



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

Regular Meeting of the Board of Directors

9:00 a.m.

Wednesday, September 25, 2024

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.

Consent Agenda

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

2. Approve the minutes from the August 28, 2024 Regular Board Meeting.
3. 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.

4. Accept the unaudited financial statements for August 2024.
5. Discuss and consider approving an amendment to the FY 2025 Capital Budget to fund the replacement of the 45SW toll system.
6. Discuss and consider approving an amendment to the FY 2025 Capital Budget to fund the replacement of automatic license plate readers to support the Habitual Violator Program.
7. Discuss and consider approving an amendment to the FY 2025 Capital Budget to fund the replacement of delineators on the MoPac Express Lane.
8. Discuss and consider approving an amendment to the FY 2025 Operating Budget to fund TollTag™ marketing efforts in the Central Texas region to improve pre-paid account penetration.
9. Discuss and consider authorizing the Executive Director to approve work authorizations for the interlocal agreement with the North Texas Tollway Authority to support TollTag™ marketing, promotional services, and account enrollment.
10. Discuss and consider approving an agreement with Deloitte Consulting LLP for enhancements to the Mobility Authority's Data Platform System.
11. Discuss and consider approving an agreement with Sistema Technologies, Inc. for enhancements to the Mobility Authority's Data Platform System for administration of users and roles.
12. Discuss and consider approving a shortlist of proposers to receive the Request for Proposals for Video Toll Billing, Payment Processing, Collections, Enforcement Support, and Customer Services.
13. Discuss and consider approving an amendment to the contract with H2O Partners, Inc. to add services for asset data collection on the 183A Phase III Project and data extraction for curb and gutter on all Mobility Authority corridors.
14. Discuss and consider approving a project development agreement with the Texas Department of Transportation for the US 183 General Purpose Lane Project.

Briefings and Reports

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

15. Project updates.
 - A. 183A Phase III.
 - B. 183 North.

16. Executive Director Report.
 - A. Recent agency staff activities.
 - B. Agency roadway performance metrics.

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:

17. Discuss acquisition of one or more parcels or interests in real property needed for a Mobility Authority headquarters, including facilities for traffic and incident management and other agency functions, pursuant to §551.071 (Consultation with Attorney) and §551.072 (Deliberation Regarding Real Property; Closed Meeting).

18. 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).

19. 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).

20. Discuss personnel matters as authorized by §551.074 (Personnel Matters).

Reconvene in Open Session.

Regular Items

Items to discuss, consider, and take appropriate action.

21. 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.

*Mobility Authority Board Meeting Agenda
Wednesday, September 25, 2024*

(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.

(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

September 25, 2024
AGENDA ITEM #1

Welcome and opportunity for public
comment

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



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024
AGENDA ITEM #2

Approve the minutes from the
August 28, 2024 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 August 28, 2024, Regular Board Meeting.

Backup provided: Draft minutes August 28, 2024, Regular Board Meeting.

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

Wednesday, August 28, 2024
9:00 a.m.

This was an in-person meeting. Notice of the meeting was posted August 23, 2024, 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, Vice Chair Nikelle Meade, Board Members David Armbrust, Mike Doss, Heather Gaddes, David Singleton, and Ben Thompson were present.

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

<https://mobilityauthority.new.swagit.com/videos/313670>

After noting that a quorum of the Board was present, Chairman Jenkins called the meeting to order at 9:05 a.m. and had each Board Member state their name for the record.

1. Welcome and opportunity for public comment.

The following persons addressed the board; Dick Kellerman, Austin Sierra Club; Miriam Schoenfield; Bill Bunch, SOS; Bobby Levinski, SOS; Roger Baker, Ashby Johnson, Capital Area Metropolitan Planning Organization; and Scott Moore, Manor City Manager

Following public comment, Chairman Jenkins took up item 17E.

17. Executive Director Report.
 - E. 290E Toll Phase IV.

Consent Agenda

2. Approve the minutes from the June 26, 2024 Regular Board Meeting.
3. Prohibit the operation of certain vehicles on Mobility Authority toll facilities pursuant to the Habitual Violator Program.

ADOPTED AS: RESOLUTION NO. 24-038

4. Approve an interlocal agreement with the Texas Department of Transportation to co-locate personnel at TxTag customer service centers.

ADOPTED AS: RESOLUTION NO. 24-039

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

ADOPTED AS: RESOLUTION NO. 24-040

6. Approve a contract with Nortex Concrete Lift and Stabilization Inc. for concrete slab lifting and stabilization on 290 Toll and 183A Toll.

ADOPTED AS: RESOLUTION NO. 24-041

7. Approve the maximum speed limit on SH 71 Toll and corresponding amendments to Mobility Authority Policy Code §301.015.

ADOPTED AS: RESOLUTION NO. 24-042

MOTION: Approve Item Nos. 2 thru 7.

RESULT: Approved (Unanimous); 7-0

MOTION: David Singleton

SECONDED BY: Nikelle Meade

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

NAY: None.

Regular Items

8. Accept the unaudited financial statements for June and July 2024.

Presentation by Jose Hernandez, Chief Financial Officer.

ADOPTED AS: RESOLUTION NO. 24-043

MOTION: Accept the unaudited financial statements for June and July 2024.

RESULT: Approved (Unanimous); 7-0

MOTION: Heather Gaddes

SECONDED BY: Mike Doss

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

NAY: None.

9. Discuss and consider approving a contract with CDM Smith Inc. for traffic and revenue engineering services.

ADOPTED AS: RESOLUTION NO. 24-044

10. Discuss and consider approving a contract with C&M Associates, Inc. for traffic and revenue engineering services.

ADOPTED AS: RESOLUTION NO. 24-045

11. Discuss and consider approving a contract with Stantec Consulting Services, Inc. for traffic and revenue engineering services.

Presentation by Jose Hernandez, Chief Financial Officer.

ADOPTED AS: RESOLUTION NO. 24-046

MOTION: Approve contracts with CDM Smith Inc., C&M Associates, Inc., and Stantec Consulting Services, Inc. for traffic and revenue engineering services.

RESULT: Approved (Unanimous); 7-0

MOTION: David Armbrust

SECONDED BY: Ben Thompson

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

NAY: None.

12. Discuss and consider approving an interlocal agreement with the Texas Municipal League for cyber liability and data breach response insurance.

Presentation by Jose Hernandez, Chief Financial Officer.

ADOPTED AS: RESOLUTION NO. 24-047

MOTION: Approve an interlocal agreement with the Texas Municipal League for cyber liability and data breach response insurance.

RESULT: Approved (Unanimous); 7-0

MOTION: Nikelle Meade

SECONDED BY: Mike Doss

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

NAY: None.

13. Discuss and consider amending Mobility Authority Policy Code §101.038 to authorize the Executive Director to negotiate and execute certain settlement agreements for claims by or against the Mobility Authority.

Presentation by James Bass, Executive Director.

ADOPTED AS: RESOLUTION NO. 24-048

MOTION: Amend the Mobility Authority Policy Code §101.038 to authorize the Executive Director to negotiate and execute certain settlement agreements for claims by or against the Mobility Authority.

RESULT: Approved (Unanimous); 7-0

MOTION: Mike Doss

SECONDED BY: Heather Gaddes

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

NAY: None.

14. Discuss and consider approving an agreement with the North Texas Tollway Authority for TollTag™ marketing, promotional services and account enrollment.

Presentation by Tracie Brown, Director of Operations and Jori Liu, Director of Communications answered questions.

ADOPTED AS: RESOLUTION NO. 24-049

MOTION: Approve an agreement with the North Texas Tollway Authority for TollTag™ marketing, promotional services and account enrollment.

RESULT: Approved (Unanimous); 7-0

MOTION: Heather Gaddes

SECONDED BY: Nikelle Meade

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

NAY: None.

15. Discuss and consider approving an interlocal agreement with Travis County to assist with design and construction of the 2023 Travis County Proposition A Road Projects.

Presentation by Mike Sexton, Director of Engineering.

ADOPTED AS: RESOLUTION NO. 24-050

MOTION: Approve an interlocal agreement with Travis County to assist with design and construction of the 2023 Travis County Proposition A Road Projects.

RESULT: Approved (Unanimous); 7-0

MOTION: David Armbrust

SECONDED BY: Nikelle Meade

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

NAY: None.

Briefings and Reports

16. Quarterly Updates.

Presentation by Mike Sexton, Director of Engineering.

- A. 183A Phase III
- B. 183 North Mobility Project

17. Executive Director Report.

Presentation by James Bass, Executive Director.

- A. Recent agency staff activities.
- B. Agency roadway performance metrics.
- C. Update on efforts to increase pre-paid account penetration.
- D. Barton Skyway Ramp Relief celebration.

Executive Session

Chairman Jenkins announced in open session at 11:11 a.m. that the Board would recess the meeting and reconvene in Executive Session to deliberate the following items:

- 18. Discuss acquisition of one or more parcels or interests in real property needed for a Mobility Authority headquarters, including facilities for traffic and incident management and other agency functions, pursuant to §551.071 (Consultation with Attorney) and §551.072 (Deliberation Regarding Real Property; Closed Meeting).
- 19. 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).

20. Discuss legal issues related to the development of the Mopac South Project, as authorized by §551.071 (Consultation with Attorney).
21. 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).
22. Discuss personnel matters as authorized by §551.074 (Personnel Matters).

Regular Items

23. Adjourn meeting.

After confirming that no member of the public wished to address the Board, Chairman Jenkins declared the meeting adjourned at 12:23 p.m.



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024 AGENDA ITEM #3

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.

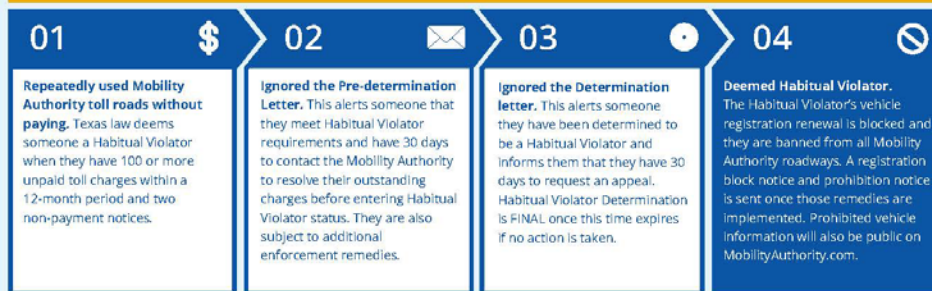
Action requested/Staff Recommendation: Staff affirms that all required steps have been followed and proper notice previously provided to customers determined to be habitual violators. To date, these customers have not appealed this determination or resolved their outstanding balances.

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. 24-0XX

**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 September 25, 2024; 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 September 2024.

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

September 25, 2024
AGENDA ITEM #4

Accept the unaudited financial
statements for August 2024

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 2024.

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

Financing: N/A

Action requested/Staff Recommendation: Accept the unaudited financial statements for August 2024.

Backup provided: Draft Resolution
Draft unaudited financial statements for August 2024

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

RESOLUTION NO. 24-0XX

ACCEPT THE UNAUDITED FINANCIAL STATEMENTS FOR AUGUST 2024

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 2024 and has caused financial statements to be prepared and attached to this resolution as Exhibit A; and

NOW THEREFORE, BE IT RESOLVED, that the Board of Directors accepts the unaudited financial statements for August 2024, attached hereto as Exhibit A.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of September 2024.

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
Income Statement
For the Period Ending August 31, 2024

	Budget Amount FY 2025	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
REVENUE				
Operating Revenue				
Toll Revenue	178,100,000	28,562,751	16.04%	25,745,239
Video Tolls	67,500,000	11,809,967	17.50%	8,447,113
Fee Revenue	13,200,000	2,845,900	21.56%	2,022,288
Total Operating Revenue	258,800,000	43,218,618	16.70%	36,214,639
Other Revenue				
Interest Income	43,025,800	6,454,347	15.00%	7,703,971
Grant Revenue	595,467	309,462	51.97%	-
Misc Revenue	100,000	5,890	5.89%	5,051
Gain/Loss on Sale of Asset	-	-	-	(476,728)
Unrealized Gain/Loss	-	123,484	-	-
Total Other Revenue	43,721,267	6,893,184	15.77%	7,232,294
TOTAL REVENUE	302,521,267	50,111,801	16.56%	43,446,933
EXPENSES				
Salaries and Benefits				
Salary Expense - Regular	4,994,532	569,109	11.39%	553,196
Salary Reserve	80,000	-	-	-
TCDRS	1,142,301	102,699	8.99%	103,773
FICA	257,234	30,583	11.89%	29,387
FICA MED	72,421	8,171	11.28%	7,948
Health Insurance Expense	586,073	78,943	13.47%	75,297
Life Insurance Expense	3,249	382	11.77%	458
Auto Allowance Expense	10,200	1,445	14.17%	1,445
Other Benefits	204,671	12,872	6.29%	11,159
Unemployment Taxes	5,760	-	-	-
Total Salaries and Benefits	7,356,441	804,205	10.93%	782,663
Administrative				
Administrative and Office Expenses				
Accounting	9,500	1,599	16.83%	1,265
Auditing	270,000	-	-	-
Financial Advisors	200,000	27,900	13.95%	36,000
Human Resources	100,000	128	0.13%	168
Legal	60,000	1,180	1.97%	4,750
IT Services	365,000	54,390	14.90%	24,503
Software Licenses	1,573,150	1,228,954	78.12%	685,645
Cell Phones	34,900	2,160	6.19%	3,326
Local Telephone Service	2,200	407	18.48%	17,386
Overnight Delivery Services	200	-	-	-
Copy Machine	15,300	2,544	16.63%	2,544
Repair & Maintenance-General	10,000	-	-	-
Meeting Facilities	2,500	-	-	-
Meeting Expense	13,750	279	2.03%	489
Toll Tag Expense	3,000	200	6.67%	100
Parking / Local Ride Share	2,500	39	1.56%	27
Mileage Reimbursement	4,600	87	1.88%	85
Insurance Expense	1,301,000	160,952	12.37%	98,062

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending August 31, 2024

	Budget Amount FY 2025	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Rent Expense	992,200	45,571	4.59%	11,939
Building Parking	3,500	67	1.90%	70
Total Legal Services	458,000	-	-	18,793
Total Administrative and Office Expenses	5,421,300	1,526,455	28.16%	905,150
Office Supplies				
Books & Publications	5,250	596	11.35%	639
Office Supplies	5,250	227	4.32%	88
Misc Office Equipment	4,500	-	-	-
Computer Supplies	201,850	5,837	2.89%	7,515
Copy Supplies	750	-	-	-
Other Reports - Printing	500	-	-	-
Office Supplies - Printed	3,500	496	14.18%	102
Postage Expense	900	-	-	329
Total Office Supplies	222,500	7,156	3.22%	8,672
Communications and Public Relations				
Print Production	75,000	-	-	-
Website Maintenance	240,000	11,361	4.73%	76,740
Research Services	210,000	11,900	5.67%	-
Communications and Marketing	500,000	5,953	1.19%	11,940
Media Planning and Placement	1,000,000	19,554	1.96%	164,199
Direct Mail Production	60,000	-	-	-
TV and Video Production	250,000	-	-	-
Photography	25,000	850	3.40%	295
Radio Production	50,000	-	-	-
Other Public Relations	20,000	10,000	50.00%	-
Promotional Items	20,000	-	-	1,166
Printing	80,000	-	-	-
Other Communication Expenses	15,000	3,403	22.69%	-
Total Communications and Public Relations	2,545,000	63,021	2.48%	254,340
Employee Development				
Subscriptions	1,250	139	11.12%	139
Agency Memberships	88,300	35	0.04%	25
Continuing Education	14,800	-	-	-
Professional Development	21,400	3,285	15.35%	-
Other Licenses	2,000	-	-	-
Seminars and Conferences	70,300	3,475	4.94%	1,445
Travel	107,000	9,180	8.58%	12,892
Total Employee Development	305,050	16,114	5.28%	14,501
Financing and Banking Fees				
Trustee Fees	75,000	15,000	20.00%	15,000
Bank Fee Expense	6,500	1,100	16.93%	947
Continuing Disclosure	10,000	-	-	-
Arbitrage Rebate Calculation	16,500	-	-	-
Rating Agency Expense	50,000	33,500	67.00%	32,500
Total Financing and Banking Fees	158,000	49,600	31.39%	48,447
Total Administrative	8,651,850	1,662,347	19.21%	1,231,111

