Testing Services	4
2.5.	User Acceptance Testing (UAT) Services	5
2.6.	Release Services	5
2.7.	Warranty Services.....	5
3.	Deliverables	6
3.1.	Description	6
3.2.	Vendor Deliverables & Payment Allocation	7
3.3.	Invoices.....	7
3.4.	Acceptance Management.....	7
4.	Project Governance	9
4.1.	Project Issues Management	9
4.2.	Change Process.....	9
4.3.	Unforeseen Conditions and Events	10
4.4.	Delays and Extensions	10
5.	Additional Terms and Conditions	11
6.	Compliance with CTRMA Information Security Guidelines	12
7.	CTRMA Provided Services.....	12
7.1.	Location of Work, Hours and Conditions	12
	Appendix A: CTRMA Information Security Policy	13

1. Statement of Work Purpose and Overview

The Tolling Operations Management Solution (“TOMS”) is an aggregate of multiple integrated solutions that support the CTRMA transaction to cash lifecycle. TOMS fully or partially automates business processes across several operational domains including Transaction Management, Product Management, Payment Path Management, Discount Management, Billing Management, Data Exchange Management, and Reporting & Analytics Management.

The purpose of this Statement of Work (“SOW”) is to define a suite of services necessary to support the development and implementation of requested enhancements to components of the existing TOMS Ecosystem. This SOW is intended to serve as a basis of understanding between CTRMA and a 3rd party Vendor (“Vendor”) for the services contracted.

1.1. Term

The Effective Date of this Contract is October 1, 2023, or the date on which this Contract is fully executed and approved according to applicable laws, rules, and regulations, whichever is later. This Contract terminates on June 30, 2024, unless otherwise terminated or extended in accordance with its terms.

2. Scope of Services

Vendor will provide the following services to CTRMA (Vendor Deliverables are noted in ***bold Italics***):

2.1. Requirements Services

CTRMA will define and document the business requirements for each scoped and prioritized feature. The business requirements will describe the expected functionality and may also include supporting artifacts such as logical models, information flow diagrams, and annotated wireframes. CTRMA will document all business requirements artifacts within the appropriate CTRMA Jira project.

In some instances, CTRMA may provide screenshots or other representations of current state for reference but are not to be considered as future state requirements.

Vendor and CTRMA will collectively review the documented business requirements and address any required clarifications.

Vendor will develop a rough order of magnitude (ROM) cost and estimated timeline for the scoped feature and present to CTRMA. Vendor and CTRMA will iteratively review and discuss the cost and estimations. If CTRMA approves the cost and estimated schedule, the feature will be moved into the Design phase. Should CTRMA decide not to proceed, the feature will be moved out of scope and placed into an appropriate backlog.

2.1.1. Vendor Requirements Services & Deliverables

- Review and analyze requirements documentation provided by CTRMA
- Identify risks and/or constraints and present feedback to CTRMA on documented requirements
- Develop cost and estimated schedule to deliver the scoped requirements
- Present rough order of magnitude (ROM) solution costs and estimated schedule to CTRMA for review and approval to proceed.

2.2. Design Services

Vendor will develop one or more designs that will provide functionality meeting the requirements defined as in scope. The initial design(s) will be presented to CTRMA for iterative review and input with the Vendor updating the initial design(s) as required. Vendor will present a final design to CTRMA that includes a revised cost and estimated schedule. If CTRMA approves the cost and estimated schedule, the feature will be moved into the Development phase. Should CTRMA decide not to proceed, the feature will be moved out of scope and placed into an appropriate backlog.

2.2.1. Vendor Design Services & Deliverables

- Create one or more recommended application designs to satisfy the documented requirements
- Create visual representations of proposed solution design(s) and risks/constraints associated with each
- Include modular and scalable solution design and architecture in recommended design(s)
- Present and review draft solution design(s), costs and estimated schedule with risk and constraints to CTRMA
- Develop revised cost and estimated schedule to deliver CTRMA selected design(s), if necessary
- ☑ ***Present final design, cost and estimated schedule to CTRMA for review and acceptance***

2.3. Development Services

Vendor will manage and complete all required solution development activities. Once completed, Vendor will present a development retrospective to CTRMA. Once accepted by CTRMA, the feature will be moved into the Testing phase.

2.3.1. Vendor Development Services & Deliverables

- Provide all application development services necessary to build the CTRMA selected design(s)
- Coordinate with CTRMA TOMS O&M Support to stand-up any/all necessary sandbox, development, and testing environments
- Manage Vendor application development resources, approach and planning
- Include modular, scalable, and/or re-usable code in all development where possible
- ☑ ***Present development retrospective including summary of modular, scalable, or re-usable code applied to CTRMA for review and acceptance***

2.4. Testing Services

Vendor will develop the testing plan and facilitate all required testing for the feature. Vendor will document the tests to be completed, expected outcomes, and actual outcomes. Vendor will document, track and manage all issues identified during testing as defects through resolution. Once all testing has been successfully completed and documented, Vendor will provide a demo of the testing results and accompanying test and defect documentation to CTRMA. After CTRMA acceptance, the feature will move into the UAT phase.

2.4.1. Vendor Testing Services & Deliverables

- Provide all testing services necessary to ensure quality assurance for developed solution(s)
- Document test cases including test scenarios, expected outcomes and actual outcomes
- ☑ ***Present documented test cases to CTRMA for review and acceptance***

- Complete all necessary smoke, unit, integration, functional, and performance testing to ensure solution quality assurance
- Coordinate with CTRMA TOMS O&M Support team to perform any/all necessary regression testing
- Document, track and manage all defects identified during testing using CTRMA Jira procedures
- ☑ ***Present a testing retrospective including documented test cases and defect resolution summary to CTRMA for review and acceptance***

2.5. User Acceptance Testing (UAT) Services

CTRMA will define the UAT scripts and facilitate any required user acceptance testing. Issues identified during UAT will be documented by CTRMA and reviewed with the Vendor. For any identified issues, CTRMA will work with the Vendor to determine if the issue is a Defect or new Requirement Specification.

For issues identified as a new Requirement Specification, CTRMA will document the requirements and add them to the TOMS Backlog for future enhancement consideration.

Issues identified as Defects will be addressed by the Vendor and are considered required for final feature acceptance. All Defects will be tracked in the CTRMA Jira system in accordance with CTRMA Jira policies and procedures. Once all Defects have been resolved and any additional UAT completed, Vendor will present a retrospective and accompanying Defect documentation to CTRMA for acceptance. Accepted features will then be moved to the Release phase.

2.5.1. Vendor Services & Deliverables

- Document, track and manage all defects identified during UAT using CTRMA Jira procedures
- ☑ ***Present a UAT retrospective with accompanying defect summary to CTRMA for review and acceptance***

2.6. Release Services

Vendor will work with the CTRMA TOMS O&M Support team to incorporate the feature into a Release Plan. Once the feature has been released to the production environment, Vendor will notify CTRMA in writing and the feature has moved into the Warranty phase.

2.6.1. Vendor Release Services & Deliverables

- Coordinate with the CTRMA TOMS O&M Support team to assign the solution to an appropriate production release
- ☑ ***Provide written notice to CTRMA that the solution has been moved into the production environment***

2.7. Warranty Services

Unless otherwise mutually agreed, the Warranty Period shall be 60 calendar days starting from the date the feature was released into production. For issues identified as Defects during the Warranty Period, the Vendor shall, at no additional charge to CTRMA, furnish such materials and services necessary to correct any Defects related to the released feature. Once the Warranty Period has ended and all Defects identified during the Warranty Period have been resolved, Vendor will present a retrospective and accompanying Warranty Period Defect summary documentation to CTRMA for acceptance.

2.7.1. Vendor Warranty Services & Deliverables

- Document, track and manage all defects identified during the Warranty Period using CTRMA Jira procedures.
- Provide all Development Services as defined in section 2.3 to resolve all defect(s) identified during the Warranty Period
- Provide all Testing Services as defined in section 2.4 to resolve all defect(s) identified during the Warranty Period
- Provide all UAT Services as defined in section 2.5 to resolve all defect(s) identified during the Warranty Period
- ☑ ***Present a Warranty Period retrospective with accompanying defect resolution summary to CTRMA for review and acceptance***

3. Deliverables

3.1. Description

“Deliverables” means all materials, documents, software (if any) and any other items set forth in this Agreement that are in scope and are originally created, developed, or produced by Vendor specifically for delivery to CTRMA.

The detailed Acceptance Criteria for each Deliverable or Service will be determined and agreed to with CTRMA, prior to the commencement of work on any Deliverable or Service. Changes to this list of Deliverables and/or Acceptance Criteria, or the definition or content of such Deliverables as described by Vendor’s management and delivery methods, or the party responsible for a Deliverable will be managed via the Change Process as defined in Section 4.2.