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending August 31, 2024

	Budget Amount FY 2025	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Operations and Maintenance				
Operations and Maintenance Consulting				
GEC-Trust Indenture Support	1,568,659	253,831	16.18%	251,825
GEC-Financial Planning Support	300,000	56,861	18.95%	50,386
GEC-Toll Ops Support	1,142,136	281,962	24.69%	152,814
GEC-Roadway Ops Support	1,515,000	155,228	10.25%	108,083
GEC-Technology Support	804,962	67,508	8.39%	167,549
GEC-Public Information Support	200,000	38,627	19.31%	23,711
GEC-General Support	2,226,000	287,635	12.92%	162,027
General System Consultant	2,307,274	135,446	5.87%	27,875
Traffic Modeling	125,000	-	-	-
Traffic and Revenue Consultant	1,200,000	176,961	14.75%	34,518
Total Operations and Maintenance Consulting	11,389,031	1,454,059	12.77%	978,788
Roadway Operations and Maintenance				
Roadway Maintenance	4,169,031	487,458	11.69%	503,586
Landscape Maintenance	3,249,260	480,554	14.79%	461,740
Signal & Illumination Maint	25,000	-	-	-
Maintenance Supplies-Roadway	400,000	-	-	-
Tools & Equipment Expense	-	957	-	-
Gasoline	30,000	2,876	9.59%	3,729
Repair & Maintenance - Vehicles	10,000	(1,694)	-16.94%	360
Natural Gas	7,500	1,525	20.34%	1,025
Electricity - Roadways	300,000	31,400	10.47%	40,653
Total Roadway Operations and Maintenance	8,190,791	1,003,077	12.25%	1,011,093
Toll Processing and Collection Expense				
Image Processing	3,300,000	400,191	12.13%	236,147
Tag Collection Fees	12,675,000	1,952,766	15.41%	1,793,431
Court Enforcement Costs	160,000	-	-	-
PBM Incentive	500,000	-	-	-
Total Processing and Collection Expense	16,635,000	2,352,958	14.14%	2,029,578
Toll Operations Expense				
Generator Fuel	3,000	-	-	-
Fire & Burglar Alarm	500	82	16.45%	82
Refuse	2,360	335	14.21%	300
Telecommunications	100,000	23,144	23.14%	-
Water - Irrigation	7,500	447	5.96%	1,409
Electricity	750	154	20.52%	178
ETC Spare Parts Expense	150,000	21,285	14.19%	-
Repair & Maintenance Toll Equip	100,000	-	-	-
Law Enforcement	725,000	82,379	11.36%	81,143
ETC Maintenance Contract	6,450,000	50,029	0.78%	499,698
Transaction Processing Maintenance Contract	2,000,000	-	-	-
ETC Toll Management Center System Operation	1,338,822	43,776	3.27%	112,851
ETC Development	456,000	-	-	29,106
ETC Testing	50,000	-	-	-
Total Toll Operations Expense	11,383,932	221,632	1.95%	724,766
Total Operations and Maintenance	47,598,754	5,031,725	10.57%	4,744,225

Central Texas Regional Mobility Authority
Income Statement
For the Period Ending August 31, 2024

	Budget Amount FY 2025	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
Other Expenses				
Special Projects and Contingencies				
HERO	711,621	-	-	24,638
Special Projects	50,000	-	-	-
Disbursement Other Government - Travis County Road	-	5,890	-	-
71 Express Interest Expense	6,750,000	290,561	4.30%	1,075,128
Customer Relations	10,000	-	-	-
Technology Initiatives	100,000	-	-	-
Other Contractual Svcs	390,000	32,000	8.21%	40,500
Contingency	200,000	-	-	-
Total Special Projects and Contingencies	8,211,621	328,452	4.00%	1,140,267
TOTAL OPERATING EXPENSE	71,818,666	7,826,729	10.90%	7,898,265
Non Cash Expenses				
Amortization Expense				
Amortization Expense - Intangible Software	-	239,186	-	-
Amortization Expense - Software	13,000,000	-	-	4,233
Amortization Expense - Right to Use Asset - Leases	515,000	85,792	16.66%	-
Amortization Expense - Refundings	6,600,000	1,150,328	17.43%	1,024,236
Subtotal Amortization Expense	20,115,000	1,475,307	7.33%	1,028,469
Depreciation Expense				
Dep Expense - Equipment	-	-	-	103,784
Dep Expense - Autos & Trucks	31,000	5,068	16.35%	5,068
Dep Expense - Buildng & Toll Fac	180,000	29,458	16.37%	29,458
Dep Expense - Highways & Bridges	53,500,000	8,753,846	16.36%	8,472,925
Dep Expense - Toll Equipment	13,640,000	565,365	4.14%	506,497
Dep Expense - Signs	1,830,000	224,639	12.28%	201,492
Dep Expense - Land Improvements	545,000	90,387	16.58%	117,969
Subtotal Depreciation Expense	69,726,000	9,668,763	13.87%	9,437,194
Total Non Cash Expenses	89,841,000	11,144,070	12.40%	10,465,663
Non Operating Expenses				
Interest Expense - Debt Obligations	109,112,756	16,539,087	15.16%	13,329,994
CAMPO RIF Payment	10,000,000	-	-	-
Community Initiatives	600,000	10,919	1.82%	-
Total Non Operating Expenses	119,712,756	16,550,006	13.82%	13,329,994
TOTAL EXPENSES	281,372,422	35,520,806	12.62%	31,693,922
Net Income	21,148,845	14,590,996		11,753,011

Central Texas Regional Mobility Authority
Balance Sheet
as of August 31, 2024

	as of 08/31/2024	as of 08/31/2023
ASSETS		
Current Assets		
Cash		
Regions Operating Account	52,184	121,234
Cash in TexStar	2,007,338	304,100
Regions Payroll Account	110,443	107,719
Restricted Cash		
Goldman Sachs FSGF 465	288,971,595	582,135,790
Restricted Cash - TexSTAR	31,186,952	8,682,213
Treasury SLGS	242,071,728	-
Total Cash and Cash Equivalents	564,400,240	591,351,056
Accounts Receivables		
Accounts Receivable - Net	8,167,796	4,979,871
Due From Other Agencies	380,952	226,563
Due From TTA	1,591,018	668,161
Due From NTTA	1,924,326	1,517,325
Due From HCTRA	2,568,227	3,771,136
Due From TxDOT	9,774,045	7,565,900
Due From Other Funds	1,700,306	-
Interest Receivable	1,045,052	693,342
Total Receivables	27,151,722	19,422,298
Short Term Investments		
Treasuries	163,106,750	118,543,252
Agencies	250,712,604	339,758,036
Total Short Term Investments	413,819,354	458,301,288
Total Current Assets	1,005,371,316	1,069,074,642
Construction in Progress	510,366,428	359,724,901
Capital Assets (Net of Depreciation and Amortization)		
Depreciable Assets		
Equipment	-	1,297,304
Autos and Trucks	11,404	41,813
Buildings and Toll Facilities	4,023,755	4,200,503
Highways and Bridges	1,672,250,167	1,716,987,621
Toll Equipment	21,611,362	15,152,659
Signs	11,260,968	11,171,404

Central Texas Regional Mobility Authority
Balance Sheet
as of August 31, 2024

	as of 08/31/2024	as of 08/31/2023
Land Improvements	4,654,042	5,196,366
Right of way	88,149,606	88,149,606
Leasehold Improvements	-	297,427
Intangible Assets		
Intangible Software	5,736,486	-
Right to Use Assets		
Leases	857,921	-
Total Fixed Assets	1,808,555,712	1,842,494,702
Other Assets		
Intangible Assets-Net	161,299,711	167,789,496
Prepaid Insurance	80,476	49,031
Deferred Outflows (pension related)	2,384,338	2,738,023
Pension Asset	-	1,046,634
Total Other Assets	163,764,524	171,623,184
Total Assets	3,488,057,980	3,442,917,429
LIABILITIES		
Current Liabilities		
Accounts Payable	14,361,164	4,880,130
Construction Payable	-	4,182,841
Overpayments	-	1,570
Interest Payable	16,186,142	13,590,075
Due to other Funds	1,700,306	-
TCDRS Payable	84,542	82,304
Due to other Agencies	12,044	3,779
Due to TTA	694,164	652,223
Due to HCTRA	170,670	161,897
Due to Other Entities	-	1,883,620
71E TxDOT Obligation - ST	998,218	3,761,703
Total Current Liabilities	34,207,250	29,200,141
Long Term Liabilities		
Compensated Absences	662,277	240,954
Right to Use Obligations - Lease	747,552	1,286,881
Deferred Inflows (pension related)	1,192,688	1,378,935
Pension Liability	1,971,627	-
Long Term Payables	4,574,144	2,906,771

Central Texas Regional Mobility Authority
Balance Sheet
as of August 31, 2024

	as of 08/31/2024	as of 08/31/2023
Bonds Payable		
Senior Lien Revenue Bonds:		
Senior Lien Revenue Bonds 2010	104,930,158	95,580,925
Senior Lien Revenue Bonds 2011	9,901,932	16,373,850
Senior Lien Revenue Bonds 2015	10,000,000	10,000,000
Senior Lien Refunding Revenue Bonds 2016	47,045,000	59,340,000
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	54,305,000	54,970,000
Senior Lien Refunding Bonds 2020C	133,210,000	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	273,650,000	274,150,000
Senior Lien Refunding Bonds 2021E	329,545,000	332,585,000
Senior Lien Premium 2016 Revenue Bonds	6,043,584	6,675,724
Sn Lien Revenue Bond Premium 2018	2,572,216	2,838,789
Senior Lien Revenue Bond Premium 2020A	10,888,713	11,130,761
Senior Lien Refunding Bond Premium 2020B	10,612,326	11,147,401
Senior Lien Revenue Bonds Premium 2020E	22,139,251	23,854,638
Senior Lien Revenue Bonds Premium 2021B	52,322,473	52,890,189
Senior Lien Refunding Bonds Premium 2021D	43,462,616	44,278,923
Total Senior Lien Revenue Bonds	1,627,473,270	1,651,096,201
Sub Lien Revenue Bonds:		
Sub Lien Refunding Bonds 2016	69,055,000	71,435,000
Sub Lien Refunding Bonds 2020D	93,430,000	97,440,000
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 2016 Prem/Disc	4,127,742	4,862,401
Subordinated Lien BANs 2020F Premium	1,334,288	5,337,153
Subordinated Lien Refunding Bonds Premium 2020G	6,292,947	6,696,919
Sub Lien BANS 2021C Premium	17,760,580	25,372,258
Total Sub Lien Revenue Bonds	608,630,558	627,773,731

Central Texas Regional Mobility Authority
Balance Sheet
as of August 31, 2024

	as of 08/31/2024	as of 08/31/2023
Other Obligations		
TIFIA Note 2021 - 183S	322,354,437	360,361,691
TIFIA Note 2021 - 290E	41,088,581	-
71E TxDOT Obligation - LT	47,253,089	51,918,220
Regions 2022 MoPac Loan	22,490,900	23,765,900
Total Other Obligations	433,187,007	436,045,811
Total Long Term Liabilities	2,673,864,979	2,717,822,513
Total Liabilities	2,708,072,229	2,747,022,654
NET ASSETS		
Contributed Capital	-	121,462,104
Net Assets Beginning	765,394,755	563,196,620
Current Year Operations	14,590,996	11,753,011
Total Net Assets	779,985,751	696,411,735
Total Liabilities and Net Assets	3,488,057,980	3,443,434,389

Central Texas Regional Mobility Authority

Statement of Cash Flow

as of August 2024

Cash flows from operating activities:

Receipts from toll revenues	48,357,538
Receipts from other sources	438,837
Payments to vendors	(42,076,440)
Payments to employees	(814,102)
Net cash flows provided by (used in) operating activities	5,905,833

Cash flows from capital and related financing activities:

Payment on Intangible assets	(1,150,328)
Interest Expense	(44,163,557)
Issuance Expense	(24,081)
Payments on bonds / loans	(8,576,425)
RIF Contribution	-
Acquisition of capital assets - non project	(948,622)
Acquisitions of construction in progress	(7,223,466)
Net cash flows provided by (used in) capital and related financing activities	(62,086,478)

Cash flows from investing activities:

Interest income	6,419,769
Purchase of investments	(176,367,756)
Net cash flows provided by (used in) investing activities	(169,947,987)

Net increase (decrease) in cash and cash equivalents	(226,128,632)
Cash and cash equivalents at beginning of period	817,680,594
Cash and cash equivalents at end of period	591,551,962

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

Operating income	14,590,996
Adjustments to reconcile change in net assets to net cash provided by operating activities:	
Depreciation and amortization	11,144,070
Changes in assets and liabilities:	
Decrease in accounts receivable	5,138,921
Increase in prepaid expenses and other assets	160,952
Decrease in accrued expenses	(35,224,765)
Decrease in Interest expense	16,550,006
Increase in interest receivable	(6,454,347)
Total adjustments	(8,685,163)
Net cash flows provided by (used in) operating activities	\$ 5,905,833

Reconciliation of cash and cash equivalents:

Unrestricted cash and cash equivalents	271,393,414
Restricted cash and cash equivalents	320,158,548
Total	591,551,962

CTRMA INVESTMENT REPORT
Month Ending August 31, 2024

	Balance 8/1/2024	Accrued Interest	Additions	Cash Transfers	Withdrawals	Balance 8/31/2024	Rate August '24
Amount in Trustee TexStar							
2011 Sr Lien Financial Assist Fund	16.82	0.04				16.86	5.29%
2013 Sub Lien Debt Service Reserve	859,433.68	3,864.17				863,297.85	5.29%
General Fund	10,129,804.91	45,545.37				10,175,350.28	5.29%
Trustee Operating Fund	9,966,675.98	65,693.90		7,000,000.00		17,032,369.88	5.29%
Renewal and Replacement	8.70					8.70	5.29%
TxDOT Grant Fund	500,428.74	2,250.02				502,678.76	5.29%
Senior Lien Debt Service Reserve Fund	425,335.06	1,912.37				427,247.43	5.29%
2015B Sr Ln Project	385,199.83	1,731.92				386,931.75	5.29%
2015C Sub TIFIA Project	765,260.15	3,440.77				768,700.92	5.29%
2018 Sr Lien Project	1,025,738.06	4,611.92				1,030,349.98	5.29%
	24,057,901.93	129,050.48	-	7,000,000.00	-	31,186,952.41	
Amount in TexStar Operating Fund							
	3,498,209.31	9,129.07		3,000,000.00	4,500,000.00	2,007,338.38	5.29%
Goldman Sachs							
Operating Fund	4,337,101.12	19,159.52	258,035.50	-	3,688.28	4,610,607.86	5.19%
2020A Senior Lien Debt Service	4,742.59	20.28		418,875.00		423,637.87	5.19%
2020B Senior Lien Debt Service	353,774.17	1,562.43		553,675.00		909,011.60	5.19%
2020C Senior Lien Debt Service	2,569,174.95	11,350.79		1,468,976.66		4,049,502.40	5.19%
2020D Sub Lien Debt Service	2,054,714.24	9,078.03		1,161,711.42		3,225,503.69	5.19%
2020D Sub Debt Service Reserve Fund	1,094,158.81	7,057.95				1,101,216.76	5.19%
2020E Sr Lien Project	98,121,424.55	452,321.83	66,749.91		6,120,829.91	92,519,666.38	5.19%
2020E Sr Ln Project Cap Interest	8,312,519.17	36,725.65				8,349,244.82	5.19%
2020F Sub Lien Debt Service	151,217.74	666.73		923,958.34		1,075,842.81	5.19%
2020G Sub Lien Debt Service	4,616.26	19.74		425,433.34		430,069.34	5.19%
2020G Sub Debt Service Reserve Fund	463,367.87	3,158.58				466,526.45	5.19%
2021A Sub Debt Service Reserve Fund	1,953,458.18	14,189.98				1,967,648.16	5.19%
2021A TIFIA Sub Lien Debt Service Acct	523,178.17	2,309.47				525,487.64	5.19%
2021B Senior Lien Cap I Project Fund	25,952,735.88	114,665.62				26,067,401.50	5.19%
2021B Senior Lien Project	24,264,709.34	103,117.55			24,000,000.00	367,826.89	5.19%
2021B Senior Lien Cap I Debt Service Acct	9,392.92	41.42				9,434.34	5.19%
2021C Sub Lien Cap I Project Fund	1,463.42	6.47				1,469.89	5.19%
2021C Sub Lien Project	8,510,776.38	33,124.26			2,207,759.59	6,336,141.05	5.19%
2021C Sub Lien Debt Service	21,926.73	93.77		2,034,875.00		2,056,895.50	5.19%
2021D Senior Lien Debt Service	284,571.01	1,254.37		1,949,000.00		2,234,825.38	5.19%
2021E Senior Lien Debt Service	1,616,852.45	7,141.39		2,148,786.40		3,772,780.24	5.19%
2011 Sr Financial Assistance Fund	143.29	0.63				143.92	5.19%
2010 Senior DSF	4,517,137.07	19,961.19		1,292,342.60		5,829,440.86	5.19%
2011 Senior Lien Debt Service	3,741,625.82	16,534.21		1,112,806.62		4,870,966.65	5.19%
2013 Senior Lien Debt Service	44,024.10	194.54				44,218.64	5.19%
2013 Sub Debt Service Reserve Fund	135.02	0.60				135.62	5.19%
2013 Subordinate Debt Service	34,648.36	153.11				34,801.47	5.19%
2015A Sr Lien Debt Service	4,589,586.71	91.12		416,666.66		5,006,344.49	5.19%
2015B Project	4,946,582.52	22,687.14			27,335.52	4,941,934.14	5.19%
2015C TIFIA Project	1,119,220.29	22,045.56				1,141,265.85	5.19%
2016 Sr Lien Rev Refunding Debt Service	8,764,341.51	38,729.56				8,803,071.07	5.19%
2016 Sub Lien Rev Refunding Debt Service	1,395,145.44	6,165.14		980,543.76		2,381,854.34	5.19%
2016 Sub Lien Rev Refunding DSR	838,531.62	5,651.52				844,183.14	5.19%
2018 Sr Lien Debt Service	506,063.82	2,235.43		536,208.34		1,044,507.59	5.19%
2018 Sr Lien Project	12,298,403.45	54,427.46			188,315.96	12,164,514.95	5.19%
TxDOT Grant Fund	526,321.98	2,325.81				528,647.79	5.19%
Renewal and Replacement	18.29	337.89		56,500.00	56,816.17	40.01	5.19%
Revenue Fund	27,433,657.34	78,075.22	19,692,536.44	(36,542,439.54)		10,661,829.46	5.19%
General Fund	17,775,914.82	122,402.36		9,513,317.30	50,662.84	27,360,971.64	5.19%
Senior Lien Debt Service Reserve Fund	3,328,572.84	71,984.85				3,400,557.69	5.19%
71E Revenue Fund	6,700,121.60	27,797.11	896,437.11	741,843.57	78,473.10	8,287,726.29	5.19%
MoPac Revenue Fund	93,139.63	2,365.57	410,919.30	(431,385.23)		75,039.27	5.19%
MoPac General Fund	9,881,465.32	41,142.02	10,186,000.00	660,712.76		20,769,320.10	5.19%
MoPac Operating Fund	2,480,224.93	10,792.98	251,980.00	400,000.00	371,950.46	2,771,047.45	5.19%
MoPac Loan Repayment Fund	204,852.18	271.73		177,592.00		382,715.91	5.19%
	291,825,753.90	1,363,438.58	31,762,658.26	(10,000,000.00)	33,105,831.83	281,846,018.91	
Amount in Fed Agencies and Treasuries							
Amortized Principal	423,818,728.30	-	-	-	9,999,374.37	413,819,353.93	
Certificates of Deposit							
Total in Pools - TxStar	27,556,111.24	138,179.55	-	10,000,000.00	4,500,000.00	33,194,290.79	
Total in GS FSGF	291,825,753.90	1,363,438.58	31,762,658.26	(10,000,000.00)	33,105,831.83	281,846,018.91	
Total in Treasury SLGS	245,000,000.00	2,571,727.52	24,000,000.00		29,500,000.00	242,071,727.52	
Total in Fed Agencies and Treasuries	423,818,728.30	-	-	-	9,999,374.37	413,819,353.93	
Total Invested	988,200,593.44	4,073,345.65	55,762,658.26	-	77,105,206.20	970,931,391.15	

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 2256.023

José Hernández, CFO

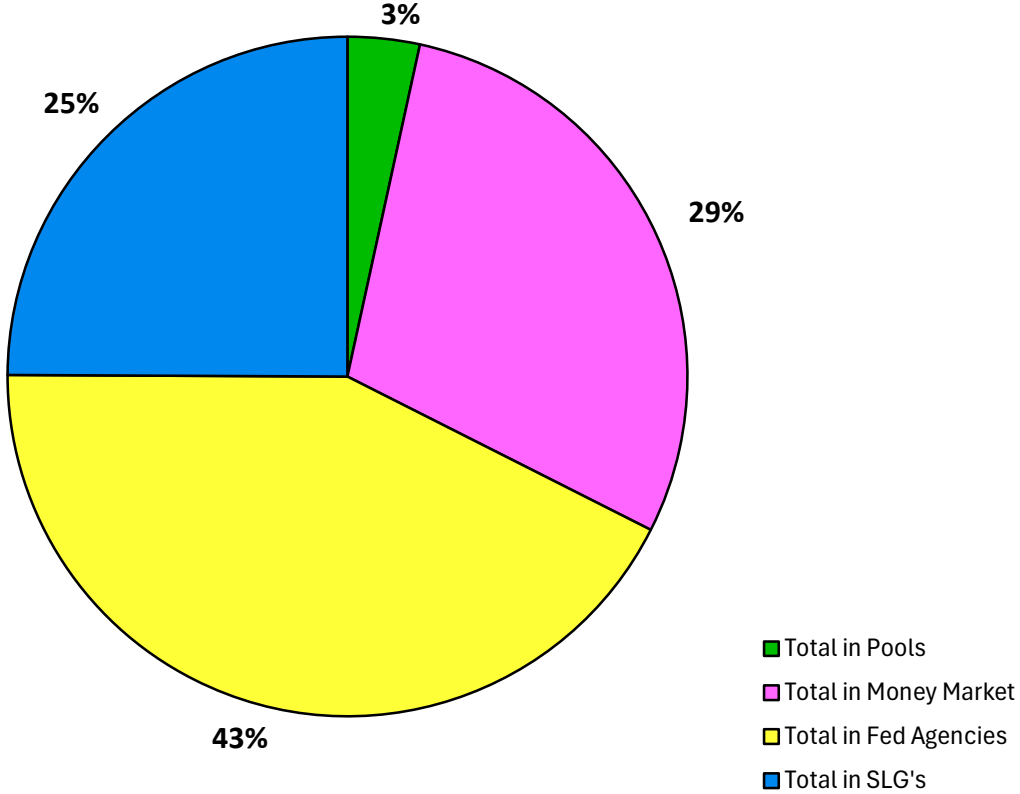
Ann Zigmund, Controller

Investments by Fund

Fund	TexSTAR	TexSTAR-Trustee	Goldman Sachs	Agencies / Treasuries / SLGS	Balance
Renewal and Replacement Fund	8.70		40.01		48.71
Grant Fund	502,678.76		528,647.79	10,000,000.00	11,031,326.55
Senior Debt Service Reserve Fund	427,247.43		3,400,557.69	114,051,334.25	117,879,139.37
2010 Senior Lien Debt Service			5,829,440.86		5,829,440.86
2011 Sr Debt Service t			4,870,966.65		4,870,966.65
2013 Sr Debt Service t			44,218.64		44,218.64
2013 Sub Debt Service			34,801.47		34,801.47
2013 Sub Debt Service Reserve Fund	863,297.85		135.62		863,433.47
2015 Sr Debt Service			5,006,344.49		5,006,344.49
2016 Sr Lien Rev Refunding Debt Service			8,803,071.07		8,803,071.07
2016 Sub Lien Rev Refunding Debt Service			2,381,854.34		2,381,854.34
2016 Sub Lien Rev Refunding DSR			844,183.14	6,825,843.85	7,670,026.99
Operating Fund	17,032,369.88	2,007,338.38	4,610,607.86		23,650,316.12
Revenue Fund			10,661,829.46		10,661,829.46
General Fund	10,175,350.28		27,360,971.64	182,098,391.72	219,634,713.64
71E Revenue Fund			8,287,726.29	29,639,926.50	37,927,652.79
MoPac Revenue Fund			75,039.27		75,039.27
MoPac General Fund			20,769,320.10		20,769,320.10
MoPac Operating Fund			2,771,047.45		2,771,047.45
MoPac Loan Repayment Fund			382,715.91		382,715.91
2015B Project	386,931.75		4,941,934.14		5,328,865.89
2015 TIFIA Project	768,700.92		1,141,265.85	40,000,000.00	41,909,966.77
2011 Sr Financial Assistance Fund	16.86		143.92		160.78
2018 Sr Lien Debt Service			1,044,507.59		1,044,507.59
2018 Sr Lien Project Cap I			-		-
2018 Sr Lien Project	1,030,349.98		12,164,514.95		13,194,864.93
2020A Senior Lien Debt Service			423,637.87		423,637.87
2020B Senior Lien Debt Service			909,011.60		909,011.60
2020C Senior Lien Debt Service			4,049,502.40		4,049,502.40
2020D Sub Lien Debt Service			3,225,503.69		3,225,503.69
2020D Sub Debt Service Reserve Fund			1,101,216.76	7,800,964.40	8,902,181.16
2020E Senior Lien Project			92,519,666.38		92,519,666.38
2020E Senior Lien Project Cap Interest			8,349,244.82		8,349,244.82
2020F Sub Lien Project			-		-
2020F Sub Lien Deb Service			1,075,842.81		1,075,842.81
2020G Sub Lien Debt Service			430,069.34		430,069.34
2020G Sub Lien Debt Service Reserve			466,526.45	3,900,482.20	4,367,008.65
2021A Sub Lien Debt Service Reserve			1,967,648.16	19,502,411.01	21,470,059.17
2021A Sub Debt Service			525,487.64		525,487.64
2021B Senior Lien Cap I Project Fund			26,067,401.50		26,067,401.50
2021B Senior Lien Project			367,826.89	212,312,599.93	212,680,426.82
2021B Senior Lien Cap I Debt Service Acct			9,434.34		9,434.34
2021C Sub Lien Cap I Project Fund			1,469.89	5,759,127.59	5,760,597.48
2021C Sub Lien Project			6,336,141.05		6,336,141.05
2021C Sub Lien Debt Service			2,056,895.50		2,056,895.50
2021D Senior Lien Debt Service			2,234,825.38		2,234,825.38
2021E Senior Lien Debt Service			3,772,780.24		3,772,780.24
Totals	31,186,952.41	2,007,338.38	281,846,018.91	631,891,081.45	946,931,391.15

8/31/2024

Allocation of Funds



Bank	Fund	Cost	Cummulative Amortization	Book Value	Maturity Value	Interest Income		
						Accrued Interest	Amortization	Interest Earned
6180000120	GENERAL	40,000,000.00		40,000,000.00	40,000,000.00			
6180000120	GENERAL	9,960,128.90		9,960,128.90	10,000,000.00	27,777.78		527,777.78
6180000120	GENERAL	9,960,128.90		9,960,128.90	10,000,000.00	27,777.78		527,777.78
6180000120	GENERAL	41,501,020.00		41,501,020.00	43,000,000.00			
6180000059	SENLIENCSR	9,651,400.00		9,651,400.00	10,000,000.00			
6180000120	GENERAL	48,794,377.50		48,794,377.50	50,000,000.00			
6180006366	2016SUBCSR	6,825,843.85		6,825,843.85	7,000,000.00			
1001017484	2020D DSRF	7,800,964.40		7,800,964.40	8,000,000.00			
1001021540	2020G DSRF	3,900,482.20		3,900,482.20	4,000,000.00			
1001021543	2021A DSRF	19,502,411.01		19,502,411.01	20,000,000.00			
6180000059	SENLIENCSR	30,228,737.05		30,228,737.05	31,000,000.00			
6180000059	SENLIENCSR	34,171,197.20		34,171,197.20	35,000,000.00			
6180000059	SENLIENCSR	20,000,000.00		20,000,000.00	20,000,000.00	22,222.22		1,022,222.22
6146001086	71E REVENU	15,000,000.00		15,000,000.00	15,000,000.00			
6146001086	71E REVENU	14,639,926.50		14,639,926.50	14,670,000.00	97,800.00		366,750.00
6180000120	GENERAL	11,882,736.42		11,882,736.42	12,000,000.00	113,036.99		288,340.12
6180000120	GENERAL	20,000,000.00		20,000,000.00	20,000,000.00			954,000.00
6180000059	SENLIENCSR	20,000,000.00		20,000,000.00	20,000,000.00			954,000.00
6180005349	2015TIFIAP	10,000,000.00		10,000,000.00	10,000,000.00			104,430.56
6180000157	TXDOTGRANT	10,000,000.00		10,000,000.00	10,000,000.00			104,430.56
6180005349	2015TIFIAP	30,000,000.00		30,000,000.00	30,000,000.00			
		413,819,353.93	-	413,819,353.93	419,670,000.00	288,614.77	-	4,745,298.46

Goldman Sachs County Road Escrow Funds

	Balance	Accrued			Balance
	8/1/2024	Interest	Additions	Withdrawals	8/31/2024
Travis County Escrow Fund - Elroy Road	3,096,962.54	13,728.34			3,110,690.88
Travis County Escrow Fund - Ross Road	334,366.80	1,506.63			335,873.43
Travis County Escrow Fund - Old San Antonio Road	113,831.47	569.04			114,400.51
Travis County Escrow Fund - Old Lockhart Road	271,958.41	1,264.12			273,222.53
Travis County Escrow Fund - County Line Road	2,611,771.78	11,855.90			2,623,627.68
Travis County Escrow Fund - South Pleasant Valley Road	249,801.16	1,143.46			250,944.62
Travis County Escrow Fund - Thaxton Road	198,111.37	911.00			199,022.37
Travis County Escrow Fund - Pearce Lane Road	216,791.19	1,003.20			217,794.39
	7,093,594.72	31,981.69	-	-	7,125,576.41

State and Local Government Series as of 8/31/24

Bank	Fund	Agency	Arbitrage Yield	CUSIP	Yield	Purchased Date	Purchase Value	Beginning	Accrued Interest	Withdrawals	End Value
1001021281	2021CPROJ	State and Local Government Series (SLGS)	1.831%	99SLA1060	4.18%	4/23/2024	35,000,000.00	35,000,000.00	259,127.59	29,500,000.00	5,759,127.59
1001021273	2021BPROJ	State and Local Government Series (SLGS)	1.831%	99SLA1078	4.18%	4/23/2024	210,000,000.00	210,000,000.00	2,312,599.93	-	212,312,599.93
1001021273	2021BPROJ	State and Local Government Series (SLGS)	1.831%	99SLA1870	4.18%	8/9/2024	24,000,000.00	24,000,000.00	-	-	24,000,000.00
											-
											-
							269,000,000.00	269,000,000.00	2,571,727.52	29,500,000.00	242,071,727.52



PERFORMANCE

As of August 31, 2024

Current Invested Balance	\$ 10,960,587,143.65
Weighted Average Maturity (1)	29 Days
Weighted Average Life (2)	65 Days
Net Asset Value	1.000150
Total Number of Participants	1048
Management Fee on Invested Balance	0.06%*
Interest Distributed	\$ 51,237,508.47
Management Fee Collected	\$ 572,671.72
% of Portfolio Invested Beyond 1 Year	5.08%
Standard & Poor's Current Rating	AAAm

August Averages

Average Invested Balance	\$ 11,268,338,188.51
Average Monthly Yield, on a simple basis	5.2939%
Average Weighted Maturity (1)	31 Days
Average Weighted Life (2)	61 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.

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

NEW PARTICIPANTS

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

- * Gladewater Economic Development Corporation
- * Galveston County Municipal Utility District No. 73
- * Harris - Waller Counties Municipal Utility District No. 12
- * City of Nacogdoches
- * Navarro College

HOLIDAY REMINDER

In observance of **Columbus Day**, **TexSTAR will be closed on Monday, October 14, 2024**. All ACH transactions initiated on Friday, October 11th will settle on Tuesday, October 15th. Standard transaction deadlines will be observed on Friday, October 11th. Please plan accordingly for your liquidity needs.

ECONOMIC COMMENTARY

Market review

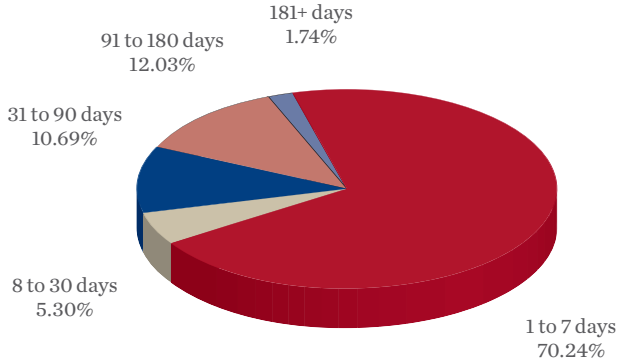
August has a reputation for a relatively quiet market environment, but this year was an exception. The first few weeks of the month provided a stark reminder of how sensitive markets can be to subtle changes in the macroeconomic outlook. A slight weakening in the labor market pushed the unemployment rate onto a path that has historically signaled impending recessions. In response, from July 31st to August 5th, Treasury yields plummeted, the VIX index—a key measure of stock market volatility—more than doubled, and stock prices took a significant hit. Although, volatility has since eased, data in August continued to strengthen the argument for the Federal Reserve (Fed) to cut rates in an effort to achieve a soft landing. The July Jobs report highlighted the ongoing cooling trend in the labor market, with job gains growing only 114,000. For the fourth consecutive month, the unemployment rate increased, this time by 0.2% to 4.3%, triggering the Sahm Rule (an empirical observation that predicts recession when the three-month moving average of the unemployment rate exceeds its lowest level over the prior 12 months by 0.5% or more), suggesting a labor market that is cooling faster than comfortable. However, while this has been a reliable recession indicator in the past, the current rise in unemployment was primarily due to an increase in labor supply rather than layoffs.

Additionally, recent benchmark revisions to nonfarm payrolls revealed that job growth in the 12 months leading up to March 2024 was less robust than initially estimated. Nonfarm payrolls were revised down by 818,000, translating to a monthly downward adjustment of approximately 68,000. The Job Openings and Labor Turnover Survey (JOLTS) also showed a decline in job openings in July from 7.9 million to 7.7 million, indicating a softening in labor demand. The ratio of job openings to unemployment fell from 1.16 to 1.07, dropping below to pre-COVID levels.