Both parties shall agree upon Acceptance Criteria consistent with the “SMART” Method of defining acceptance criteria, i.e., Specific, Measurable, Achievable, Relevant, and Time-bound. Notwithstanding the Vendor’s commencement or completion of any Deliverable under this Agreement, the Vendor will not submit any Deliverable or Service to CTRMA for review and CTRMA will be under no obligation to review, Accept or Reject any Deliverable or Service until the Acceptance Criteria for that Deliverable has been defined and agreed to by both parties.

Further, the Vendor is not obligated to start work on a specific Deliverable or Work Product until the parties have agreed in writing on the Acceptance Criteria for that Deliverable or Work Product, nor is the Vendor responsible for any delays caused by a failure of CTRMA to timely agree on the Acceptance Criteria.

Formal Acceptance by CTRMA of the Deliverables and Services is the sole indication that the Deliverables or Services have been completed in accordance with this Agreement. Neither party may unreasonably withhold Formal Acceptance where the agreed upon Acceptance Criteria for the Deliverable or Service have been satisfied.

3.2. Vendor Deliverables & Payment Allocation

For each scoped and prioritized feature, the Vendor will deliver the following as Deliverables as defined in Section 2: Scope of Services:

Phase	Deliverable	Payment Allocation
Design	Present final design, cost, and estimated schedule to CTRMA for review and acceptance.	20%
Development	Present development retrospective including summary of modular, scalable, or re-usable code applied to CTRMA for review and acceptance.	20%
Testing	Present documented test cases to CTRMA for review and acceptance. Present a testing retrospective including documented test cases and defect resolution summary to CTRMA for review and acceptance.	20%
UAT	Present a UAT retrospective with accompanying defect summary to CTRMA for review and acceptance.	30%
Release	Provide written notice to CTRMA that the solution has been moved into the production environment.	-
Warranty	Present a Warranty Period retrospective with accompanying defect resolution summary to CTRMA for review and acceptance.	10%

3.3. Invoices

The Vendor may invoice CTRMA after each Payment Deliverable is accepted. CTRMA will not make partial payments for deliverable subtasks.

This pricing is subject to and governed by the DBITS terms and conditions as set forth in DBITS # DIR-CPO-4919. CTRMA will purchase any additional required software, hardware, and hosting in support of the agreed upon Scope of Work. All Google Cloud Platform services are available on Texas DIR contract # DIR-TSO-4162, via Google Cloud’s exclusive government distributor, Carahsoft Technology Corporation.

3.4. Acceptance Management

Acceptance by CTRMA of the project’s Services and Deliverables means that the Services and Deliverables have been completed in accordance with this Agreement.

Vendor and CTRMA will agree upon acceptance criteria for the Services and each Deliverable. Acceptance criteria must be documented prior to the commencement of work on any Deliverable or Service. The parties agree to the following Acceptance Management process:

The respective Project Manager will submit a Deliverable and Service Acceptance form for each completed Deliverable or Service to the designated Approver.

1. The following Acceptance Definitions apply to this SOW:

- a. **Accepted:** The deliverable is approved 'As Is' and is considered complete.
 - b. **Rejected:** Does not meet Acceptance criteria and is returned for remediation (see below requirements for Rejected).
 - c. **Conditional Acceptance:** Is considered Accepted (for invoicing purposes only) under the condition that minor modifications and or updates that do not impact the holistic content of the Deliverable (See below requirements for Conditional Acceptance)
2. CTRMA approver will Accept (by written notice of Acceptance or Conditional Acceptance) or reject the Services and/or Deliverable within five (5) business days from the receipt of the acceptance form from the Vendor Project Manager.
 3. If CTRMA approver does not accept or reject the Deliverables and/or Services within five (5) business days from the receipt of the acceptance form from the Vendor Project Manager and does not communicate a reasonable timeframe in which a decision will be made, the Deliverables and Services will be considered accepted.
 - a. Work will progress to maintain the established project schedule, with the understanding that any changes to an Accepted Deliverable or Service may constitute a change in scope, and for any change that is determined to be a change in scope the parties will invoke the Escalation Process (See Issues Management).
 - b. A Change Order may result if modifications to the Accepted Deliverable or Service are required, and those modifications affect Accepted or in-progress project work.
 4. If CTRMA approver Conditionally Accepts a Deliverable or Service, the cause for the Conditional Acceptance and any known defects CTRMA wants to be addressed will be documented by CTRMA and provided to the Vendor in a notice of Conditional Acceptance as set forth above. The Vendor will correct or revise the Deliverable or Service, as applicable, and resubmit to CTRMA for review within five (5) business days from the receipt of CTRMA's notice of Conditional Acceptance or such other time as agreed upon in writing between the parties, unless the Vendor is not in agreement with the Conditional Acceptance, in which case the parties will invoke the Escalation Process as set forth in this Amendment. A Deliverable or Service is deemed complete when CTRMA has formally Accepted the Service or Deliverable under the process set forth in this section.
 5. If CTRMA rejects any Services or Deliverable, the cause for rejection and all non-conformities and defects to be addressed must be documented by CTRMA and provided to Vendor for Vendor to correct or revise. The Vendor will correct or revise the Deliverable or Service, as applicable, and resubmit to CTRMA for review withing five (5) business days from receipt of CTRMA's notice of Rejection or such other time as agreed upon in writing between the parties, unless the Vendor is not in agreement with the Rejection, in which case the parties will invoke the Escalation Process set forth in this Amendment. Any Services and Deliverables are deemed complete upon re-performance and/or resubmission of the corrected or revised Services or Deliverable by Vendor to CTRMA.

The following person(s) has been designated as the CTRMA approver of Deliverables and Services for the project:

Name: *Greg Mack*
 Title: *Director of Information Technology*

4. Project Governance

4.1. Project Issues Management

Throughout the Term of the Agreement, issues may arise requiring further information or a decision for resolution. The project team’s objective is to resolve all issues at the lowest level possible. When an issue cannot be resolved at the project team level, the following escalation path will be followed. Each contact shall have the amount of time indicated in the “Response Time” column for bringing resolution to the issue, prior to the issue being escalated to the next contact level.

Table 1: Escalation Contacts

Tier	Vendor	CTRMA	Response Time
First Level Contact	<i>Name, Title</i>	Name, Title	Three (3) business days
Second Level Contact	<i>Name, Title</i>	Name, Title	Three (3) business days
Third Level Contact	<i>Name, Title</i>	Name, Title	Three (3) business days

Should no resolution be reached after following this escalation path, either party may terminate this Agreement as a termination for convenience subject to the Early Termination provisions defined herein, and/or to the dispute resolution process defined in the Agreement, if any, and exercise any other rights and remedies available at law or in equity.

4.2. Change Process

The following Change Process will be used to manage all alterations to this Agreement. Examples of alterations include but are not limited to changes in scope, to Deliverables (including accepted Deliverables), to the schedule and to costs occurring for any reason, including failure of CTRMA to fulfill its roles and responsibilities, unforeseen events, delays caused by CTRMA, and inaccurate assumptions and dependencies. Vendor will not perform services not described in this Agreement until a Change Order has been approved.

4.2.1. Change Order Process

1. Either party shall notify the other of requested changes by completing a “**Change Order**” (“**CO**”) form that provides justification for the change and the proposed impact to the scope, schedule, and cost.
2. If CTRMA initiates the CO, Vendor will respond to the CO with the impact to the scope, schedule, and cost, also referred to as a CO in this process.

3. The CTRMA approver will approve or reject the requested Change Order within five (5) business days from the receipt of the CO form.
4. If the CTRMA approver does not approve or reject the requested Change Order within five (5) business days from the receipt of the CO form and does not communicate a reasonable timeframe in which a decision will be made, the requested Change Order will be considered deferred:
 - a. The CO status will be logged, tracked, and managed as a ‘deferred’ request.
 - b. Services will progress without incorporating the requested change into the work plan.
 - c. Where an approval or rejection decision is necessary for the Services under this Agreement to progress, Vendor and CTRMA will use the Issues Management process above.
5. For COs outside the stated project scope, CTRMA will authorize budget allowance and payment, on a time and materials basis, for Vendor to perform the initial analysis of a requested change.
6. Vendor shall coordinate any changes in hardware, network, software, configuration, or Services with CTRMA. CTRMA may defer the change based on impact to business operations.
7. Vendor and CTRMA shall work in good faith to resolve disputes regarding the In-Scope or Out-of-Scope classification of work, using the Issues Management process above.

4.2.2. Change Order Approvals

The following persons are responsible for obtaining signature approval of Change Orders for the engagement:

Vendor		CTRMA	
Name	Uday Katira	Greg Mack	
Role	Managing Director	IT Manager	

4.3. Unforeseen Conditions and Events

If unforeseen conditions are discovered or unforeseen events occur that materially affect the original scope of work, Vendor will work with CTRMA to adjust the scope, cost and schedule of this Agreement using the above Change Process or to terminate this Agreement without penalty.

4.4. Delays and Extensions

Vendor has a limited ability to mitigate the impact of delays caused by CTRMA or by events outside Vendor’s control. Vendor’s rates, prices, and schedules do not include a contingency for the cost and schedule impacts of such delays.

Vendor will notify CTRMA promptly upon discovery of any delay caused by CTRMA or caused by events outside CTRMA’s or Vendor’s control and Vendor will work with CTRMA to mitigate the cost and schedule impacts;

however, Vendor will be entitled to adjust the schedule accordingly and shall inform CTRMA of any charges for additional work caused by such delays. Vendor will submit a Change Order for required cost and schedule adjustments. Vendor reserves the right to amend any Change Order to address the cumulative impacts of subsequent delays.

5. Additional Terms and Conditions

CTRMA reserves the rights with respect to this SOW to:

1. Modify, withdraw, or cancel this SOW in whole or in part at any time prior to the execution of the Contract by CTRMA, without incurring any costs obligations or liabilities.
2. Issue a new SOW after withdrawal of this SOW.
3. Accept or reject any and all submittals and responses received at any time.
4. Modify dates set or projected in this SOW.
5. Terminate evaluations of responses received at any time.
6. Require confirmation of information furnished by a Vendor, require additional information from a Vendor concerning its response, and require additional evidence of qualifications to perform the work described in this SOW.
7. Seek or obtain data from any source that has the potential to improve the understanding and evaluation of the responses to this SOW.
8. Waive any weaknesses, informalities, irregularities or omissions in a response, permit corrections, and seek and receive clarifications to a response.
9. Accept other than the lowest priced response.
10. Issue addenda, supplements, and modifications to this SOW.
11. Disqualify any Vendor that changes its response without CTRMA approval.
12. Modify the SOW process (with appropriate notice to Vendors).
13. Establish a competitive range, hold discussions and/or request BAFOs.
14. Approve or disapprove changes to the Vendor teams.
15. Revise and modify, at any time before the submission deadline, the factors it will consider in evaluating Vendors, and to otherwise revise or expand its evaluation methodology. If such revisions or modifications are made, CTRMA shall circulate an addendum to all Vendors setting forth the changes to the evaluation criteria or methodology. CTRMA may extend the submission deadline if such changes are deemed by CTRMA, in its sole discretion, to be material and substantive.
16. Hold meetings, conduct discussions, and communicate with one or more of the Vendors responding to this SOW to seek an improved understanding and evaluation of the response.
17. Add or delete work to/from the scope of services.
18. Negotiate with one or more Vendors concerning its response and/or the Contract.
19. Suspend and/or terminate negotiations at any time, elect not to commence negotiations with any responding Vendor and engage in negotiations with other than the highest ranked Vendor.
20. Retain ownership of all materials submitted in hard-copy and/or electronic format.
21. Exercise any other right reserved or afforded to CTRMA under this SOW.
22. Vendor responses received become the property of CTRMA.

This SOW does not commit CTRMA to enter into a contract or proceed with the procurement described herein. CTRMA assumes no obligations, responsibilities, and liabilities, fiscal or otherwise, to reimburse all or part of the costs incurred or alleged to have been incurred by parties responding to this SOW. All such costs shall be borne solely by the Vendor. In no event shall CTRMA be bound by, or liable for, any obligations with respect to the procurement until such time (if at all) as a Contract, in form and substance satisfactory to CTRMA, has been authorized and executed by CTRMA and then, only to the extent set forth herein. CTRMA makes no representation that the Contract will be awarded based on the requirements of this SOW. Vendors are advised that CTRMA may modify the procurement documents at any time.

6. Compliance with CTRMA Information Security Guidelines

The Vendor shall become familiar with and adhere to CTRMA's Information Security policies, provided that such Information Security Policies (i) do not expand the scope of such services (absent a corresponding change pursuant to the change process herein), (ii) shall not apply to security controls on Vendor's computers, equipment, information systems or networks, (iii) are applicable to Vendor in performance of the services, (iv) do not conflict with or modify the terms of this Contract, or Vendor's own policies, and (v) shall not be deemed to permit CTRMA to conduct and audit, inspection or testing of Vendor's systems, equipment or facilities. Consultants that have access to CTRMA IT environments will be required to sign a user acknowledgement and agree to comply with the CTRMA Information Security Policy (Appendix A).

7. CTRMA Provided Services

If required, CTRMA will provide the following for Vendor staff working onsite:

- Desk and workspace
- Desk phone
- Security access to required physical areas
- Access to subject matter experts available during normal work hours
- Laptop or desktop computers with required network and Internet access
- CTRMA will not provide a cell phone, smart phone, tablet or other personal electronic equipment
- System access will be provided by CTRMA

7.1. Location of Work, Hours and Conditions

Given the dynamic health advisory climate, where possible, project work will be performed at the Vendor's resource center. Depending upon the nature of a particular deliverable, CTRMA may supply access to Vendor resources and temporary on-site workspace and/or access to facilities required for performing assigned tasks. Space will be provided for Vendors with staff working on-site. CTRMA's normal work hours on the Project are a standard 5-day workweek, excluding US National holidays.

Appendix A: CTRMA Information Security Policy

Acceptable Encryption Policy

1. Overview

See Purpose.

2. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

3. Scope

This policy applies to all CTRMA employees and affiliates.

4. Policy

4.1 Algorithm Requirements

- 4.1.1 Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the [IETF/IRTF Cipher Catalog](#), or the set defined for use in the United States [National Institute of Standards and Technology \(NIST\) publication FIPS 140-2](#), or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.
- 4.1.2 Algorithms in use must meet the standards defined for use in NIST publication [FIPS 140-2](#) or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.
- 4.1.3 Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Cisco Legal recommends RFC6090 compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

4.2 Hash Function Requirements

In general, CTRMA adheres to the [NIST Policy on Hash Functions](#).

4.3 Key Agreement and Authentication

- 4.3.1 Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
- 4.3.2 End points must be authenticated prior to the exchange or derivation of session keys.
- 4.3.3 Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
- 4.3.4 All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
- 4.3.5 All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.4 Key Generation

- 4.4.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- 4.4.2 Key generation must be seeded from an industry standard random number generator (RNG). For examples, see [NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2](#).

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

[National Institute of Standards and Technology \(NIST\) publication FIPS 140-2,](#)

[NIST Policy on Hash Functions](#)

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- Proprietary Encryption

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Acceptable Use Policy

6. Overview

Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to CTRMA's established culture of openness, trust and integrity. Infosec is committed to protecting CTRMA's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of CTRMA. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every CTRMA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

7. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at CTRMA. These rules are in place to protect the employee and CTRMA. Inappropriate use exposes CTRMA to risks including virus attacks, compromise of network systems and services, and legal issues.

8. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct CTRMA business or interact with internal networks and business systems, whether owned or leased by CTRMA, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at CTRMA and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CTRMA policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at CTRMA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by CTRMA.

9. Policy

a. General Use and Ownership

- i. CTRMA proprietary information stored on electronic and computing devices whether owned or leased by CTRMA, the employee or a third party, remains the sole property of CTRMA. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard*.
- ii. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of CTRMA proprietary information.
- iii. You may access, use or share CTRMA proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- iv. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- v. For security and network maintenance purposes, authorized individuals within CTRMA may monitor equipment, systems and network traffic at any time, per Infosec's *Audit Policy*.
- vi. CTRMA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

b. Security and Proprietary Information

- i. All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.
- ii. System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- iii. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- iv. Postings by employees from a CTRMA email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CTRMA, unless posting is in the course of business duties.
- v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

c. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of CTRMA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CTRMA-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

i. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CTRMA.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CTRMA or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting CTRMA business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a CTRMA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any CTRMA account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the CTRMA network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, CTRMA employees to parties outside CTRMA.

ii. Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within CTRMA's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CTRMA or connected via CTRMA's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

iii. Blogging and Social Media

1. Blogging by employees, whether using CTRMA's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of CTRMA's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate CTRMA's policy, is not detrimental to CTRMA's best interests, and does not interfere with an employee's regular work duties. Blogging from CTRMA's systems is also subject to monitoring.
2. CTRMA's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of CTRMA and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by CTRMA's *Non-Discrimination and Anti-Harassment* policy.
4. Employees may also not attribute personal statements, opinions or beliefs to CTRMA when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of CTRMA. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, CTRMA's trademarks, logos and any other CTRMA intellectual property may also not be used in connection with any blogging activity

10. Policy Compliance

a. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

b. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

c. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

11. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

12. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

13. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format

Clean Desk Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

14. Overview

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

15. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

16. Scope

This policy applies to all CTRMA employees and affiliates.