(continued page 4)

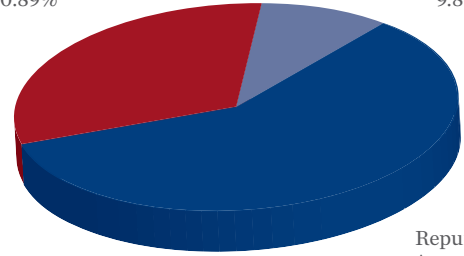
INFORMATION AT A GLANCE

PORTFOLIO BY TYPE OF INVESTMENT AS OF AUGUST 31, 2024

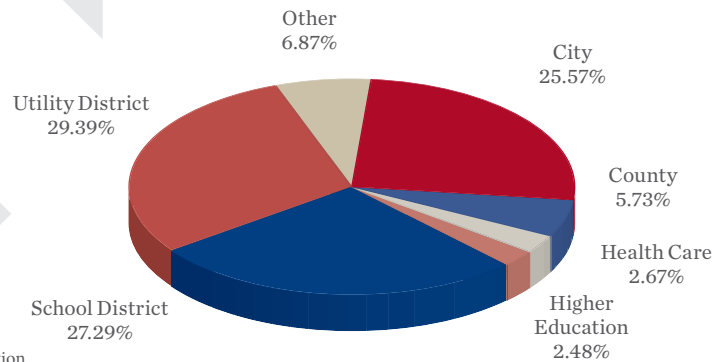


Treasuries
30.89%

Agencies
9.84%



PORTFOLIO BY MATURITY AS OF AUGUST 31, 2024 (1)



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

HISTORICAL PROGRAM INFORMATION

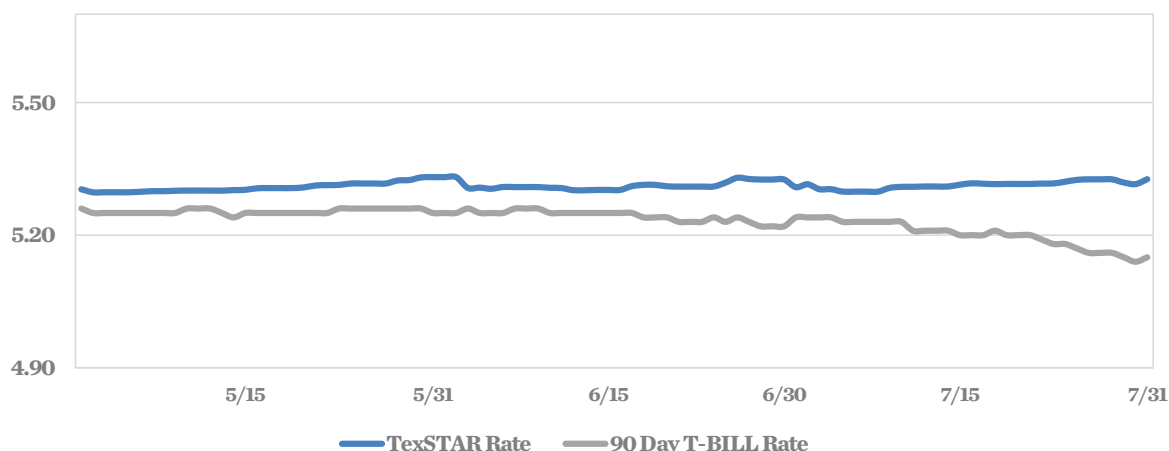
MONTH	AVERAGE RATE	BOOK VALUE	MARKET VALUE	NET ASSET VALUE	WAM (1)	WAL (2)	NUMBER OF PARTICIPANTS
Aug 24	5.2939%	\$10,960,587,143.65	\$10,963,170,866.05	1.000150	31	61	1048
Jul 24	5.3131%	11,614,008,231.39	11,614,697,399.72	1.000059	33	64	1043
Jun 24	5.3126%	10,696,510,063.51	10,695,858,054.79	0.999939	36	66	1040
May 24	5.3078%	10,946,135,253.27	10,946,064,280.53	0.999895	37	67	1037
Apr 24	5.3057%	11,388,285,240.44	11,386,977,182.36	0.999885	35	65	1031
Mar 24	5.2986%	11,373,415,394.49	11,372,687,872.41	0.999936	36	68	1025
Feb 24	5.3035%	11,928,691,803.89	11,927,911,436.19	0.999934	36	69	1024
Jan 24	5.3200%	11,483,316,119.03	11,483,741,551.85	1.000037	42	77	1024
Dec 23	5.3378%	10,557,076,424.02	10,557,101,303.24	0.999972	44	85	1037
Nov 23	5.3307%	10,148,883,026.83	10,148,191,305.12	0.999931	33	74	1034
Oct 23	5.3231%	10,017,668,653.01	10,016,121,800.83	0.999845	29	69	1031
Sep 23	5.3105%	9,992,445,950.80	9,990,730,955.61	0.999816	29	56	1028

PORTFOLIO ASSET SUMMARY AS OF AUGUST 31, 2024

	BOOK VALUE	MARKET VALUE
Uninvested Balance	\$ 624.14	\$ 624.14
Accrual of Interest Income	9,378,491.11	9,378,491.11
Interest and Management Fees Payable	(51,221,473.27)	(51,221,473.27)
Payable for Investment Purchased	0.00	0.00
Repurchase Agreement	6,520,570,999.95	6,520,570,999.95
Government Securities	4,481,858,501.72	4,484,442,224.12
TOTAL	\$ 10,960,587,143.65	\$ 10,963,170,866.05

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 2024

DATE	MNY MKT FUND EQUIV. [SEC Std.]	DAILY ALLOCATION FACTOR	INVESTED BALANCE	MARKET VALUE PER SHARE	WAM DAYS (1)	WAL DAYS (2)
8/1/2024	5.3039%	0.000145311	\$11,675,336,269.42	1.000105	33	62
8/2/2024	5.2982%	0.000145156	\$11,652,947,836.76	1.000212	32	61
8/3/2024	5.2982%	0.000145156	\$11,652,947,836.76	1.000212	32	61
8/4/2024	5.2982%	0.000145156	\$11,652,947,836.76	1.000212	32	61
8/5/2024	5.2900%	0.000144932	\$11,656,993,626.30	1.000194	31	60
8/6/2024	5.2870%	0.000144848	\$11,372,782,217.43	1.000151	32	61
8/7/2024	5.2890%	0.000144903	\$11,492,767,503.66	1.000148	32	61
8/8/2024	5.2952%	0.000145073	\$11,371,794,661.58	1.000148	32	61
8/9/2024	5.2965%	0.000145110	\$11,439,355,622.92	1.000124	31	59
8/10/2024	5.2965%	0.000145110	\$11,439,355,622.92	1.000124	31	59
8/11/2024	5.2965%	0.000145110	\$11,439,355,622.92	1.000124	31	59
8/12/2024	5.2977%	0.000145142	\$11,402,524,667.30	1.000142	30	59
8/13/2024	5.3037%	0.000145306	\$11,317,521,885.57	1.000167	31	59
8/14/2024	5.2926%	0.000145004	\$11,154,709,810.32	1.000154	32	61
8/15/2024	5.2994%	0.000145189	\$11,420,195,459.97	1.000113	32	60
8/16/2024	5.2913%	0.000144968	\$11,114,576,371.70	1.000116	32	61
8/17/2024	5.2913%	0.000144968	\$11,114,576,371.70	1.000116	32	61
8/18/2024	5.2913%	0.000144968	\$11,114,576,371.70	1.000116	32	61
8/19/2024	5.2874%	0.000144861	\$11,042,244,013.06	1.000145	32	61
8/20/2024	5.2877%	0.000144869	\$11,154,465,045.15	1.000165	32	61
8/21/2024	5.2841%	0.000144770	\$11,134,735,756.91	1.000198	32	61
8/22/2024	5.2813%	0.000144692	\$11,009,583,578.99	1.000164	32	62
8/23/2024	5.2898%	0.000144925	\$11,100,289,377.03	1.000169	31	60
8/24/2024	5.2898%	0.000144925	\$11,100,289,377.03	1.000169	31	60
8/25/2024	5.2898%	0.000144925	\$11,100,289,377.03	1.000169	31	60
8/26/2024	5.2935%	0.000145027	\$11,052,519,121.39	1.000164	30	60
8/27/2024	5.3021%	0.000145262	\$11,006,122,576.96	1.000189	30	60
8/28/2024	5.3028%	0.000145281	\$11,137,867,928.52	1.000187	30	65
8/29/2024	5.2970%	0.000145122	\$11,073,637,808.79	1.000178	29	65
8/30/2024	5.2945%	0.000145055	\$10,960,587,143.65	1.000150	29	65
8/31/2024	5.2945%	0.000145055	\$10,960,587,143.65	1.000150	29	65
Average	5.2939%	0.000145038	\$11,268,338,188.51		31	61



ECONOMIC COMMENTARY (cont.)

Meanwhile, the July CPI report provided more evidence that inflation is on a sustainable path lower. Headline inflation rose 0.2% month-over-month (m/m) and 2.9% year-over-year (y/y), its slowest pace since March 2021, while core inflation rose 0.2% m/m and 3.2% y/y. Both measures were roughly in line with expectations. In the details, core goods prices fell 0.3% due to lower apparel and vehicle prices, marking the category's fifth straight monthly decline. Shelter inflation remained elevated, although the 0.4% m/m rise in owners' equivalent rent was its second slowest increase since late 2021. Headline and core PCE inflation came in as expected, rising 2.5% and 2.6% y/y, respectively. While some of the services components looked more mixed, the lack of troubling details in this report keeps the Fed on track to begin cutting rates. At the same time, the economy continued to grow at a healthy pace. Second-quarter GDP growth was revised up to a 3.0% seasonally adjusted annualized rate, bringing the average GDP growth from the first half of the year to a solid 2.2%, in line with trend growth. Consumer spending rose by an upward revised 2.9% due to a bounce back in spending on goods. Consumers remained resilient in July as retail sales came in much stronger than expected, showing a 1% headline increase for the month.

The July Federal Open Market Committee (FOMC) meeting minutes reflected increased confidence in inflation while noting increasing downside risks in the labor market, resulting in stronger consideration for potential rate cuts. At the annual Economic Policy Symposium in Jackson Hole, Wyoming, Fed Chairman Powell's remarks reaffirmed the dovish tone and signaled that a rate cut is imminent, stating, "The time has come for policy to adjust." However, he did not specify how large the cut would be, indicating that the timing and size would depend on incoming data, the evolving economic outlook, and the balance of risks. Expressing growing confidence that inflation is on a sustainable path back to 2%, he highlighted the Fed's focus on labor market conditions, noting that while the current state of the labor market is not worrisome, the Fed does not welcome further cooling. The softer than expected inflation and labor market data, coupled with the Fed suggesting imminent rate cuts, caused Treasury yields to drop across the curve. Three- and six-month Treasury bill yields fell by 17 basis points (bps) and 23 bps to 5.12% and 4.86%, respectively. Longer-term Treasury yields fell even further, with one- and two-year Treasury yields declining 34 bps to 4.41% and 3.92%, respectively.

Outlook

It has become clear that inflation is no longer the primary risk on the Fed's radar. July core PCE inflation has remained low, with the annualized 3-month run rate now below target at 1.72%, which supports the Fed's focus on the labor market and allows it to respond confidently to any further weakening. Despite strong income and spending data, there is no immediate pressure for the Fed to make larger rate cuts.

"The time has come" was a memorable phrase from Chair Powell's speech at the Jackson Hole Symposium. Federal Reserve rate cuts are imminent, with the discussion now shifting to how quickly rates will come down. In our view, the Fed will likely cut three times this year, to maintain a balanced economy, with 25-basis point rate cuts at the September, November and December meetings. The market is anticipating a 45% probability of a 50-basis point rate cut in September. The size of the first cut will likely depend on the August payroll report due out soon.

This information is an excerpt from an economic report dated August 2024 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
David Medanich	Hilltop Securities	Governing Board Secretary
Andrew Linton	J.P. Morgan Asset Management	Governing Board Asst. Sec./Treas
Brett Starr	City of Irving	Advisory Board
Sandra Newby	Qualified 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 August change at any time based on market or other conditions and August 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

September 25, 2024 AGENDA ITEM #5

Discuss and consider approving
an amendment to the FY 2025
Capital Budget to fund the
replacement of the 45SW toll
system

Strategic Plan Relevance:	Innovation, Stewardship
Department:	Information Technology
Contact:	Greg Mack, Director of IT and Toll Systems
Associated Costs:	\$1,450,000
Funding Source:	FY25 Capital Budget
Action Requested:	Consider and act on draft resolution

Background: The Fiscal Year 2025 Annual Operating Budget contains revenue estimates, departmental spending plans, debt service requirements, and a capital budget for the fiscal year beginning July 1, 2024, ending June 30, 2025. The capital budget consists of new acquisition and renewal and replacement items for the System and the MoPac North managed lanes (ML). The Authority's five-year capital plan includes projects ranked by priority that are contemplated for future funding and implementation consideration.

A major renewal and replacement initiative of the Authority is the retrofit of the electronic toll collection roadside system on each toll road. These systems collect the roadside transactions and transmit them to the data platform for revenue collection processing. The toll collection systems on the 71E and 290E Authority roadways have been replaced. The FY25 capital budget has allocated renewal and replacement funding for the toll collection system retrofit on MoPac N managed lanes and to commence the same for the 183A corridor toll roads. The toll collection systems on all the Authority's roadways will be replaced as the current systems will reach the end of their useful life soon. Those not approved and funded in the current or prior fiscal year capital budget are included in the five-year capital plan as Priority 1 projects, including the 45SW toll collection system currently programmed for funding and implementation in FY27.

Current Action: The schedule for the toll system integrator performing the work will accommodate moving up the replacement of the toll collection system from FY27 to the current fiscal year. Funding the 45SW toll collection system retrofit will require \$1,450,000 from the System General Fund, which is available for the project. The 45SW toll collection system retrofit addition to the FY25 capital budget is outlined in the attached Draft Capital Budget amendment.

Staff Recommendation: Staff requests the Board's approval to amend the Fiscal Year 2025 Capital Budget to add the 45SW toll collection system replacement of \$1,450,000 with funding to be provided from the System General Fund.

Backup provided: Draft resolution

Draft Capital Budget amendment

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

RESOLUTION NO. 24-0XX

**AMENDING THE CAPITAL BUDGET FOR FISCAL YEAR 2025 TO FUND THE
REPLACEMENT OF THE 45SW ELECTRONIC TOLL COLLECTION SYSTEM**

WHEREAS, the Central Texas Regional Mobility Authority (the “Mobility Authority”) was created pursuant to the request of Travis and Williamson Counties and in accordance with provisions of the Transportation Code and the petition and approval process established in 43 Tex. Admin. Code § 26.01, *et. seq.* (the “RMA Rules”); and

WHEREAS, the prudent management and fiscal oversight are overriding objectives of the Mobility Authority Board of Directors; and

WHEREAS, by Resolution No. 24-031, dated June 26, 2024, the Board of Directors adopted the operating budget for fiscal year 2024-2025 (the “FY 2025 Budget”); and

WHEREAS, the FY 2025 Budget includes \$6,901,000 in funding for the renewal and replacement of the electronic toll collection system on each toll road identified in the FY 2025 Budget; and

WHEREAS, the FY 2024-2029 Five-Year Capital Plan includes the replacement of the electronic toll collection system of the 45SW Toll in FY 2027; and

WHEREAS, the schedule for the toll system integrator performing the work will accommodate moving up the replacement of the toll collection system of the 45SW Toll from FY 2027 to the current fiscal year; and

WHEREAS, staff proposes amending the Renewal & Replacement section of the FY 2025 Budget to provide for an additional amount of \$1,450,000 to fund the replacement of the electronic toll collection system of the 45SW Toll; and

WHEREAS, the requested amount of \$1,450,000 will be funded by the General Fund; and

WHEREAS, the Executive Director recommends that the FY 2025 Budget be amended as described in Exhibit A attached hereto, to fund the replacement of the electronic toll collection system of the 45SW Toll.