17. Policy

- 4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- 4.2 Computer workstations must be locked when workspace is unoccupied.
- 4.3 Computer workstations must be shut completely down at the end of the work day.
- 4.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- 4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- 4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- 4.7 Laptops must be either locked with a locking cable or locked away in a drawer.
- 4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- 4.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- 4.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- 4.11 Whiteboards containing Restricted and/or Sensitive information should be erased.
- 4.12 Lock away portable computing devices such as laptops and tablets.

4.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up. **Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

4.14

18. Policy Compliance

8.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

8.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9 Related Standards, Policies and Processes

None.

10 Definitions and Terms

None.

11 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

<ORGANIZATION NAME> Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how <ORGANIZATION NAME>'s established culture of openness, trust and integrity should respond to such activity.

<ORGANIZATION NAME> Information Security is committed to protecting <ORGANIZATION NAME>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of <ORGANIZATION NAME> Protected data or <ORGANIZATION NAME> Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Helpdesk@<ORGANIZATION NAME>.org, by calling 555-1212, or through the use of the help desk reporting web page at <http://<ORGANIZATION NAME>>. This e-mail address, phone number, and web page are monitored by the <ORGANIZATION NAME>'s Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information

(PHI) of <ORGANIZATION NAME> members. Any agreements with vendors will contain language similar that protects the fund.

3.0 Policy Confirmed theft, data breach or exposure of <ORGANIZATION NAME> Protected data or <ORGANIZATION NAME> Sensitive data

As soon as a theft, data breach or exposure containing <ORGANIZATION NAME> Protected data or <ORGANIZATION NAME> Sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach or exposure of <ORGANIZATION NAME> data

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by <ORGANIZATION NAME> cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan.

Work with <ORGANIZATION NAME> communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

3.2 Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the <ORGANIZATION NAME> community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any <ORGANIZATION NAME> Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of the <ORGANIZATION NAME> community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the <ORGANIZATION NAME> community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

4.0 Enforcement

Any < ORGANIZATION NAME > personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

5.0 Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text – Unencrypted data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

Protected data - See PII and PHI

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

6.0 Revision History

Version	Date of Revision	Author	Description of Changes
1.0	August 17, 2016	SANS Institute	Initial version

1.0			
-----	--	--	--

Digital Signature Acceptance Policy

19. Overview

See Purpose.

20. Purpose

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in CTRMA electronic documents and correspondence, and thus a substitute for traditional “wet” signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

21. Scope

This policy applies to all CTRMA employees and affiliates.

This policy applies to all CTRMA employees, contractors, and other agents conducting CTRMA business with a CTRMA-provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non-CTRMA affiliated persons or organizations.

22. Policy

A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence, with the exception of those noted on the site of the Chief Financial Officer (CFO) on the organization’s intranet: <CFO’s Office URL>

The CFO’s office will maintain an organization-wide list of the types of documents and correspondence that are not covered by this policy.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

4.1 Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

4.2 Signer Responsibilities

4.2.1 Signers must obtain a signing key pair from <Company Name identity management group>. This key pair will be generated using CTRMA’s Public Key Infrastructure

(PKI) and the public key will be signed by the CTRMA's Certificate Authority (CA), <CA Name>.

- 4.2.2 Signers must sign documents and correspondence using software approved by CTRMA IT organization.
- 4.2.3 Signers must protect their private key and keep it secret.
- 4.2.4 If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact CTRMA Identity Management Group immediately to have the signer's digital key pair revoked.

4.3 Recipient Responsibilities

- 4.3.1 Recipients must read documents and correspondence using software approved by CTRMA IT department.
- 4.3.2 Recipients must verify that the signer's public key was signed by the CTRMA's Certificate Authority (CA), <CA Name>, by viewing the details about the signed key using the software they are using to read the document or correspondence.
- 4.3.3 If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.
- 4.3.4 If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to CTRMA Identity Management Group.

23. Policy Compliance

11.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

11.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

11.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12 Related Standards, Policies and Processes

None.

13 References

Note that these references were used only as guidance in the creation of this policy template. We highly recommend that you consult with your organization's legal counsel, since there may be federal, state, or local regulations to which you must comply. Any other PKI-related policies your organization has may also be cited here.

American Bar Association (ABA) Digital Signature Guidelines
<http://www.abanet.org/scitech/ec/isc/dsgfree.html>

Minnesota State Agency Digital Signature Implementation and Use

http://mn.gov/oet/policies-and-standards/business/policy-pages/standard_digital_signature.jsp

Minnesota Electronic Authentication Act

https://www.revisor.leg.state.mn.us/statutes/?id=325K&view=chapter_stat.325K.001

City of Albuquerque E-Mail Encryption / Digital Signature Policy

<http://mesa.cabq.gov/policy.nsf/WebApprovedX/4D4D4667D0A7953A87256E7B004F6720?OpenDocument>

West Virginia Code §39A-3-2: Acceptance of electronic signature by governmental entities in satisfaction of signature requirement. <http://law.justia.com/westvirginia/codes/39a/wvc39a-3-2.html>

14 Definitions and Terms

None.

15 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Disaster Recovery Plan Policy

24.Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives CTRMA a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

25. Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by CTRMA that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

26. Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

27. Policy

4.1 Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed and updated on an annual basis.

28. Policy Compliance

15.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

15.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

15.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

16 Related Standards, Policies and Processes

None.

17 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- Disaster

18 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Email Policy

29. Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

30. Purpose

The purpose of this email policy is to ensure the proper use of CTRMA email system and make users aware of what CTRMA deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within CTRMA Network.

31. Scope

This policy covers appropriate use of any email sent from a CTRMA email address and applies to all employees, vendors, and agents operating on behalf of CTRMA.

32. Policy

- 4.1 All use of email must be consistent with CTRMA policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- 4.2 CTRMA email account should be used primarily for CTRMA business-related purposes; personal communication is permitted on a limited basis, but non-CTRMA related commercial uses are prohibited.
- 4.3 All CTRMA data contained within an email message or an attachment must be secured according to the *Data Protection Standard*.
- 4.4 Email should be retained only if it qualifies as a CTRMA business record. Email is a CTRMA business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- 4.5 Email that is identified as a CTRMA business record shall be retained according to CTRMA Record Retention Schedule.
- 4.6 The CTRMA email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any CTRMA employee should report the matter to their supervisor immediately.
- 4.7 Users are prohibited from automatically forwarding CTRMA email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain CTRMA confidential or above information.
- 4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct CTRMA business, to create or memorialize any binding transactions, or to store or retain email on behalf of CTRMA. Such communications and transactions should be conducted through proper channels using CTRMA-approved documentation.
- 4.9 Using a reasonable amount of CTRMA resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a CTRMA email account is prohibited.
- 4.10 CTRMA employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- 4.11 CTRMA may monitor messages without prior notice. CTRMA is not obliged to monitor email messages.

33. Policy Compliance

18.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

18.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

18.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

19 Related Standards, Policies and Processes

- Data Protection Standard

20 Definitions and Terms

None.

21 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Updated and converted to new format.

End User Encryption Key Protection Policy

34. Overview

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys used to secure sensitive data and hence, compromise of the data. While users may understand it's important to encrypt certain documents and electronic communications, they may not be familiar with minimum standards for protecting encryption keys.

35. Purpose

This policy outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

36. Scope

This policy applies to any encryption keys listed below and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are:

- encryption keys issued by CTRMA
- encryption keys used for CTRMA business

- encryption keys used to protect data owned by CTRMA

The public keys contained in digital certificates are specifically exempted from this policy.

37. Policy

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

4.1 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in CTRMA's *Acceptable Encryption Policy*. If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and the each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

4.2 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

4.2.1 CTRMA's Public Key Infrastructure (PKI) Keys

The public-private key pairs used by the CTRMA's public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the smart card. This prevents the Infosec Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with CTRMA policies.

Access to the private keys stored on a CTRMA issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

4.2.2 Other Public Key Encryption Keys

Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on smartcard, the

requirements for protecting the private keys are the same as those for private keys associated with <Company Name's> PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage.

The Infosec Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with CTRMA *Password Policy*. Infosec representatives will store and protect the escrowed keys as described in the CTRMA *Certificate Practice Statement Policy*.

4.2.2.1 Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

4.2.2.2 PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

4.3 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in CTRMA's *Physical Security policy*, when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

4.4 Personal Identification Numbers (PINs), Passwords and Passphrases

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in CTRMA's *Password Policy*.

4.5 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to The Infosec Team. Infosec personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

38. Policy Compliance

21.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

21.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

21.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

22 Related Standards, Policies and Processes

- Acceptable Encryption Policy
- Certificate Practice Statement Policy
- Password Policy
- Physical Security policy

23 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- Certificate authority (CA)
- Digital certificate
- Digital signature
- Key escrow
- Plaintext
- Public key cryptography

Ethics Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

39. Overview

CTRMA is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When CTRMA addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

CTRMA will not tolerate any wrongdoing or impropriety at any time. CTRMA will take the appropriate measures act quickly in correcting the issue if the ethical code is broken.

40. Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every CTRMA employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

41. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at CTRMA, including all personnel affiliated with third parties.

42. Policy

4.1 Executive Commitment to Ethics

- 4.1.1 Senior leaders and executives within CTRMA must set a prime example. In any business practice, honesty and integrity must be top priority for executives.
- 4.1.2 Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.
- 4.1.3 Executives must disclose any conflict of interests regard their position within CTRMA.

4.2 Employee Commitment to Ethics

- 4.2.1 CTRMA employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
- 4.2.2 Every employee needs to apply effort and intelligence in maintaining ethics value.
- 4.2.3 Employees must disclose any conflict of interests regard their position within CTRMA.
- 4.2.4 Employees will help CTRMA to increase customer and vendor satisfaction by providing quality products and timely response to inquiries.
- 4.2.5 Employees should consider the following questions to themselves when any behavior is questionable:

- Is the behavior legal?
- Does the behavior comply with all appropriate CTRMA policies?
- Does the behavior reflect CTRMA values and culture?
- Could the behavior adversely affect company stakeholders?
- Would you feel personally concerned if the behavior appeared in a news headline?
- Could the behavior adversely affect CTRMA if all employees did it?

4.3 Company Awareness

4.3.1 Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

4.3.2 CTRMA will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4 Maintaining Ethical Practices

4.4.1 CTRMA will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

4.4.2 Employees at CTRMA should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.4.3 CTRMA has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

4.4.4 Employees are required to recertify their compliance to Ethics Policy on an annual basis.

4.5 Unethical Behavior

4.5.1 CTRMA will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

4.5.2 CTRMA will not tolerate harassment or discrimination.

4.5.3 Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

4.5.4 CTRMA will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

4.5.5 CTRMA employees will not use corporate assets or business relationships for personal use or gain.

43. Policy Compliance

23.1 Compliance Measurement

The <Employee Resource Team> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

23.2 Exceptions

None.

23.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

24 Related Standards, Policies and Processes

None.

25 Definitions and Terms

None.

26 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Pandemic Response Planning Policy

44. Overview

This policy is intended for companies that do not meet the definition of critical infrastructure as defined by the federal government. This type of organization may be requested by public health officials to close their offices to non-essential personnel or completely during a worst-case scenario pandemic to limit the spread of the disease. Many companies would run out of cash and be forced to go out of business after several weeks of everyone not working. Therefore, developing a response plan in advance that addresses who can work remotely, how they will work and identifies what other issues may be faced will help the organization survive at a time when most people will be concerned about themselves and their families.

Disasters typically happen in one geographic area. A hurricane or earthquake can cause massive damage in one area, yet the worst damage is usually contained within a few hundred miles. A global pandemic,

such as the 1918 influenza outbreak which infected 1/3 of the world's population, cannot be dealt with by failing over to a backup data center. Therefore, additional planning steps for IT architecture, situational awareness, employee training and other preparations are required.

45. Purpose

This document directs planning, preparation and exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process. The objective is to address the reality that pandemic events can create personnel and technology issues outside the scope of the traditional DR/BCP planning process as potentially 25% or more of the workforce may be unable to come to work for health or personal reasons.

46. Scope

The planning process will include personnel involved in the business continuity and disaster recovery process, enterprise architects and senior management of CTRMA. During the implementation of the plan, all employees and contractors will need to undergo training before and during a pandemic disease outbreak.

47. Policy

CTRMA will authorize, develop and maintain a Pandemic Response Plan addressing the following areas:

- 4.1 The Pandemic Response Plan leadership will be identified as a small team which will oversee the creation and updates of the plan. The leadership will also be responsible for developing internal expertise on the transmission of diseases and other areas such as second wave phenomenon to guide planning and response efforts. However, as with any other critical position, the leadership must have trained alternates that can execute the plan should the leadership become unavailable due to illness.
- 4.2 The creation of a communications plan before and during an outbreak that accounts for congested telecommunications services.
- 4.3 An alert system based on monitoring of World Health Organization (WHO) and other local sources of information on the risk of a pandemic disease outbreak.
- 4.4 A predefined set of emergency policies that will preempt normal CTRMA policies for the duration of a declared pandemic. These policies are to be organized into different levels of response that match the level of business disruption expected from a possible pandemic disease outbreak within the community. These policies should address all tasks critical to the continuation of the company including:
 - a) How people will be paid
 - b) Where they will work – including staying home with or bringing kids to work.
 - c) How they will accomplish their tasks if they cannot get to the office
- 4.5 A set of indicators to management that will aid them in selecting an appropriate level of response bringing into effect the related policies discussed in section 4.4—for the organization. There should be a graduated level of response related to the WHO pandemic alert level or other local indicators of a disease outbreak.
- 4.6 An employee training process covering personal protection including:
 - a) Identifying symptoms of exposure
 - b) The concept of disease clusters in day cares, schools or other gathering places

- c) Basic prevention - limiting contact closer than 6 feet, cover your cough, hand washing
 - d) When to stay home
 - e) Avoiding travel to areas with high infection rates
- 4.7 A process for the identification of employees with first responders or medical personnel in their household. These people, along with single parents, have a higher likelihood of unavailability due to illness or child care issues.
- 4.8 A process to identify key personnel for each critical business function and transition their duties to others in the event they become ill.
- 4.9 A list of supplies to be kept on hand or pre-contracted for supply, such as face masks, hand sanitizer, fuel, food and water.
- 4.10 IT related issues:
- a) Ensure enterprise architects are including pandemic contingency in planning
 - b) Verification of the ability for significantly increased telecommuting including bandwidth, VPN concentrator capacity/licensing, ability to offer voice over IP and laptop/remote desktop availability
 - c) Increased use of virtual meeting tools – video conference and desktop sharing
 - d) Identify what tasks cannot be done remotely
 - e) Plan for how customers will interact with the organization in different ways
- 4.11 The creation of exercises to test the plan.
- 4.12 The process and frequency of plan updates at least annually.
- 4.13 Guidance for auditors indicating that any review of the business continuity plan or enterprise architecture should assess whether they appropriately address the CTRMA Pandemic Response Plan.

48. Policy Compliance

26.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

26.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

26.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

27 Related Standards, Policies and Processes

[World Health Organization](#)

28 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

<https://www.sans.org/security-resources/glossary-of-terms/>

- Pandemic

29 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Password Protection Policy

49. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of CTRMA's resources. All users, including contractors and vendors with access to CTRMA systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

50. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

51. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CTRMA facility, has access to the CTRMA network, or stores any non-public CTRMA information.

52. Policy

4.1 Password Creation

- 4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
- 4.1.2 Users must not use the same password for CTRMA accounts as for other non-CTRMA access (for example, personal ISP account, option trading, benefits, and so on).
- 4.1.3 Where possible, users must not use the same password for various CTRMA access needs.
- 4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
- 4.1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings

must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

4.2 Password Change

- 4.2.1 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
- 4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
- 4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

- 4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential CTRMA information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
- 4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
- 4.3.3 Passwords must not be revealed over the phone to anyone.
- 4.3.4 Do not reveal a password on questionnaires or security forms.
- 4.3.5 Do not hint at the format of a password (for example, "my family name").
- 4.3.6 Do not share CTRMA passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- 4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- 4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).
- 4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

- 4.4.1 Applications must support authentication of individual users, not groups.

- 4.4.2 Applications must not store passwords in clear text or in any easily reversible form.
- 4.4.3 Applications must not transmit passwords in clear text over the network.
- 4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

53. Policy Compliance

29.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

29.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

29.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

30 Related Standards, Policies and Processes

- Password Construction Guidelines

31 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- Simple Network Management Protocol (SNMP)

32 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Security Response Plan Policy

54. Overview

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

55. Purpose

The purpose of this policy is to establish the requirement that all business units supported by the Infosec team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

56. Scope

This policy applies any established and defined business unity or entity within the CTRMA.