NOW THEREFORE, BE IT RESOLVED that the Board of Directors hereby amends the FY 2025 Budget as shown in Exhibit A attached hereto, to fund the replacement of the electronic toll collection system of the 45SW Toll.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of September 2024.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

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

Exhibit A

Exhibit A

Capital Budget

	FY 2025 Adopted	FY 2025 Amended
Capital Budget		
CTRMA App - Requirements Gathering and Procurement	190,000	
TIM Center Video Wall Technology	1,015,000	
TIM Center Furniture, Fixtures, and Equipment (FFE)	574,000	
CTRMA Co-location Buildout	75,000	
TIM Center Building Improvements	300,000	
DPS Enhancements	350,000	
CCTV Camera Replacements (Systemwide)	275,000	
Roadside Hardening	633,000	
Maintenance Yard Improvement Support & Additional Site Investigations - 183A	250,000	
Maintenance Yard Site Acquisition (ROW Purchase) - 183A	4,400,000	
Maintenance Equipment	35,000	
Maintenance Yard Expansion and Brine Production Facilities - 290E	400,000	
UTV and Trailer for Maintenance	35,000	
Maintenance Vehicle with Attachments - 1	125,000	
IT Buildout of new CTRMA building	60,000	
Fiber Connection to new CTRMA building	498,000	
Generator for new CTRMA building	100,000	
Total Capital Budget	9,315,000	
Renewal and Replacement		
General Fund		
Toll System Replacement - 45SW	-	1,450,000
Toll System Replacement - 183A	1,000,000	
Slab Stabilization - 183S	103,000	
Slab Stabilization - 290E	250,000	
Pond Repair - 183A	848,000	
Scottsdale Wall Investigation - 183A	200,000	
Metal Beam Guard Fence Upgrade - 290E	1,600,000	
Parmer Lane Wall Repairs - 290E	1,400,000	
Annual Safety Improvements - Systemwide	1,500,000	
Total General Fund	6,904,000	8,351,000
MoPac General		
Roadway Traveler Communications - Single Line DMS - MoPac MNLN	1,700,000	
Delineation Replacement - MoPac MNLN	590,000	
Total MoPac General Fund	2,290,000	
Total Renewal and Replacement	9,194,000	10,641,000
Total all Projects	18,506,000	18,506,000



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024 AGENDA ITEM #6

Discuss and consider approving an amendment to the FY 2025 Capital Budget to fund the replacement of automatic license plate readers to support the Habitual Violator Program

Strategic Plan Relevance:	Innovation, Stewardship
Department:	Information Technology
Contact:	Cory Bluhm, Assistant Director of Toll & IT Systems
Associated Costs:	\$375,000
Funding Source:	FY25 Capital Budget
Action Requested:	Consider and act on draft resolution

Background: The Fiscal Year 2025 Annual Operating Budget contains revenue estimates, departmental spending plans, debt service requirements, and a capital budget for the fiscal year beginning July 1, 2024, ending June 30, 2025. The capital budget consists of new acquisition and renewal and replacement items for the System and the MoPac North managed lanes (ML). The Mobility Authority's five-year capital plan includes projects ranked by priority that are contemplated for future funding and implementation consideration.

Roadside toll violator enforcement using automatic license plate reader (ALPR) technology is a significant initiative to mitigate revenue loss and enhance collections. This technology identifies violators on the roadways and notifies peace officers patrolling the roadway so that enforcement action can be taken. This method has been effective in promoting enforcement, and the acquisition of replacement equipment sooner than initially planned will continue the Mobility Authority's efforts to ensure toll road users are paying their tolls.

Current Action: The FY2024-2029 Five-Year Capital Plan includes the purchase of replacement and new ALPR technology in fiscal years 2026 and 2027 in the aggregate amount of \$375,000. To ensure continued enforcement efforts, the request is to move up the purchase of ALPR technology to the approved FY25 Capital Budget. The purchase will replace cameras at the Park Street main lanes and add new cameras to the Crystal

Falls main lanes. The specific item is referenced in the attached Draft Capital Budget Amendment.

Staff Recommendation: Staff requests the Board's approval to amend the Fiscal Year 2025 Capital Budget to approve the acquisition of automated license plate readers in the amount of \$375,000 from the General Fund.

Backup provided: Draft resolution
Draft Capital Budget amendment

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

RESOLUTION NO. 24-0XX

**AMENDING THE CAPITAL BUDGET FOR FISCAL YEAR 2025 TO FUND THE
REPLACEMENT OF AUTOMATIC LICENSE PLATE READER TECHNOLOGY FOR
THE MOBILITY AUTHORITY'S HABITUAL VIOLATOR ENFORCEMENT
PROGRAM**

WHEREAS, the Central Texas Regional Mobility Authority (the "Mobility Authority") was created pursuant to the request of Travis and Williamson Counties and in accordance with provisions of the Transportation Code and the petition and approval process established in 43 Tex. Admin. Code § 26.01, *et. seq.* (the "RMA Rules"); and

WHEREAS, the prudent management and fiscal oversight are overriding objectives of the Mobility Authority Board of Directors; and

WHEREAS, by Resolution No. 24-031, dated June 26, 2024, the Board of Directors adopted the operating budget for fiscal year 2024-2025 (the "FY 2025 Budget"); and

WHEREAS, roadside toll violator enforcement using automatic license plate reader ("ALPR") technology is a significant initiative to mitigate revenue loss and enhance collections; and

WHEREAS, the FY 2024-2029 Five-Year Capital Plan includes the purchase of replacement of ALPR technology in FY 2026 and FY 2027; and

WHEREAS, the replacement of ALPR technology is needed prior to FY 2026 to ensure continued enforcement efforts for the Mobility Authority's Habitual Violator Enforcement Program; and

WHEREAS, staff proposes amending the Capital Budget section of the FY 2025 Budget to provide for an additional amount of \$375,000 to purchase replacement of ALPR technology for the Mobility Authority's Habitual Violator Enforcement Program; and

WHEREAS, the requested amount of \$375,000 will be funded by the General Fund; and

WHEREAS, the Executive Director recommends that the FY 2025 Budget be amended as described in Exhibit A attached hereto, to fund the replacement of ALPR technology for the Mobility Authority's Habitual Violator Enforcement Program.

NOW THEREFORE, BE IT RESOLVED that the Board of Directors hereby amends the FY 2025 Budget as shown in Exhibit A attached hereto, to fund the replacement of ALPR technology for the Mobility Authority's Habitual Violator Enforcement Program.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of September 2024.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

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

Exhibit A



Capital Budget

	FY 2025 Adopted	FY 2025 Amended
Capital Budget		
Automated License Plate Reader (ALPR)	-	375,000
CTRMA App - Requirements Gathering and Procurement	190,000	
TIM Center Video Wall Technology	1,015,000	
TIM Center Furniture, Fixtures, and Equipment (FFE)	574,000	
CTRMA Co-location Buildout	75,000	
TIM Center Building Improvements	300,000	
DPS Enhancements	350,000	
CCTV Camera Replacements (Systemwide)	275,000	
Roadside Hardening	633,000	
Maintenance Yard Improvement Support & Additional Site Investigations - 183A	250,000	
Maintenance Yard Site Acquisition (ROW Purchase) - 183A	4,400,000	
Maintenance Equipment	35,000	
Maintenance Yard Expansion and Brine Production Facilities - 290E	400,000	
UTV and Trailer for Maintenance	35,000	
Maintenance Vehicle with Attachments - 1	125,000	
IT Buildout of new CTRMA building	60,000	
Fiber Connection to new CTRMA building	498,000	
Generator for new CTRMA building	100,000	
Total Capital Budget	9,315,000	9,690,000
Renewal and Replacement		
General Fund		
Toll System Replacement - 183A	1,000,000	
Slab Stabilization - 183S	103,000	
Slab Stabilization - 290E	250,000	
Pond Repair - 183A	848,000	
Scottsdale Wall Investigation - 183A	200,000	
Metal Beam Guard Fence Upgrade - 290E	1,600,000	
Parmer Lane Wall Repairs - 290E	1,400,000	
Annual Safety Improvements - Systemwide	1,500,000	
Total General Fund	6,901,000	
MoPac General		
Roadway Traveler Communications - Single Line DMS - MoPac MNLN	1,700,000	
Delineation Replacement - MoPac MNLN	590,000	
Total MoPac General Fund	2,290,000	
Total Renewal and Replacement	9,191,000	
Total all Projects	18,506,000	18,881,000



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024 AGENDA ITEM #7

Discuss and consider approving
an amendment to the FY 2025
Capital Budget to fund the
replacement of delineators on
the MoPac Express Lane

Strategic Plan Relevance:	Safety, Stewardship
Department:	Engineering
Contact:	Mike Sexton, Director of Engineering
Associated Costs:	\$593,700 (additional \$3,700 to capital budget)
Funding Source:	FY25 Capital Budget
Action Requested:	Consider and act on draft resolution

Background: The Fiscal Year 2025 Annual Operating Budget contains revenue estimates, departmental spending plans, debt service requirements, and a capital budget for the fiscal year beginning July 1, 2024, ending June 30, 2025. The capital budget consists of new acquisition and renewal and replacement items for the System and the MoPac North managed lanes (ML).

The renewal and replacement fund capital budget included the replacement of delineators for the entire MoPac N ML corridor. The delineators serve as a safety measure to segregate ML traffic from vehicles in the MoPac general purpose lanes. Throughout the year, individual delineators are replaced by the Authority's roadway maintenance as needed. Periodically delineators in the entire corridor warrant replacement, which was the case for requesting in the current fiscal year capital budget.

Current Action: The approved FY25 Capital Budget anticipated the costs of the MoPac N ML delineators to be \$590,000. Staff has now determined that the delineator replacement will cost \$593,663.91. This request is to amend and increase the capital budget for the MoPac N ML delineators by \$3,700 to \$593,700. The specific item is outlined on page 42 of the FY25 Budget and in the Draft Capital Budget Amendment, both of which are attached.

Staff Recommendation: Staff requests the Board's approval to amend the Fiscal Year 2025 Capital Budget to provide an additional \$3,700 of funding from the MoPac General Fund for the MoPac N ML delineator replacement project.

Backup provided: Draft resolution

Draft Capital Budget amendment

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

RESOLUTION NO. 24-0XX

**AMENDING THE CAPITAL BUDGET FOR FISCAL YEAR 2025 TO FUND THE
REPLACEMENT OF DELINEATORS ON THE MOPAC EXPRESS LANES**

WHEREAS, the Central Texas Regional Mobility Authority (the “Mobility Authority”) was created pursuant to the request of Travis and Williamson Counties and in accordance with provisions of the Transportation Code and the petition and approval process established in 43 Tex. Admin. Code § 26.01, *et. seq.* (the “RMA Rules”); and

WHEREAS, the prudent management and fiscal oversight are overriding objectives of the Mobility Authority Board of Directors; and

WHEREAS, by Resolution No. 24-031, dated June 26, 2024, the Board of Directors adopted the operating budget for fiscal year 2024-2025 (the “FY 2025 Budget”); and

WHEREAS, the FY 2025 Budget includes \$590,000 in funding for renewal and replacement initiatives, including the replacement of delineators on the MoPac Express Lanes; and

WHEREAS, staff has determined that the cost to replace the delineators on the MoPac Express Lanes will be \$593,663.91; and

WHEREAS, staff proposes amending the Renewal & Replacement section of the FY 2025 Budget to provide for an additional amount of \$3,700 to fund the replacement of delineators on the MoPac Express Lanes; and

WHEREAS, the requested amount of \$3,700 will be funded by the General Fund; and

WHEREAS, the Executive Director recommends that the FY 2025 Budget be amended as described in Exhibit A attached hereto, to fund the replacement of delineators on the MoPac Express Lanes.

NOW THEREFORE, BE IT RESOLVED that the Board of Directors hereby amends the FY 2025 Budget as shown in Exhibit A attached hereto, to fund the replacement of delineators on the MoPac Express Lanes.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of September 2024.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

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

Exhibit A

Capital Budget

Capital Budget

CTRMA App - Requirements Gathering and Procurement	190,000
TIM Center Video Wall Technology	1,015,000
TIM Center Furniture, Fixtures, and Equipment (FFE)	574,000
CTRMA Co-location Buildout	75,000
TIM Center Building Improvements	300,000
DPS Enhancements	350,000
CCTV Camera Replacements (Systemwide)	275,000
Roadside Hardening	633,000
Maintenance Yard Improvement Support & Additional Site Investigations - 183A	250,000
Maintenance Yard Site Acquisition (ROW Purchase) - 183A	4,400,000
Maintenance Equipment	35,000
Maintenance Yard Expansion and Brine Production Facilities - 290E	400,000
UTV and Trailer for Maintenance	35,000
Maintenance Vehicle with Attachments - 1	125,000
IT Buildout of new CTRMA building	60,000
Fiber Connection to new CTRMA building	498,000
Generator for new CTRMA building	100,000
Total Capital Budget	<u>9,315,000</u>

Renewal and Replacement

General Fund

Toll System Replacement - 183A	1,000,000
Slab Stabilization - 183S	103,000
Slab Stabilization - 290E	250,000
Pond Repair - 183A	848,000
Scottsdale Wall Investigation - 183A	200,000
Metal Beam Guard Fence Upgrade - 290E	1,600,000
Parmer Lane Wall Repairs - 290E	1,400,000
Annual Safety Improvements - Systemwide	1,500,000
Total General Fund	<u>6,901,000</u>

MoPac General

Roadway Traveler Communications - Single Line DMS - MoPac MNLN	1,700,000
Delineation Replacement - MoPac MNLN	590,000
Total MoPac General Fund	<u>2,290,000</u>

Total Renewal and Replacement 9,191,000

Total all Projects 18,506,000

Capital Budget

	FY 2025 Adopted	FY 2025 Amended
Capital Budget		
CTRMA App - Requirements Gathering and Procurement	190,000	
TIM Center Video Wall Technology	1,015,000	
TIM Center Furniture, Fixtures, and Equipment (FFE)	574,000	
CTRMA Co-location Buildout	75,000	
TIM Center Building Improvements	300,000	
DPS Enhancements	350,000	
CCTV Camera Replacements (Systemwide)	275,000	
Roadside Hardening	633,000	
Maintenance Yard Improvement Support & Additional Site Investigations - 183A	250,000	
Maintenance Yard Site Acquisition (ROW Purchase) - 183A	4,400,000	
Maintenance Equipment	35,000	
Maintenance Yard Expansion and Brine Production Facilities - 290E	400,000	
UTV and Trailer for Maintenance	35,000	
Maintenance Vehicle with Attachments - 1	125,000	
IT Buildout of new CTRMA building	60,000	
Fiber Connection to new CTRMA building	498,000	
Generator for new CTRMA building	100,000	
Total Capital Budget	9,315,000	
Renewal and Replacement		
General Fund		
Toll System Replacement - 183A	1,000,000	
Slab Stabilization - 183S	103,000	
Slab Stabilization - 290E	250,000	
Pond Repair - 183A	848,000	
Scottsdale Wall Investigation - 183A	200,000	
Metal Beam Guard Fence Upgrade - 290E	1,600,000	
Parmer Lane Wall Repairs - 290E	1,400,000	
Annual Safety Improvements - Systemwide	1,500,000	
Total General Fund	6,901,000	
MoPac General		
Roadway Traveler Communications - Single Line DMS - MoPac MNLN	1,700,000	
Delineation Replacement - MoPac MNLN	590,000	593,700
Total MoPac General Fund	2,290,000	2,293,700
Total Renewal and Replacement	9,191,000	9,194,700
Total all Projects	18,506,000	18,509,700



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024 AGENDA ITEM #8

Discuss and consider approving an amendment to the FY 2025 Operating Budget to fund TollTag™ marketing efforts in the Central Texas region to improve pre-paid account penetration

Strategic Plan Relevance:	Innovation, Service, Stewardship
Department:	Communications
Contact:	Jori Liu, Director of Communications
Associated Costs:	\$225,000 increase to the FY25 Operating Budget
Funding Source:	FY25 Operating Budget Revenues
Action Requested:	Consider and act on draft resolution

Background: The Fiscal Year 2025 Annual Operating Budget contains revenue estimates and departmental spending plans for the fiscal year beginning July 1, 2024, ending June 30, 2025. The estimated revenues of \$302.5 million include Operating Revenue of \$258.8 million and Other Revenue of \$43.7 million. Total estimated operating expenses are \$119.7 million and \$71.8 million of bond and loan debt service. In addition to the department-level budget estimates, the FY25 Budget includes the Authority's Capital Budget, System Operating Budget, and Debt Service Schedule for FY25.

One of the major initiatives anticipated in the FY25 Operating Budget is to increase pre-paid account penetration. Pre-paid electronic toll collection is the most efficient way to facilitate payment for travel on tolled facilities. Pre-paid electronic toll collection methods include transponders (more commonly known as "tags") and license plate-based accounts. The Mobility Authority benefits from pre-paid electronic toll collection through more efficient transaction processing which results in faster revenue realization. The lower costs to collect and mitigation of toll violations aid the Authority's credit rating which translates to lower borrowing costs.

The Mobility Authority experienced a sharp decline in prepaid account usage in 2020 while the number of Pay By Mail invoices issued each month increased. Pay By Mail represents a revenue collection risk. To mitigate this risk, a substantial increase in the number of customers using pre-paid electronic toll payment methods is necessary.

Current Action: The approved FY25 Operating Budget includes funding to promote the use of electronic toll tags as a payment method on Authority-operated toll facilities. This “tagnostic” approach stresses that there are many different tag payment options available to the Mobility Authority’s customers that will save them money and time. These tag options include Cameron County’s Fuego tag; Colorado’s ExpressToll tag; Florida’s SunPass; Harris County’s EZTAG; Kansas’s KTAG; NTTA’s TollTag; Oklahoma’s PikePass; and TxDOT’s TxTag.

A new partnership with the North Texas Tollway Authority (NTTA) allows the Authority to market and distribute TollTag products in the Central Texas area. Funding is needed to support specific TollTag marketing activities during the fall 2024 / winter 2025 season related to this initiative. Examples of these activities are:

- In-game and game adjacent sponsorships
- Audio (podcasts and over-the air radio)
- In-game sports Programming (college)
- Non-sports programming (local news programming and Connected TV)
- Outdoor (billboards)

Costs for these activities are dependent on timing, spot availability, and the size of the media buy. Therefore, it is difficult to estimate an exact amount until these factors are known. In addition to the cost of the specific marketing activities, there is a 15% ad agency placement fee. Staff requests a budget amendment of \$225,000 to offset these costs and support this important and critical initiative.

The Communications and Public Relations component of the FY25 Communications Department operating budget for these programs is \$2,195,000.

The proposed budget amendment would increase the funding for the Communications and Public Relations programs to \$2,420,000.

Note that the proposed amendments to the FY25 Operating Budget will increase the overall adopted FY25 Operating Budget amount.

Staff Recommendation: Staff requests the Board's approval to amend the Fiscal Year 2025 Operating Budget to fund marketing activities related to the TollTag pre-paid account initiative.

Backup provided: Draft resolution
Draft Operating Budget amendment
TollTag marketing plan

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

RESOLUTION NO. 24-0XX

**AMENDING THE OPERATING BUDGET FOR FISCAL YEAR 2025 TO FUND
TOLLTAG™ MARKETING EFFORTS IN THE CENTRAL TEXAS REGION TO
IMPROVE PRE-PAID ACCOUNT PENETRATION**

WHEREAS, the Central Texas Regional Mobility Authority (the “Mobility Authority”) was created pursuant to the request of Travis and Williamson Counties and in accordance with provisions of the Transportation Code and the petition and approval process established in 43 Tex. Admin. Code § 26.01, *et. seq.* (the “RMA Rules”); and

WHEREAS, the prudent management and fiscal oversight are overriding objectives of the Mobility Authority Board of Directors; and

WHEREAS, by Resolution No. 24-031, dated June 26, 2024, the Board of Directors adopted the operating budget for fiscal year 2024-2025 (the “FY 2025 Budget”); and

WHEREAS, a crucial goal of the Mobility Authority is to increase the pre-paid account penetration in the Central Texas region; and

WHEREAS, by Resolution No. 24-049, dated August 29, 2024, the Board of Directors approved an interlocal agreement with the North Texas Tollway Authority (NTTA) to market and distribute TollTag products in the Central Texas region to increase pre-paid account penetration; and

WHEREAS, staff proposes amending the Communications and Public Relations section of the FY 2025 Budget to provide for an additional amount of \$225,000 to fund the marketing and distribution of TollTag products in the Central Texas region to increase pre-paid account penetration; and

WHEREAS, the requested amount of \$225,000 will be funded by Operating Revenue; and

WHEREAS, the Executive Director recommends that the FY 2025 Budget be amended as described in Exhibit A attached hereto, to fund the marketing and distribution of TollTag products in the Central Texas region to increase pre-paid account penetration.

NOW THEREFORE, BE IT RESOLVED that the Board of Directors hereby amends the FY 2025 Budget as shown in Exhibit A attached hereto, to fund the marketing and distribution of TollTag products in the Central Texas region to increase pre-paid account penetration.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of September 2024.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

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

Exhibit A

Communications

Central Texas Regional Mobility Authority

Operating Budget - FY 2025

Communications

Account Name	FY 2022 Actual Results	FY 2023 Actual Results	FY 2024 Adopted Budget	FY 2025 Adopted Budget	% Change From Prior Year
Salaries and Benefits					
Salaries & Wages					
Salary Expense-Regular	339,724	365,175	450,090	432,539	-3.9%
Total Salaries	339,724	365,175	450,090	432,539	-3.9%
Benefits					
TCDRS	52,044	66,136	81,016	77,857	-3.9%
FICA	19,674	21,752	26,842	25,242	-6.0%
FICA MED	4,686	5,227	6,526	6,272	-3.9%
Health Insurance Expense	52,103	54,619	60,429	61,441	1.7%
Life Insurance Expense	555	438	545	300	-44.9%
Other Benefits	1,266	1,440	13,502	12,976	-3.9%
Total Benefits	130,328	149,614	188,861	184,088	-2.5%
Payroll Taxes					
Unemployment Taxes	334	-149	540	540	0.0%
Total Payroll Taxes	334	-149	540	540	0.0%
Total Salaries and Benefits	470,385	514,640	639,491	617,167	-3.5%
Administrative					
Administrative and Office Expenses					
Internet	0	0	150	0	-100.0%
Cell Phones	1,000	650	1,800	1,800	0.0%
Meeting Expense	0	542	2,000	2,000	0.0%
Parking / Local Ride Share	0	25	1,000	1,000	0.0%
Mileage Reimbursement	0	120	500	500	0.0%
Total Administrative and Office Expenses	1,000	1,337	5,450	5,300	-2.8%
Office Supplies					
Office Supplies	0	0	250	250	0.0%
Computer Supplies	0	0	500	500	0.0%
Other Reports-Printing	0	0	1,500	500	-66.7%
Office Supplies-Printed	0	250	1,000	500	-50.0%
Postage Expense	0	0	0	250	
Total Office Supplies	0	250	3,250	2,000	-38.5%
Communications and Public Relations					
Graphic Design Services	0	0	75,000	75,000	0.0%
Website Maintenance	203	38,557	375,000	150,000	-60.0%
Research Services	0	3,600	25,000	75,000	200.0%
Communications and Marketing	16,527	41,743	400,000	500,000	25.0%
Advertising Expense	324,813	474,322	500,000	1,000,000	100.0%
Direct Mail	0	0	20,000	25,000	25.0%
Video Production	7,706	29,097	150,000	250,000	66.7%
Photography	424	14,090	25,000	25,000	0.0%
Radio	0	0	50,000	50,000	0.0%
Other Public Relations	0	0	2,500	0	-100.0%
Promotional Items	6,491	14,694	20,000	20,000	0.0%
Annual Report printing	0	0	500	0	-100.0%
Direct Mail Printing	0	0	10,000	10,000	0.0%
Other Communication Expenses	14,849	-30	15,000	15,000	0.0%
Total Communications and Public Relations	371,013	616,074	1,668,000	2,195,000	31.6%

Communications

Central Texas Regional Mobility Authority

Operating Budget - FY 2025

Communications

Account Name	FY 2022 Actual Results	FY 2023 Actual Results	FY 2024 Adopted Budget	FY 2025 Adopted Budget	% Change From Prior Year
Employee Development					
Subscriptions	0	540	250	1,000	300.0%
Agency Memberships	0	0	5,000	5,000	0.0%
Professional Development	0	0	2,500	2,500	0.0%
Seminars and Conferences	0	3,025	7,500	7,500	0.0%
Travel	0	0	7,500	7,500	0.0%
Total Employee Development	0	3,565	22,750	23,500	3.3%
Total Administrative	372,013	621,226	1,699,450	2,225,800	31.0%
Operations and Maintenance					
Operations and Maintenance Consulting					
General Engineering Consultant					
GEC-Public Information Support					
GEC 6.2 Public Information - Non Project	179,929	171,725	200,000	200,000	0.0%
Total Operations and Maintenance Consulting	179,929	171,725	200,000	200,000	0.0%
Total Operations and Maintenance	179,929	171,725	200,000	200,000	0.0%
Total Expenses	1,022,328	1,307,591	2,538,941	3,042,967	19.9%



Communications

Central Texas Regional Mobility Authority

Operating Budget - FY 2025

Communications

Account Name	FY 2024 Adopted Budget	FY 2025 Adopted Budget	FY 2025 Initiative for Addl Funding	FY 2025 Proposed Amended Budget	% Change From FY 2024 As Amended
Salaries and Benefits					
Salaries & Wages					
Salary Expense-Regular	450,090	432,539		432,539	-3.9%
Total Salaries	450,090	432,539		432,539	-3.9%
Benefits					
TCDRS	81,016	77,857		77,857	-3.9%
FICA	26,842	25,242		25,242	-6.0%
FICA MED	6,526	6,272		6,272	-3.9%
Health Insurance Expense	60,429	61,441		61,441	1.7%
Life Insurance Expense	545	300		300	-44.9%
Other Benefits	13,502	12,976		12,976	-3.9%
Total Benefits	188,861	184,088		184,088	-2.5%
Payroll Taxes					
Unemployment Taxes	540	540		540	0.0%
Total Payroll Taxes	540	540		540	0.0%
Total Salaries and Benefits	639,491	617,167		617,167	-3.5%
Administrative					
Administrative and Office Expenses					
Internet	150	0		0	-100.0%
Cell Phones	1,800	1,800		1,800	0.0%
Meeting Expense	2,000	2,000		2,000	0.0%
Parking / Local Ride Share	1,000	1,000		1,000	0.0%
Mileage Reimbursement	500	500		500	0.0%
Total Administrative and Office Expenses	5,450	5,300		5,300	-2.8%
Office Supplies					
Office Supplies	250	250		250	0.0%
Computer Supplies	500	500		500	0.0%
Other Reports-Printing	1,500	500		500	-66.7%
Office Supplies-Printed	1,000	500		500	-50.0%
Postage Expense	0	250		250	
Total Office Supplies	3,250	2,000		2,000	-38.5%
Communications and Public Relations					
Graphic Design Services	75,000	75,000		75,000	0.0%
Website Maintenance	375,000	150,000		150,000	-60.0%
Research Services	25,000	75,000		75,000	200.0%
Communications and Marketing	400,000	500,000		500,000	25.0%
Advertising Expense	500,000	1,000,000	225,000	1,225,000	145.0%
Direct Mail	20,000	25,000		25,000	25.0%
Video Production	150,000	250,000		250,000	66.7%
Photography	25,000	25,000		25,000	0.0%
Radio	50,000	50,000		50,000	0.0%
Other Public Relations	2,500	0		0	-100.0%
Promotional Items	20,000	20,000		20,000	0.0%
Annual Report printing	500	0		0	-100.0%
Direct Mail Printing	10,000	10,000		10,000	0.0%
Other Communication Expenses	15,000	15,000		15,000	0.0%
Total Communications and Public Relations	1,668,000	2,195,000	225,000	2,420,000	45.1%

Communications

Central Texas Regional Mobility Authority

Operating Budget - FY 2025

Communications

Account Name	FY 2024 Adopted Budget	FY 2025 Adopted Budget	FY 2025 Initiative for Addl Funding	FY 2025 Proposed Amended Budget	% Change From FY 2024 As Amended
Employee Development					
Subscriptions	250	1,000		1,000	300.0%
Agency Memberships	5,000	5,000		5,000	0.0%
Professional Development	2,500	2,500		2,500	0.0%
Seminars and Conferences	7,500	7,500		7,500	0.0%
Travel	7,500	7,500		7,500	0.0%
Total Employee Development	22,750	23,500	0	23,500	3.3%
Total Administrative	1,699,450	2,225,800	225,000	2,450,800	44.2%
Operations and Maintenance					
Operations and Maintenance Consulting					
General Engineering Consultant					
GEC-Public Information Support					
GEC 6.2 Public Information - Non Project	200,000	200,000		200,000	0.0%
Total Operations and Maintenance Consulting	200,000	200,000	0	200,000	0.0%
Total Operations and Maintenance	200,000	200,000	0	200,000	0.0%
Total Expenses	2,538,941	3,042,967	225,000	3,267,967	28.7%



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024 AGENDA ITEM #9

Discuss and consider authorizing the Executive Director to approve work authorizations for the interlocal agreement with the North Texas Tollway Authority to support TollTag™ marketing, promotional services, and account enrollment

Strategic Plan Relevance:	Innovation, Service, Stewardship
Department:	Operations
Contact:	Tracie Brown, Director of Operations
Associated Costs:	Not to exceed \$175,000
Funding Source:	FY25 Operating Budget
Action Requested:	Consider and act on draft resolution

Background: Among its many charges, the operations Department is tasked with increasing pre-paid account penetration. Pre-paid electronic toll collection methods include transponders (more commonly known as “tags”) and license plate-based accounts. Pre-paid electronic toll collection is the most efficient way to facilitate payment for travel on tolled facilities. Pre-paid toll payment methods mitigate the revenue collection risk, allowing the Authority to operate current facilities and build new projects at a lower cost. The Interlocal Agreement between the Mobility Authority and the North Texas Tollway Authority (NTTA) provides the opportunity to market, promote, and distribute TollTag™ products in the Central Texas area.

Current Action: The Interlocal Agreement between CTRMA and NTTA contemplates work authorizations as the vehicle to progress work activity. This work includes:

- studio revisions for TollTag-related TV and radio ads;
- the purchase of TollTag™ inventory for distribution at special events;
- assistance at special events to facilitate in person TollTag™ enrollment;

- limited media consultation and strategic support from NTTA vendors; and
- updates to TollTag™ marketing collateral to align with the Austin demographic area.

The cost of the work effort is dependent upon the final work plans which are still under development. Therefore, staff requests that the Board authorize the Executive Director to approve work authorizations as they are developed. In a total amount not to exceed for these Work Authorizations is \$175,000.

Staff Recommendation: Staff recommends the Board authorize the Executive Director to approve Work Authorizations for the interlocal agreement with the North Texas Tollway Authority for TollTag™ marketing, promotional services, and account enrollment.

Previous Actions: In August 2024 the Board approved an interlocal agreement with the North Texas Tollway Authority (NTTA) for the marketing and distribution of TollTag™ products.

Backup provided: Draft resolution

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

RESOLUTION NO. 24-0XX

**AUTHORIZING THE EXECUTIVE DIRECTOR TO APPROVE WORK
AUTHORIZATIONS UNDER THE INTERLOCAL AGREEMENT WITH NORTH
TEXAS TOLLWAY AUTHORITY**

WHEREAS, the Central Texas Regional Mobility Authority (the “Mobility Authority”) was created pursuant to the request of Travis and Williamson Counties and in accordance with provisions of the Transportation Code and the petition and approval process established in 43 Tex. Admin. Code § 26.01, *et. seq.* (the “RMA Rules”); and

WHEREAS, the prudent management and fiscal oversight are overriding objectives of the Mobility Authority Board of Directors; and

WHEREAS, a crucial goal of the Mobility Authority is to increase the pre-paid account penetration in the Central Texas region; and

WHEREAS, by Resolution No, 24-049, dated August 29, 2024, the Board of Directors approved an interlocal agreement with the North Texas Tollway Authority (NTTA) to market and distribute TollTag products in the Central Texas region to increase pre-paid account penetration (the “Interlocal Agreement”); and

WHEREAS, the Interlocal Agreement contemplates the issuance of work authorizations to NTTA to progress work activity which will include the marketing, promotional services, and account enrollment of TollTag products in the Central Texas region; and

WHEREAS, the work plans for the work authorization are under development and the estimated cost of the work effort is a cumulative amount not to exceed \$175,000; and

WHEREAS, the staff recommends the Board of Directors authorize the Executive Director to approve work authorizations as the work plans are developed for the marketing, promotional services, and account enrollment of TollTag products in the Central Texas region for a cumulative amount not to exceed \$175,000.

NOW THEREFORE, BE IT RESOLVED that the Board of Directors hereby authorizes the Executive Director to issue work authorizations under the Interlocal Agreement for a cumulative amount not to exceed \$175,000.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of September 2024.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

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



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024 AGENDA ITEM #10

Discuss and consider approving an agreement with Deloitte Consulting LLP for enhancements to the Mobility Authority's Data Platform System

Strategic Plan Relevance:	Innovation
Department:	Operations
Contact:	Greg Mack, Director of IT and Toll Systems
Associated Costs:	Not to exceed \$1,500,000
Funding Source:	Capital Budget
Action Requested:	Consider and act on draft resolution

Project Description/Background: 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 provides 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 Quarterhill, the Mobility Authority's Lane vendors, collect the toll transaction at the roadside and forward the transaction and vehicle images to the DPS. Business logic then consumes the transaction and routes 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. The third project release was completed October 2023 on schedule. This release 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. The DPS went live in August 2023.

The Mobility Authority desires continued 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 continued 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 and subsequently extended to provide services through September 2023, when another contract was awarded to Deloitte to provide services through September 2024. The initial one-year contract for enhancement development was awarded to Deloitte in October 2023.

Financing: 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 7/25/24)
DIR Public Records Act Agreement – Deloitte Consulting TOMS Enhancements Statement of Work
DIR Vendor Agreement – Deloitte Consulting TOMS Enhancements Statement of Work

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

RESOLUTION NO. 24-0XX

**APPROVING AN AGREEMENT WITH DELOITTE CONSULTING LLP FOR
ENHANCEMENTS TO THE MOBILITY AUTHORITY’S DATA PLATFORM SYSTEM**

WHEREAS, the Mobility Authority hosts its own system for processing all toll transaction data and performing data management after the point of transaction creation (the “Data Platform System”); and

WHEREAS, t, the Mobility Authority desires to make certain enhancements to the Data Platform System from time to time that are determined to be beneficial for toll processing and data management; and

WHEREAS, the Executive Director has negotiated a scope of work with Deloitte Consulting LLP in an amount not to exceed \$1,500,000 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 \$1,500,000 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 \$1,500,000 through their cooperative contract with the Texas Department of Information Resources for 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 September 2024.

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)**

Enhancements for FY 2025

July 25, 2024

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	11
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 July 1, 2024, 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, 2026, 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 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 fifteen (15) business days from the receipt of the deliverable from the Vendor Project Manager.
 3. If CTRMA approver does not accept or reject the Deliverables and/or Services within fifteen (15) business days from the receipt of the deliverable 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 fifteen (15) 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 within fifteen (15) 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*

Name: *Jay Ashton*
 Title: *Data Platform & TOMS Manager*

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>	Jay Ashton, Data Platform & TOMS Manager	Three (3) business days
Second Level Contact	<i>Name, Title</i>	Greg Mack, Director of Information Technology	Three (3) business days
Third Level Contact	<i>Name, Title</i>	Tracie Brown, Director of Operations	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 fifteen (15) business days from the receipt of the CO form.
4. If the CTRMA approver does not approve or reject the requested Change Order within fifteen (15) 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.