4 Policy

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation with the Infosec Team. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the <organizational information security unit> in the development and maintenance of a Security Response Plan.

4.1 Service or Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

4.2 Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

4.3 Triage

The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4.4 Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

4.5 Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

5 Policy Compliance

5.1 Compliance Measurement

Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2 Exceptions

Any exception to this policy must be approved by the Infosec Team in advance and have a written record.

5.3 Non-Compliance

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Public key pairs

- Symmetric cryptography

33 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Acquisition Assessment Policy

1. Overview

The process of integrating a newly acquired company can have a drastic impact on the security posture of either the parent company or the child company. The network and security infrastructure of both entities may vary greatly and the workforce of the new company may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

- Assess company's security landscape, posture, and policies
- Protect both CTRMA and the acquired company from increased security risks
- Educate acquired company about CTRMA policies and standard
- Adopt and implement CTRMA Security Policies and Standards
- Integrate acquired company
- Continuous monitoring and auditing of the acquisition

2. Purpose

The purpose of this policy is to establish Infosec responsibilities regarding corporate acquisitions, and define the minimum security requirements of an Infosec acquisition assessment.

3. Scope

This policy applies to all companies acquired by CTRMA and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired company.

4. Policy

4.1 General

Acquisition assessments are conducted to ensure that a company being acquired by CTRMA does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. The Infosec Team will provide personnel to serve as active members of the acquisition team throughout the entire acquisition process. The Infosec role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to CTRMA's networks. Below are the minimum requirements that the acquired company must meet before being connected to the CTRMA network.

4.2 Requirements

4.2.1 Hosts

- 4.2.1.1 All hosts (servers, desktops, laptops) will be replaced or re-imaged with a CTRMA standard image or will be required to adopt the minimum standards for end user devices.

- 4.2.1.2 Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by Infosec.
- 4.2.1.3 All PC based hosts will require CTRMA approved virus protection before the network connection.
- 4.2.2 Networks
 - 4.2.2.1 All network devices will be replaced or re-imaged with a CTRMA standard image.
 - 4.2.2.2 Wireless network access points will be configured to the CTRMA standard.
- 4.2.3 Internet
 - 4.2.3.1 All Internet connections will be terminated.
 - 4.2.3.2 When justified by business requirements, air-gapped Internet connections require Infosec review and approval.
- 4.2.4 Remote Access
 - 4.2.4.1 All remote access connections will be terminated.
 - 4.2.4.2 Remote access to the production network will be provided by CTRMA.
- 4.2.5 Labs
 - 4.2.5.1 Lab equipment must be physically separated and secured from non-lab areas.
 - 4.2.5.2 The lab network must be separated from the corporate production network with a firewall between the two networks.
 - 4.2.5.3 Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Lab Security Group (LabSec).
 - 4.2.5.4 All acquired labs must meet with LabSec lab policy, or be granted a waiver by LabSec.
 - 4.2.5.5 In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the CTRMA Chief Information Officer (CIO) must acknowledge and approve of the risk to CTRMA's networks

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- Business Critical Production Server

8 Revision History

Date of Change	Responsible	Summary of Change

Bluetooth Baseline Requirements Policy

6. Overview

Bluetooth enabled devices are exploding on the Internet at an astonishing rate. At the range of connectivity has increased substantially. Insecure Bluetooth connections can introduce a number of potential serious security issues. Hence, there is a need for a minimum standard for connecting Bluetooth enable devices.

7. Purpose

The purpose of this policy is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the CTRMA network or CTRMA owned devices. The intent of the minimum standard is to ensure sufficient protection Personally Identifiable Information (PII) and confidential CTRMA data.

8. Scope

This policy applies to any Bluetooth enabled device that is connected to CTRMA network or owned devices.

9. Policy

4.1 Version

No Bluetooth Device shall be deployed on CTRMA equipment that does not meet a minimum of Bluetooth v2.1 specifications without written authorization from the Infosec Team. Any Bluetooth

equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

4.2 Pins and Pairing

When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where your PIN can be compromised.

If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, you must refuse the pairing request and report it to Infosec, through your Help Desk, immediately.

4.3 Device Security Settings

- All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
- Use a minimum PIN length of 8. A longer PIN provides more security.
- Switch the Bluetooth device to use the hidden mode (non-discoverable)
- Only activate Bluetooth only when it is needed.
- Ensure device firmware is up-to-date.

4.4 Security Audits

The Infosec Team may perform random audits to ensure compliancy with this policy. In the process of performing such audits, Infosec Team members shall not eavesdrop on any phone conversation.

4.5 Unauthorized Use

The following is a list of unauthorized uses of CTRMA-owned Bluetooth devices:

- Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
- Using CTRMA-owned Bluetooth equipment on non-CTRMA-owned Bluetooth enabled devices.
- Unauthorized modification of Bluetooth devices for any purpose.

4.6 User Responsibilities

- It is the Bluetooth user's responsibility to comply with this policy.
- Bluetooth mode must be turned off when not in use.
- PII and/or CTRMA Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.
- Bluetooth users must only access CTRMA information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to Infosec.

10. Policy Compliance

8.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

8.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9 Related Standards, Policies and Processes

None.

10 Definitions and Terms

None.

11 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Remote Access Policy

11. Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, we must mitigate these external risks the best of our ability.

12. Purpose

The purpose of this policy is to define rules and requirements for connecting to CTRMA's network from any host. These rules and requirements are designed to minimize the potential exposure to CTRMA from damages which may result from unauthorized use of CTRMA resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical CTRMA internal systems, and fines or other financial liabilities incurred as a result of those losses.

13. Scope

This policy applies to all CTRMA employees, contractors, vendors and agents with a CTRMA-owned or personally-owned computer or workstation used to connect to the CTRMA network. This policy applies to remote access connections used to do work on behalf of CTRMA, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to CTRMA networks.

14. Policy

It is the responsibility of CTRMA employees, contractors, vendors and agents with remote access privileges to CTRMA's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to CTRMA.

General access to the Internet for recreational use through the CTRMA network is strictly limited to CTRMA employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the CTRMA network from a personal computer, Authorized Users are responsible for preventing access to any CTRMA computer resources or data by non-Authorized Users. Performance of illegal activities through the CTRMA network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use CTRMA networks to access the Internet for outside business interests.

For additional information regarding CTRMA's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (company url).

4.1 Requirements

- 4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.
- 4.1.2 Authorized Users shall protect their login and password, even from family members.
- 4.1.3 While using a CTRMA-owned computer to remotely connect to CTRMA's corporate network, Authorized Users shall ensure the remote host is not connected to any other

network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

- 4.1.4 Use of external resources to conduct CTRMA business must be approved in advance by InfoSec and the appropriate business unit manager.
- 4.1.5 All hosts that are connected to CTRMA internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
- 4.1.6 Personal equipment used to connect to CTRMA's networks must meet the requirements of CTRMA-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to CTRMA Networks*.

15. Policy Compliance

11.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

11.2 Exceptions

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

11.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12 Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of CTRMA's network:

- *Acceptable Encryption Policy*
- *Acceptable Use Policy*
- *Password Policy*
- *Third Party Agreement*
- *Hardware and Software Configuration Standards for Remote Access to CTRMA Networks*

13 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.
April 2015	Christopher Jarko	Added an Overview; created a group term for company employees, contractors, etc. (“Authorized Users”); strengthened the policy by explicitly limiting use of company resources to Authorized Users only; combined Requirements when possible, or eliminated Requirements better suited for a Standard (and added a reference to that Standard); consolidated list of related references to end of Policy.

Remote Access Tools Policy

16. Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the CTRMA network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on CTRMA computer systems.

17. Purpose

This policy defines the requirements for remote access tools used at <Company Name

18. Scope

This policy applies to all remote access where either end of the communication terminates at a CTRMA computer asset

19. Policy

All remote access tools used to communicate between CTRMA assets and other systems must comply with the following policy requirements.

4.1 Remote Access Tools

CTRMA provides mechanisms to collaborate between internal users, with external partners, and from non-CTRMA systems. The approved software list can be obtained from <link-to-

approved-remote-access-software-list>. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

- a) All remote access tools or systems that allow communication to CTRMA resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
- b) The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
- c) Remote access tools must support the CTRMA application layer proxy rather than direct connections through the perimeter firewall(s).
- d) Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the CTRMA network encryption protocols policy.
- e) All CTRMA antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard CTRMA procurement process, and the information technology group must approve the purchase.

20. Policy Compliance

13.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

13.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

13.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

14 Related Standards, Policies and Processes

None.

15 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- Application layer proxy

16 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Router and Switch Security Policy

21. Overview

See Purpose.

22. Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of CTRMA.

23. Scope

All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. All routers and switches connected to Cisco production networks are affected.

24. Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled:
 - a. IP directed broadcasts
 - b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
 - c. TCP small services
 - d. UDP small services
 - e. All source routing and switching
 - f. All web services running on router

- g. Cisco discovery protocol on Internet connected interfaces
 - h. Telnet, FTP, and HTTP services
 - i. Auto-configuration
- 4. The following services should be disabled unless a business justification is provided:
 - a. Cisco discovery protocol and other discovery protocols
 - b. Dynamic trunking
 - c. Scripting environments, such as the TCL shell
- 5. The following services must be configured:
 - a. Password-encryption
 - b. NTP configured to a corporate standard source
- 6. All routing updates shall be done using secure routing updates.
- 7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
- 8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- 9. Access control lists for transiting the device are to be added as business needs arise.
- 10. The router must be included in the corporate enterprise management system with a designated point of contact.
- 11. Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

- 12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
- 13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
- 14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
 - a. IP access list accounting
 - b. Device logging
 - c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped

- d. Router console and modem access must be restricted by additional security controls

25. Policy Compliance

16.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

16.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

16.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

17 Related Standards, Policies and Processes

None.

18 Definitions and Terms

None.

19 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Wireless Communication Policy

26. Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

27. Purpose

The purpose of this policy is to secure and protect the information assets owned by CTRMA. CTRMA provides computer devices, networks, and other electronic information systems to meet

missions, goals, and initiatives. CTRMA grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to CTRMA network. Only **those** wireless infrastructure devices that meet the standards **specified** in this policy or are granted an exception by the Information Security Department are approved for connectivity to a CTRMA network.

28.Scope

All employees, contractors, consultants, temporary and other workers at CTRMA, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of CTRMA must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a CTRMA network or reside on a CTRMA site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

29.Policy

4.1 General Requirements

All wireless infrastructure devices that reside at a CTRMA site and connect to a CTRMA network, or provide access to information classified as CTRMA Confidential, or above must:

- Abide by the standards specified in the *Wireless Communication Standard*.
- Be installed, supported, and maintained by an approved support team.
- Use CTRMA approved authentication protocols and infrastructure.
- Use CTRMA approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to CTRMA Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the CTRMA network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the *Lab Security Policy*.
- Not interfere with wireless access deployments maintained by other support organizations.

4.3 Home Wireless Device Requirements

- 4.3.1 Wireless infrastructure devices that provide direct access to the CTRMA corporate network, must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.
- 4.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the CTRMA corporate network. Access to the CTRMA corporate network through this device must use standard remote access authentication.

30. Policy Compliance

19.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

19.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

19.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

20 Related Standards, Policies and Processes

- Lab Security Policy
- Wireless Communication Standard

21 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- MAC Address

22 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Wireless Communication Standard

31. Overview

See Purpose.

32. Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a CTRMA network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Team are approved for connectivity to a CTRMA network.

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Security (Infosec) approved support organization. Lab network devices must comply with the *Lab Security Policy*.

33. Scope

All employees, contractors, consultants, temporary and other workers at CTRMA and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of CTRMA, must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

Infosec must approve exceptions to this standard in advance.

34. Standard

4.1 General Requirements

All wireless infrastructure devices that connect to a CTRMA network or provide access to CTRMA Confidential, CTRMA Highly Confidential, or CTRMA Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

4.2 Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from CTRMA production device SSID.
- Broadcast of lab device SSID must be disabled.

4.3 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a CTRMA network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

35. Policy Compliance

22.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

22.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

22.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

23 Related Standards, Policies and Processes

- Lab Security Policy

24 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

<https://www.sans.org/security-resources/glossary-of-terms/>

- AES
- EAP-FAST
- EAP-TLS
- PEAP

- SSID
- TKIP
- WPA-PSK

25 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Database Credentials Coding Policy

1. Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

2. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of CTRMA's networks.

Software applications running on CTRMA's networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

3. Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the CTRMA Network. This policy applies to all software (programs, modules, libraries or APIS that will access a CTRMA, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don't always use sanitized information.

4. Policy

General

In order to maintain the security of CTRMA's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

Specific Requirements

Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
- Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication

may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.

- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPSS authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Coding Techniques for implementing this policy

[Add references to your site-specific guidelines for the different coding languages such as Perl, JAVA, C and/or Cpro.]

5. Policy Compliance

5.1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.2. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with CTRMA.

Any program code or application that is found to violate this policy must be remediated within a 90 day period.

6. Related Standards, Policies and Processes

- Password Policy

7. Definitions and Terms

- Credentials
- Executing Body
- Hash Function
- LDAP
- Module

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Formatted into new template and made minor wording changes.

Information Logging Standard

9. Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

10. Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

11. Scope

This policy applies to all production systems on CTRMA Network.

12. Standard

4.1 General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity, including where or on what system the activity was performed from (subject)?
3. What the activity was performed on (object)?
4. When was the activity performed?
5. What tool(s) was the activity was performed with?
6. What was the status (such as success vs. failure), outcome, or result of the activity?
- 7.

4.2 Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
2. Create, update, or delete information not covered in #1;
3. Initiate a network connection;
4. Accept a network connection;
5. User authentication and authorization for activities covered in #1 or #2 such as user login and logout;

6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
7. System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
8. Application process startup, shutdown, or restart;
9. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
10. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3 Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection.
2. Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
3. Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
5. Before and after values when action involves updating a data element, if feasible.
6. Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
7. Whether the action was allowed or denied by access-control mechanisms.
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4 Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

1. Microsoft Windows Event Logs collected by a centralized log management system;

2. Logs in a well-documented format sent via *syslog*, *syslog-ng*, or *syslog-reliable* network protocols to a centralized log management system;
3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and
4. Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

13. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Lab Security Policy

14. Overview

See Purpose.

15.Purpose

This policy establishes the information security requirements to help manage and safeguard lab resources and CTRMA networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

16.Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at CTRMA and its subsidiaries must adhere to this policy. This policy applies to CTRMA owned and managed labs, including labs outside the corporate firewall (DMZ).

17.Policy

4.1 General Requirements

- 4.1.1 Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.
- 4.1.2 Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard CTRMA from security vulnerabilities.
- 4.1.3 Lab managers are responsible for the lab's compliance with all CTRMA security policies.
- 4.1.4 The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.
- 4.1.5 All user passwords must comply with CTRMA's *Password Policy*.
- 4.1.6 Individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months).
- 4.1.7 PC-based lab computers must have CTRMA's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.
- 4.1.8 Any activities with the intention to create and/or distribute malicious programs into CTRMA's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

- 4.1.9 No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.
- 4.1.10 In accordance with *the Data Classification Policy*, information that is marked as CTRMA Highly Confidential or CTRMA Restricted is prohibited on lab equipment.
- 4.1.11 Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*.
- 4.1.12 InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

4.2 Internal Lab Security Requirements

- 4.2.1 The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.
- 4.2.2 The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.
- 4.2.3 The Network Support Organization must record all lab IP addresses, which are routed within CTRMA networks, in Enterprise Address Management database along with current contact information for that lab.
- 4.2.4 Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.
- 4.2.5 All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.
- 4.2.6 Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.
- 4.2.7 Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-CTRMA networks. These activities must be restricted within the lab.
- 4.2.8 Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.
- 4.2.9 InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.
- 4.2.10 Lab owned gateway devices are required to comply with all CTRMA product security advisories and must authenticate against the Corporate Authentication servers.
- 4.2.11 The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with CTRMA's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

- 4.2.12 In labs where non-CTRMA personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no CTRMA confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.
- 4.2.13 Lab networks with external connections are prohibited from connecting to the corporate production network or other internal networks through a direct connection, wireless connection, or other computing equipment.

4.3 DMZ Lab Security Requirements

- 4.3.1 New DMZ labs require a business justification and VP-level approval from the business unit. Changes to the connectivity or purpose of an existing DMZ lab must be reviewed and approved by the InfoSec Team.
- 4.3.2 DMZ labs must be in a physically separate room, cage, or secured lockable rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.
- 4.3.3 DMZ lab POCs must maintain network devices deployed in the DMZ lab up to the network support organization point of demarcation.
- 4.3.4 DMZ labs must not connect to corporate internal networks, either directly, logically (for example, IPSEC tunnel), through a wireless connection, or multi-homed machine.
- 4.3.5 An approved network support organization must maintain a firewall device between the DMZ lab and the Internet. Firewall devices must be configured based on least privilege access principles and the DMZ lab business requirements. Original firewall configurations and subsequent changes must be reviewed and approved by the InfoSec Team. All traffic between the DMZ lab and the Internet must go through the approved firewall. Cross-connections that bypass the firewall device are strictly prohibited.
- 4.3.6 All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
- 4.3.7 Operating systems of all hosts internal to the DMZ lab running Internet Services must be configured to the secure host installation and configuration standards published the InfoSec Team.
- 4.3.8 Remote administration must be performed over secure channels (for example, encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.
- 4.3.9 DMZ lab devices must not be an open proxy to the Internet.
- 4.3.10 The Network Support Organization and InfoSec reserve the right to interrupt lab connections if a security concern exists.