IN WITNESS WHEREOF, the parties have caused this SOW to be executed as of the date signed by the CTRMA and written below.

DELOITTE CONSULTING LLP

CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY



Uday Katira, Managing Director
Deloitte Consulting LLP

James M. Bass
CTRMA Executive Director

08/11/2024

Date

Date

DIR Vendor Agreement

This is to signify that the Central Texas Regional Mobility Authority and Deloitte Consulting LLP Corporation have entered into a two-year Agreement **in an amount not to exceed \$1,500,000** pursuant to Texas Government Code Section 2054.0565 utilizing Texas Department of Information Resources Contract No. #DIR-CPO-4919 for deliverable-based information technology services described in this proposal. All terms and conditions of Texas Department of Information Resources Contract No. #DIR-CPO-4919 are applicable to and made part of this agreement.

DELOITTE CONSULTING LLP



Uday Katira, Managing Director
Deloitte Consulting LLP

08/04/2024

Date

**CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY**

James M. Bass
Executive Director

Date

Public Records Act Agreement

Contractor acknowledges and agrees that all records, documents, drawings, plans, specifications and other materials in the Authority's possession, including materials submitted by Contractor, are subject to the provisions of the Texas Public Information Act (see Texas Government Code § 552.001). 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 Authority are clearly and prominently labeled "Trade Secret" or "Confidential" by Contractor, the Authority 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 Authority 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 Authority or its officers, employees, contractors or consultants.

In the event of litigation concerning the disclosure of any material marked by Contractor as "Trade Secret" or "Confidential," the Authority'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 Authority 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 reasonable attorneys' fees and costs, incurred by the Authority in connection with any litigation, proceeding or request for disclosure shall be reimbursed and paid by Contractor.

DELOITTE CONSULTING LLP



Uday Katira, Managing Director
Deloitte Consulting, LLP

08/04/2024

Date

**CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY**

James M. Bass
Executive Director

Date



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024 AGENDA ITEM #11

Discuss and consider approving an agreement with Sistema Technologies, Inc. for enhancements to the Mobility Authority's Data Platform System for administration of users and roles

Strategic Plan Relevance:	Innovation
Department:	Operations
Contact:	Greg Mack, Director of IT and Toll Systems
Associated Costs:	Not to exceed \$88,000 (with 10% contingency)
Funding Source:	FY25 Capital Budget
Action Requested:	Consider and act on draft resolution

Project Description/Background: The Data Platform System (DPS) is the the agency's evolution to a mature toll entity that controls transaction pricing and revenue recognition timing. The DPS provides the Mobility 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 process all toll transaction data processing and data management capabilities after the point of transaction creation to a Mobility Authority-managed solution. Kapsch and Quarterhill, the Mobility Authority's Lane vendors, collect the toll transaction at the roadside and forward the transaction and vehicle images to the DPS. Business logic then consumes the transaction and routes 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 Mobility Authority's toll transactions. The DPS went live in August 2023.

The Mobility Authority desires continued development services as the system matures and seeks engagement of additional vendors to understand the system in order to mitigate risks in having a single vendor with complete knowledge of the system. This

development item is to enhance the security administration of the data platform of users and privileged roles within the system. This security management console will allow a consolidated view of users and access privilege within and improve the administration. Today's action is directly related to the engagement of additional resources for such understanding and development.

Previous Actions & Brief History of the Program/Project: Deloitte Consulting has been awarded contracts since February 2021 for the initial development, ongoing operations and maintenance and enhancement support of the Data Platform. This will be the first contract for a new vendor to assist with enhancement development for TOMS.

Financing: FY25 Capital Budget

Action requested/Staff Recommendation: Staff recommends approving an agreement with Sistema Technologies, Inc. for consulting services for enhancement development of the Mobility Authority's Data Platform System.

Backup provided:

Draft Resolution
Statement of Work - Tolling Operations Management
Solution (TOMS) - 2024 UI Administration of Users and
Roles (March 2024)
Technical and Commercial Proposal For Building the TOMS
User and Role Management To CTRMA
DIR Public Records Act Agreement – Sistema Technologies
TOMS Statement of Work
DIR Vendor Agreement – Sistema Technologies TOMS
Statement of Work

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

RESOLUTION NO. 24-0XX

**APPROVING AN AGREEMENT WITH SISTEMA TECHNOLOGIES, INC. FOR
SECURITY ENHANCEMENTS TO THE MOBILITY AUTHORITY'S DATA
PLATFORM SYSTEM**

WHEREAS, the Mobility Authority hosts its own system for processing all toll transaction data processing and performing data management after the point of transaction creation (the "Data Platform System"); and

WHEREAS, the Mobility Authority desires to make certain security enhancements to the Data Platform System related to the ability to manage users through the Tolling Operations Management Solution user interface; and

WHEREAS, the Executive Director has negotiated a scope of work with Sistema Technologies, Inc. in an amount not to exceed \$88,000.00 for certain security 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 Sistema Technologies, Inc. for certain security enhancements to the Data Platform System in an amount not to exceed \$88,000.00 through their DIR cooperative contract.

NOW THEREFORE BE IT RESOLVED that the Board of Directors hereby approves the scope of work for the security 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 Sistema Technologies, Inc. in an amount not to exceed \$88,000.00 through their cooperative contract with the Texas Department of Information Resources for security enhancements to the Data Platform System.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of September 2024.

Submitted and reviewed by:

James M. Bass
Executive Director

Approved:

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

Exhibit A



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

Statement of Work

Tolling Operations Management Solution (TOMS)

2024 – UI Administration of Users and Roles

March 2024

Contents

1.	Statement of Work Purpose and Overview	4
1.1.	Term.....	5
1.2.	General Assumptions.....	5
2.	Scope of Services.....	5
2.1.	Requirements & Design Services.....	5
2.2.	Development Services	6
2.3.	Testing Services	6
2.4.	User Acceptance Testing (UAT) Services	6
2.5.	Release Services.....	7
2.6.	Warranty Services.....	7
3.	Deliverables.....	7
3.1.	Description.....	7
3.2.	Vendor Deliverables & Payment Allocation	8
3.3.	Invoices	8
3.4.	Acceptance Management.....	8
4.	Project Governance.....	9
4.1.	Project Issues Management	9
4.2.	Change Process.....	10
4.3.	Unforeseen Conditions and Events	11
4.4.	Delays and Extensions	11
5.	Payment Terms	11
6.	Additional Terms and Conditions.....	11
7.	Compliance with CTRMA Information Security Guidelines	12
8.	Location of Work, Hours and Conditions.....	12
9.	Vendor Response	13
9.1.	General Guidelines.	13
9.2.	Staff Capabilities.....	13
9.3.	Vendor History and Experience	13
9.4.	Project Work Plan.....	13
9.5.	Additional Considerations	14
9.6.	Pricing	14
10.	Schedule of Events and Response Guidelines:	14
11.	Response Evaluation Criteria	15
12.	Additional Agreements	15
12.1.	DIR Vendor Agreement.....	15

12.2.	Public Records Act Agreement	15
13.	Appendix 1 - Scope of Work.....	16
13.1.	Requirements (User Stories)	16
13.2.	Wireframes	19

1. Statement of Work Purpose and Overview

The Central Texas Regional Mobility Authority (CTRMA) is a Texas political subdivision with broad powers under state law to construct, maintain, and operate transportation projects. The CTRMA currently operates projects in Travis and Williamson Counties, and may do so in adjacent counties if they join the CTRMA in the future or as otherwise permitted by law. The powers and duties exercised by CTRMA and its Board of Directors (the "Board") are established by and subject to state and federal laws and regulations.

CTRMA works cooperatively with the Texas Department of Transportation (TxDOT) and the Capital Area Metropolitan Area Planning Organization (CAMPO) to identify and implement transportation projects in the Central Texas area. CTRMA is currently operating several toll projects, including the 183A Toll, 290 Toll (Manor Expressway), 71 Toll Lane, the MoPac Express Lane, SH 45SW, and a portion of 183 South (Bergstrom Expressway), and is constructing the remainder of 183 South and 290/130 Flyovers projects. In addition, the agency is pursuing the development of several toll projects, including 183A Toll Phase III, MoPac South, and 183 North.

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.

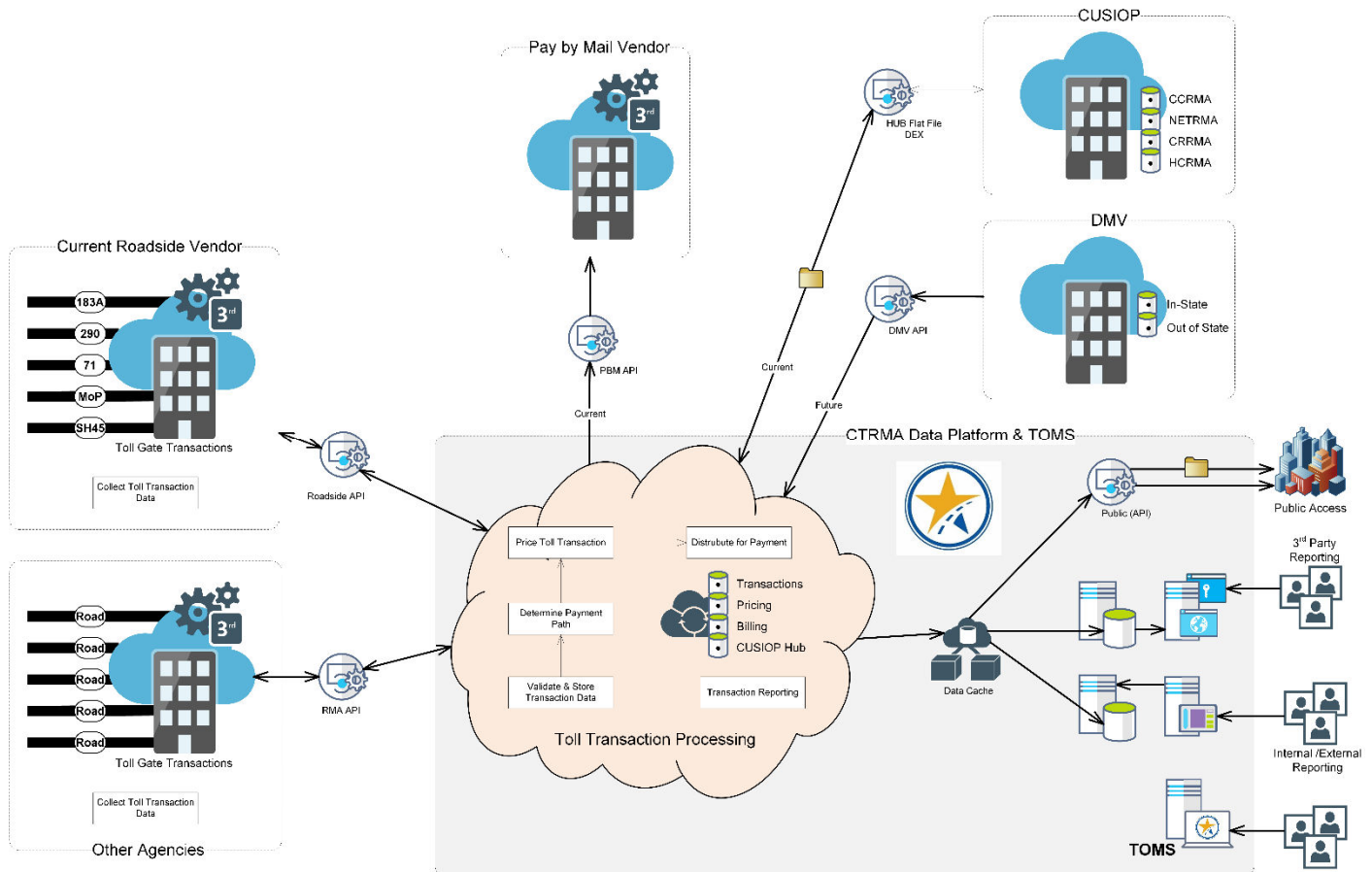


Figure 1: CTRMA DPS and TOMS Logical Architecture

The purpose of this Statement of Work (“SOW”) is to define a suite of services necessary to support the development and implementation of in-scope 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.

The services solicited by this SOW are detailed in Appendix 1 - Scope of Work. The selected Vendor will work at the direction and supervision of CTRMA to provide the services and work cooperatively and collaboratively with CTRMA’s other consultants.

1.1. Term

The Effective Date of this Contract is the date on which this Contract is fully executed and approved according to applicable laws, rules, and regulations. This Contract terminates on June 30, 2025, unless otherwise terminated or extended in accordance with its terms.

1.2. General Assumptions

- 1.2.1. CTRMA’s development environment is currently in place and shared by multiple internal and external development teams.
- 1.2.2. Vendor will provide any necessary development support tools unique to their approach and standard development methods.

2. Scope of Services

Vendor will provide the following services to CTRMA (Vendor Deliverables are noted in ***bold italics***):

2.1. Requirements & Design Services

CTRMA will define and document the requirements for each scoped and prioritized feature. The 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 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 requirements and address any required clarifications.

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 an estimated sprint schedule. If CTRMA approves the design and sprint schedule, the Enhancement will be moved into the Development phase.

2.1.1. Vendor Requirements / Design Services & Deliverables

- Review and analyze requirements documentation provided by CTRMA
- Identify risks and/or constraints and present feedback to CTRMA on documented requirements
- 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) and estimated Sprint schedule with risk and constrains to CTRMA
- Develop revised cost and estimated schedule to deliver CTRMA selected design(s), if necessary

- Present final design and estimated sprint schedule to CTRMA for review and acceptance***

2.2. 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.

2.2.1. 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***

2.3. 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.

2.3.1. 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***

2.4. 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.

2.4.1. 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***

2.5. 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.

2.5.1. 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***

2.6. Warranty Services

Unless otherwise mutually agreed, the Warranty Period shall be 90 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, Vendor will present a retrospective and accompanying Warranty Period Defect summary documentation to CTRMA for acceptance.

2.6.1. 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
Requirement and Design	Present final design and estimated Sprint 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 should invoice the CTRMA after each Payment Deliverable is accepted. CTRMA will not make partial payments for deliverable subtasks.

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 in 3 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 and Tolling*

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	<i>Name</i>	Greg Mack
Role	<i>Role</i>	Director of IT and Tolling

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. Payment Terms

Payment Terms shall be governed by and in accordance with active Vendor DIR Contract.

6. 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 Best and Final Offer (if required).
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.

7. Compliance with CTRMA Information Security Guidelines

The Vendor shall become familiar with and adhere to CTRMA's Information Security policies. 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 E)

8. 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.

9. Vendor Response

The following information shall be provided in the Vendor's Response:

9.1. General Guidelines.

- i. All written responses must be phrased in terms and language that can be easily understood by non-technical personnel (e.g., laypersons without subject matter expertise)
- ii. All document deliverables must be in formats (hard copy and electronic) as specified by the Customer - at a minimum, the formats must be in industry accepted standards (e.g., MS Word, MS PowerPoint, MS Project)
- iii. The Vendor must demonstrate its knowledge and expertise of the environment (e.g., platforms, software, applications, network, tools, etc.).

9.2. Staff Capabilities

Vendor staff capabilities specific to this SOW:

- i. Organization chart
- ii. Management team resumes
- iii. Key personnel resumes, illustrating the qualifications of each to perform the services described in this SOW including expertise in Agile development methodology and processes.

9.3. Vendor History and Experience

Vendor shall provide evidence of its services capabilities, including but not limited to:

- i. Description of three (3) projects of similar size and scope that Vendor has conducted within the past five (5) years.
 - a. Brief project description, including the experience with providing similar systems and services.
 - b. Project location
 - c. Client name
 - d. Client contact (name, telephone & email)
 - e. Status: Active, Completed, Maintenance, Terminated, other
 - f. Project innovation that has been evaluated and implemented
 - g. Start date (Notice to Proceed)
 - h. Completion date of project implementation (if completed)
 - i. The client contact names provided will be used as reference checks by the CTRMA Evaluation Committee. Inaccurate contact information may result in disqualification.
- ii. Vendor shall include an outline of its capability to deliver the required services, including process, functional and technical expertise.
- iii. Vendor may also include the types of information that it anticipates providing as part of each deliverable.

9.4. Project Work Plan

Vendor shall provide a draft high-level project work plan addressing the tasks specified in the SOW, which shall include:

- i. A description of key activities and milestones.
- ii. A detailed methodology description of the Vendor's approach to analyze, assess, validate, document and complete each sprint/iteration.

- iii. A description of the resources necessary from CTRMA to support the process, including estimates of time needed from CTRMA’s subject matter experts and high-level analysis of data gathering requirements.
- iv. Any assumptions and dependencies of the project.