18. Policy Compliance

8.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

8.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9 Related Standards, Policies and Processes

- Audit Policy
- Acceptable Use Policy
- Data Classification Policy
- Password Policy

10 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

- DMZ
- Firewall

11 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated, made general lab and included DMZ lab requirements, and converted to new format.

Server Security Policy

19. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

20. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by CTRMA. Effective implementation of this policy will minimize unauthorized access to CTRMA proprietary information and technology.

21. Scope

All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Cisco or registered under a Cisco-owned internal network domain.

This policy specifies requirements for equipment on the internal Cisco network. For secure configuration of equipment external to Cisco on the DMZ, see the Internet *DMZ Equipment Policy*.

22. Policy

4.1 General Requirements

4.1.1 All internal servers deployed at CTRMA must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
 - Server contact(s) and location, and a backup contact
 - Hardware and Operating System/Version
 - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures

4.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Policy*.

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved InfoSec guidelines.

4.2.2 Services and applications that will not be used must be disabled where practical.

- 4.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- 4.2.4 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- 4.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- 4.2.6 Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
- 4.2.7 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- 4.2.8 Servers should be physically located in an access-controlled environment.
- 4.2.9 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

- 4.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
 - All security related logs will be kept online for a minimum of 1 week.
 - Daily incremental tape backups will be retained for at least 1 month.
 - Weekly full tape backups of logs will be retained for at least 1 month.
 - Monthly full backups will be retained for a minimum of 2 years.
- 4.3.2 Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
 - Port-scan attacks
 - Evidence of unauthorized access to privileged accounts
 - Anomalous occurrences that are not related to specific applications on the host.

23. Policy Compliance

11.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

11.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

11.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12 Related Standards, Policies and Processes

- Audit Policy

- DMZ Equipment Policy

13 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: <https://www.sans.org/security-resources/glossary-of-terms/>

- De-militarized zone (DMZ)

14 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Software Installation Policy

24. Overview

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization’s network are examples of the problems that can be introduced when employees install software on company equipment.

25. Purpose

The purpose of this policy is to outline the requirements around installation software on <Company Owned> computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within <Company Name’s> computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

26. Scope

This policy applies to all CTRMA employees, contractors, vendors and agents with a CTRMA-owned mobile devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within CTRMA.

27. Policy

- Employees may not install software on <Company Name's> computing devices operated within the CTRMA network.
- Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email.
- Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.
- The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

28. Policy Compliance

14.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

14.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

14.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

15 Related Standards, Policies and Processes

None.

16 Definitions and Terms

None.

17 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Technology Equipment Disposal Policy

29. Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of CTRMA data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

30. Purpose

The purpose of this policy is to define the guidelines for the disposal of technology equipment and components owned by CTRMA.

31. Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within CTRMA including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All CTRMA employees and affiliates must comply with this policy.

32. Policy

4.1 Technology Equipment Disposal

- 4.1.1 When Technology assets have reached the end of their useful life they should be sent to the <Equipment Disposal Team> office for proper disposal.
- 4.1.2 The <Equipment Disposal Team> will securely erase all storage mediums in accordance with current industry best practices.
- 4.1.3 All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.
- 4.1.4 No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).
- 4.1.5 No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around CTRMA. These can be used to dispose of equipment. The <Equipment Disposal Team> will properly remove all data prior to final disposal.
- 4.1.6 All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

- 4.1.7 Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
 - 4.1.8 The <Equipment Disposal Team> will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
 - 4.1.9 Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.
- 4.2 Employee Purchase of Disposed Equipment
- 4.2.1 Equipment which is working, but reached the end of its useful life to CTRMA, will be made available for purchase by employees.
 - 4.2.2 A lottery system will be used to determine who has the opportunity to purchase available equipment.
 - 4.2.3 All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or “reserve” a system. This ensures that all employees have an equal chance of obtaining equipment.
 - 4.2.4 Finance and Information Technology will determine an appropriate cost for each item.
 - 4.2.5 All purchases are final. No warranty or support will be provided with any equipment sold.
 - 4.2.6 Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information
 - 4.2.7 Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.
 - 4.2.8 Prior to leaving CTRMA premises, all equipment must be removed from the Information Technology inventory system.

33. Policy Compliance

17.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

17.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

17.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

18 Related Standards, Policies and Processes

None.

19 Definitions and Terms

None.

20 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Workstation Security (For HIPAA) Policy

34. Overview

See Purpose.

35. Purpose

The purpose of this policy is to provide guidance for workstation security for CTRMA workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule “Workstation Security” Standard 164.310(c) are met.

36. Scope

This policy applies to all CTRMA employees, contractors, workforce members, vendors and agents with a CTRMA-owned or personal-workstation connected to the CTRMA network.

37. Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

3.1 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

3.2 CTRMA will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

3.3 Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with *CTRMA Password Policy*.
- Complying with all applicable password policies and procedures. See *CTRMA Password Policy*.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including protected health information (PHI) on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the *Portable Workstation Encryption Policy*
- Complying with the *Baseline Workstation Configuration Standard*
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the *Wireless Communication policy*

38. Policy Compliance

20.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

20.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

20.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

21 Related Standards, Policies and Processes

- Password Policy
- Portable Workstation Encryption Policy
- Wireless Communication policy
- Workstation Configuration Standard

HIPPA 164.210

<http://www.hipaasurvivalguide.com/hipaa-regulations/164-310.php>

About HIPPA

<http://abouthipaa.com/about-hipaa/hipaa-hitech-resources/hipaa-security-final-rule/164-308a1i-administrative-safeguards-standard-security-management-process-5-3-2-2/>

22 Definitions and Terms

None.

23 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Web Application Security Policy

1. Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

2. Purpose

The purpose of this policy is to define web application security assessments within **CTRMA**. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of **CTRMA** services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at **CTRMA**.

All web application security assessments will be performed by delegated security personnel either employed or contracted by **CTRMA**. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of **CTRMA** is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. Policy

4.1 Web applications are subject to security assessments based on the following criteria:

- a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- b) Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
- c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

- d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

- a) High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
- b) Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- c) Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

- a) Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
- b) Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
- c) Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4 The current approved web application security assessment tools in use which will be used for testing are:

- <Tool/Application 1>
- <Tool/Application 2>

- ...

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

6 Related Standards, Policies and Processes

[OWASP Top Ten Project](#)

[OWASP Testing Guide](#)

[OWASP Risk Rating Methodology](#)

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #12

Quarterly Project Updates

Strategic Plan Relevance: Stewardship, Service & Safety
Department: Engineering
Contact: Mike Sexton, Acting Director of Engineering
Associated Costs: N/A
Funding Source: N/A
Action Requested: Briefing and Board Discussion Only

Project Description/Background:

Projects under construction:

- A. 183A Phase III Project
- B. 183 North Mobility Project
- C. Barton Skyway Ramp Relief Project

Backup provided: None



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #13

Executive Director Board Report

Strategic Plan Relevance: Stewardship, Collaboration, Innovation, Service & Safety

Department: Executive

Contact: James M. Bass, Executive Director

Associated Costs: N/A

Funding Source: N/A

Action Requested: Briefing and Board Discussion Only

Project Description/Background:

Executive Director Report.

- A. IBTTA Annual Meeting.
- B. Agency performance metrics.
 - i. Roadway Performance
 - ii. Call-Center Performance

Backup provided: None



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #14

Executive Session

Executive Session:

Discuss the exchange or sale of one or more parcels or interests in real property owned by the Mobility Authority and related legal issues as authorized by §551.071 (Consultation with Attorney) and §551.072 (Deliberation Regarding Real Property; Closed Meeting).



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #15

Executive Session

Executive Session:

Discuss legal issues related to claims by or against the Mobility Authority; pending or contemplated litigation and any related settlement offers; or other matters as authorized by §551.071 (Consultation with Attorney).



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #16

Executive Session

Executive Session:

Discuss legal issues relating to procurement and financing of Mobility Authority transportation projects and toll system improvements, as authorized by §551.071 (Consultation with Attorney).



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #17

Executive Session

Executive Session:

Discuss personnel matters as authorized by §551.074 (Personnel Matters).



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #18

Adjourn Meeting

Adjourn Board Meeting.