9.4.1. Sample Project Plan

No	Item	Date/Sprint(s)	Comments
1	Ability to View TOMS Users in the TOMS UI		
2	Ability to View TOMS Roles in the TOMS UI		
3	Ability to Create TOMS Users and Assign Roles		
4	Ability to Create TOMS Roles and Assign Permissions		
5	Ability to Export Users and Roles to a formatted Excel template		

9.5. Additional Considerations

- i. Vendor shall indicate their agreement to comply with the confidentiality and non-disclosure requirements stated in this SOW.
- ii. All written deliverables must be phrased in terms and language that can be easily understood by non-technical personnel (e.g., laypersons without subject matter expertise)
- iii. All items of this agreement shall be done in accordance with the Service Level Agreement.
- iv. CTRMA may request oral presentations.

9.6. Pricing

The main purpose of this section is to detail the pricing for the deliverables-based services. Vendor should also provide a summary of any assumptions and exclusions.

9.6.1. Sample Pricing Table

No	Item	Price
1	Ability to View TOMS Users in the TOMS UI	
2	Ability to View TOMS Roles in the TOMS UI	
3	Ability to Create TOMS Users and Assign Roles	
4	Ability to Create TOMS Roles and Assign Permissions	
5	Ability to Export Users and Roles to a formatted Excel template	

10. Schedule of Events and Response Guidelines:

The following dates represent CTRMA’s desired schedule of events associated with this Statement of Work inquiry. CTRMA reserves the right to modify these dates at any time, with appropriate notice to prospective Vendors.

Event	Date
SOW Released	March 25, 2024
Questions due to CTRMA at DataPlatformProcurement@CTRMA.org	5 business days later
Pre-submission Bidders Conference (Attendance Optional)	3 business days after SOW released
Last Day Responses to Questions will be provided	2 days after questions due
Qualification Statements Due	3 weeks after SOW release
Oral Presentations (Optional)	One week after statements due
Formal Notice of Selection of Qualified Contractors	August 2024

11. Response Evaluation Criteria

(The following criteria are examples that could be used in determining the best fit.)

- i. Technical Approach to Agile methodology (overview of performance-based solution and quality control and performance measurement approach)
- ii. Method for planning and sizing of work to be performed
- iii. Project Work Plan
- iv. Vendor History and Experience (including references).

12. Additional Agreements

The selected vendor will comply with additional agreements as drafted below

12.1. DIR Vendor Agreement

This is to signify that the Central Texas Regional Mobility Authority and _____ have entered into an Agreement in an amount not to exceed _____ pursuant to Texas Government Code Section 2054.0565 utilizing Texas Department of Information Resources Contract No. # _____ for the deliverable-based information technology services described in this proposal. All terms and conditions of Texas Department of Information Resources Contract No. # _____ are applicable to and made part of this agreement.

12.2. Public Records Act Agreement

Contractor acknowledges and agrees that all records, documents, drawings, plans, specifications and other materials in the Authority's possession, including materials submitted by Contractor, are subject to the provisions of the Texas Public Information Act (see Texas Government Code § 552.001). 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 Authority are clearly and prominently labeled "Trade Secret" or "Confidential" by Contractor, the Authority 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 Authority 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 Authority or its officers, employees, contractors or consultants.

In the event of litigation concerning the disclosure of any material marked by Contractor as "Trade Secret" or "Confidential," the Authority'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 Authority 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 reasonable attorneys' fees and costs, incurred by the Authority in connection with any litigation, proceeding or request or disclosure shall be reimbursed and paid by Contractor.

13. Appendix 1 - Scope of Work

13.1. Requirements (User Stories)

13.1.1. Ability to View TOMS Users in the TOMS UI

As a TOMS Administrator

I want to view Users and their Assigned Roles

So I can understand which Roles each User is assigned to

ACCEPTANCE CRITERIA

Given I am authenticated and on the TOMS Home Page

When I click on the Menu

Then an option to navigate to the TOMS User and Admin page(s) will be available

And selecting the menu item will navigate me to the User Main Page

And the view will contain a single User table with:

- User Name (sortable)
- User Email (sortable)
- Agency(s) (sortable, filterable)
- Date Created (sortable)
- Created By (sortable, filterable)
- Date Modified (sortable)
- Modified by (sortable, filterable)

When I select an Agency from the Global Agency Filter

Then Users displayed in the User table will filter the records for the selected Agency

Given I am viewing the User Main Page

When I select a User

Then it will navigate me to the User Summary Page

Where the properties of the currently selected User will appear in form format in the left window pane

Where the Main User table would appear in the right window pane

When I select a different User in the Main User Table

Then the left window pane will update to show the properties of the newly selected User

When I select an Agency from the Global Agency Filter

Then Users displayed in the User table will filter the records for the selected Agency

When I click the Back link

Then I will navigate to the User Main Page

Given I am viewing the TOMS User Summary Page

When I click the View Details link

Then it will navigate me to the User Details Page

Where the properties of the currently selected User will appear in form format in the left window pane

Where the Assigned Roles table would appear in the right window pane

And the Assigned Roles table will contain:

- Agency (sortable)
- Role Name (sortable)
- Date Added (sortable)
- Role Description

When I select an Agency from the Global Agency Filter

Then Roles displayed in the Assigned Roles table will filter the records for the selected Agency

When I click the Back link

Then I will navigate to the User Summary Page

When I click the Role Name link

Then a new session will open

Then I will navigate to the Role Details Page of the selected Role in the new session

13.1.2. Ability to View TOMS Roles in the TOMS UI

As a TOMS Administrator

I want to view Roles and their Assigned Permissions

So I can understand which Permissions are assigned to each Role

ACCEPTANCE CRITERIA

Given I am authenticated and on any TOMS User page

When I click on the Roles link

Then I will navigate to the TOMS Roles Main Page

And the view will contain a single Role table with:

- Role Name (sortable)
- Agency(s) (sortable)
- Date Created (sortable)
- Created By (sortable, filterable)
- Date Modified (sortable)
- Modified by (sortable, filterable)

When I select an Agency from the Global Agency Filter

Then the Roles displayed in the Roles table will filter the records for the selected Agency

Given I am viewing the TOMS Role Main Page

When I select a Role

Then it will navigate me to the Role Summary Page

Where the properties of the currently selected Role will appear in form format in the left window pane

Where the Main Role table would appear in the right window pane

When I select a different Role in the Main Role Table

Then the left window pane will update to show the properties of the newly selected Role

When I select an Agency from the Global Agency Filter

Then the Roles displayed in the Role table will filter the records for the selected Agency

When I click the Back link

Then I will navigate to the Role Main Page

Given I am viewing the Role Summary Page

When I click the View Details link

Then it will navigate me to the Role Details Page

Where the properties of the currently selected Role will appear in form format in the left window pane

Where the Assigned Permissions table would appear in the right window pane

And the Assigned Permissions table will contain:

- Agency (sortable)
- Permission (sortable)
- Date Added (sortable)
- Permission Description

When I select an Agency from the Global Agency Filter

Then Permissions displayed in the Assigned Permissions table will filter the records for the selected Agency

When I click the Back link

Then I will navigate to the Role Summary Page

13.1.3. Ability to Create TOMS Users and Assign Roles

As a TOMS Administrator

I want to Create Users and assign Roles to them

So I can manage TOMS user access permissions

ACCEPTANCE CRITERIA

Given I am authenticated and on any TOMS User page

When I click on the +New User button

Then the Create User page will open

Where the properties of the new User will appear in form format in the left window pane

And the new User form will contain:

- User Name (required), pull-down list of available Users
- User Email (required), pull-down list of available User Emails
- Date Created (non-editable)
- Created By (non-editable)
- Date Modified (non-editable), null until first edit
- Modified by (non-editable), null until first edit
- Assign Agencies, list of agencies available to the User (multi-select), limited by User access controls
- Assign Roles, list of roles related to selected Agencies (multi-select)
- Cancel button
- Save button (available only when all required fields are populated)

Where the Assigned Roles table would appear in the right window pane

And the view will contain a single unpopulated Role table with:

- Agency(s)
- Role Name
- Date Added
- Role Description

When I select an Agency from the Assign Agency field

Then the Assign Roles field will populate with the Roles associated to the selected agencies

When I click the Save button

Then the User and associated roles will be saved in the system

And I will navigate the User Details Page of the newly created User

13.1.4. Ability to Create TOMS Roles and Assign Permissions

As a TOMS Administrator

I want to Create Roles and assign Permissions to them

So I can manage TOMS user access permissions

ACCEPTANCE CRITERIA

Given I am authenticated and on any TOMS Role page

When I click on the +New Role button

Then the Create Role page will open

Where the properties of the new Role will appear in form format in the left window pane

And the new User form will contain:

Role Name (required)

- Role Agency (required), pull-down list of available Agencies
- Date Created (non-editable)
- Created By (non-editable)
- Date Modified (non-editable), null until first edit
- Modified by (non-editable), null until first edit
- Assign Permissions, list of permission available to the User (multi-select), limited by User access controls
- Cancel button
- Save button (available only when all required fields are populated)

Where the Assigned Permissions table would appear in the right window pane

And the view will contain a single unpopulated Permissions table with:

- Agency(s)
- Permission Name
- Permission Description

When I select an Agency from the Agency field

Then the Assign Permissions field will populate with the permissions associated to the selected agency

When I click the Save button

Then the Role and associated Permissions will be saved in the system

And I will navigate the Role Details Page of the newly created Role

13.1.5. Ability to export User and Roles to a formatted Excel template

When I am viewing User or Role information

I want to export the data to Excel

So I can analyze and consume the data outside of TOMS

ACCEPTANCE CRITERIA

Given I am authenticated and in the TOMS User or Role views

When I select the download to Excel button

Then a download function would execute

And it would provide a formatted Excel file with the relevant User, Role, and/or Permission data

See Attached Templates:



Export Users.xlsx



Export User Details.xlsx



Export Roles.xlsx



Export Role Details.xlsx

13.2. Wireframes



CTRMA Users and Roles Wireframes v1

IN WITNESS WHEREOF, the parties have caused this SOW to be executed as of the date signed by the Central Texas Regional Mobility Authority and written below.

SISTEMA TECHNOLOGIES, INC.

CENTRAL TEXAS REGIONAL MOBILITY
AUTHORITY

(Signature)

(Signature)

Joe Vallejo

(Printed Name)

James M. Bass

(Printed Name)

President

(Title)

Executive Director

(Title)

(Date)

(Date)

DIR Vendor Agreement

This is to signify that the Central Texas Regional Mobility Authority and Sistema Technologies, Inc. have entered into a one-year Agreement **in an amount not to exceed \$88,000.00** pursuant to Texas Government Code Section 2054.0565 utilizing Texas Department of Information Resources Contract No. #DIR-CPO-4937 for the Microsoft Enterprise Agreement services described in this proposal. All terms and conditions of Texas Department of Information Resources Contract No. #DIR-CPO- 4937 are applicable to and made part of this agreement.

SISTEMA TECHNOLOGIES, INC.

**CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY**

Joe Vallejo
President

James M. Bass
Executive Director

Date

Date

Public Records Act Agreement

Contractor acknowledges and agrees that all records, documents, drawings, plans, specifications and other materials in the Authority's possession, including materials submitted by Contractor, are subject to the provisions of the Texas Public Information Act (see Texas Government Code § 552.001). 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 Authority are clearly and prominently labeled "Trade Secret" or "Confidential" by Contractor, the Authority 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 Authority 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 Authority or its officers, employees, contractors or consultants.

In the event of litigation concerning the disclosure of any material marked by Contractor as "Trade Secret" or "Confidential," the Authority'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 Authority 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 reasonable attorneys' fees and costs, incurred by the Authority in connection with any litigation, proceeding or request for disclosure shall be reimbursed and paid by Contractor.

SISTEMA TECHNOLOGIES, INC.

**CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY**

Joe Vallejo
President

James M. Bass
Executive Director

Date

Date



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024 AGENDA ITEM #12

Discuss and consider approving a shortlist of proposers to receive the Request for Proposals for Video Toll Billing, Payment Processing, Collections, Enforcement Support, and Customer Services

Strategic Plan Relevance:	Innovation
Department:	Operations
Contact:	Tracie Brown, Director of Operations
Associated Costs:	\$850,000
Funding Source:	FY24 Operating Budget
Action Requested:	Consider and act on draft resolution

Project Description/Background: CTRMA toll facilities utilize modern Electronic Toll Collection System (ETCS) technology to capture data from passing vehicles enabling CTRMA to collect tolls electronically. CTRMA employs All Electronic Tolling (AET), in which roadside equipment identifies radio frequency transponders when present and mounted in the vehicles of customers with transponder-based accounts.

Data is initially transmitted to CTRMA's Data Platform System (DPS), and then directed to either the Central United States (CUSIOP) or Southeastern United States (SEIOP) interoperable hub systems for posting and debiting of eligible customer home agency accounts. CTRMA facilities are interoperable and currently accept TxDOT's TxTag, North Texas Tollway Authority's TollTag, Harris County Toll Road Authority's EZ Tag, Kansas Turnpike Authority's K-TAG, Oklahoma Turnpike Authority's PikePass, Florida Turnpike Enterprise's SunPass, and other tag and electronic products facilitated by their interoperable partners.

For the remaining vehicles not deemed eligible for CUSIOP or SEIOP posting, the roadside system captures images of the vehicle's license plate(s). Through the process of Optical Character Recognition (OCR) and/or Human Image Review, image-based

transactions, along with the transactional information (location, date/time, classification of the vehicle, toll amount, license plate information, etc.) are sent to CTRMA's Pay By Mail system for revenue collection. Pay By Mail processing generally includes invoicing, payment processing, customer support/call center services, enhanced enforcement remedies, legal action, and collections activities.

Current Action: In late 2022, the Mobility Authority's staff began to evaluate Pay By Mail Best Practices by engaging AtkinsRéalis to perform an industry survey. The output of this effort was the documentation of the Pay By Mail Industry Survey Results in February 2023.

Following the Industry Survey, the Mobility Authority began drafting scope for two-step procurement process including a Request for Qualifications (RFQ) and a Request for Proposal (RFP). The RFQ phase of the procurement establishes a shortlist of the most qualified Respondents (shortlist) based on the evaluation criteria set forth in the RFQ document. Only Respondents shortlisted during the RFQ phase can participate in the RFP portion of the procurement.

The scope of the procurement is for Pay By Mail services for CTRMA's Payment Program for services including a back-office system and the operational staff and support needed to facilitate invoicing and processing (video billing), violations processing, collections, enforcement of unpaid tolls, and customer services. The services may also include pre-paid (plate-based) account management and transponder account management and distribution services.

The initial term of the contract is seven years. CTRMA shall have the option to extend the contract for two (2) additional two-year renewals. Final details containing the contract terms and renewals are subject to approval by the CTRMA Board of Directors.

On May 1, 2024, the Authority publicly issued a Request for Qualifications (RFQ) for Pay By Mail services on CIVCAST. The Authority also advertised a public notice in the Austin American-Statesman. One addendum was subsequently issued. In response to the RFQ, the Mobility Authority received eleven Statements of Qualifications ("submissions"). Submissions were received from the following Proposers, listed alphabetically:

1. Conduent
2. Emovis

3. Global Agility Solutions
4. Indra USA
5. InteLogix
6. Neology
7. Professional Account Management
8. Quarterhill
9. SWC Group
10. TTEC
11. ViaPlus

Each submission was reviewed for compliance with the Mobility Authority's stated criteria including company references, past contract performance, projects and client listings, financial ability to implement the project, and compliance with providing SOC 1 Type 2 audits, Level 1 PCI Compliance, as well as insurance and bonding requirements.

All submissions received were reviewed by the Pass/Fail Committee and conveyed to evaluation team members for consensus scoring. The resultant ranking and shortlist recommendation was then presented to the Mobility Authority's Executive Director. The outcome of this process was a recommended shortlist. Per the RFQ, this shortlist of Proposers is eligible to receive and respond to the Request for Proposals (RFP), which signifies the beginning of step two of the two stage procurement process.

Next Steps: Should the board approve this item, staff will release the Request for Proposal to the pre-qualified respondents in November or December 2024. Vendor responses will be due February or March 2025. Staff expects to present its recommendation for the selected vendor at the July 2025 board meeting and request approval for the Executive Director to negotiate and execute a contract with the selected vendor.

Previous Actions: In December 2018 the CTRMA Board of Director approved the first amendment to the Agreement with Cofiroute USA outlining CUSA's expected recompense for processing and collecting Pay By Mail toll transactions paid from post-paid accounts, overpayments and prior to notice generation (*Pay Item #1*). The amendment also added pay items related to insufficient funds (*Pay Item #9*) and out of state license plate lookups (*Pay Item #10*).

In July 2019 the Board approved Amendment No. 2 to the Agreement with Cofiroute USA to add a new pay item to support habitual violator program, additional customer service hours, and additional support for the qualified veteran program. A third amendment was approved in February 2023 to allow for a vendor incentive if certain customer service and collection metrics are met.

Financing: FY25 Operating Budget

Action Requested/Staff Recommendation: Staff recommends approving a shortlist of vendors to receive the Request for Proposals for back-office services supporting the Authority's customer service, payment processing, collections, enforcement, and account management operations functions as determined through the Request for Qualification (RFQ) process.

Backup provided: Draft Resolution

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

RESOLUTION NO. 24-0XX

**APPROVING A SHORTLIST OF PROPOSERS TO RECEIVE
THE REQUEST FOR PROPOSALS FOR VIDEO TOLLING, PAYMENT PROCESSING,
COLLECTIONS, ENFORCEMENT SUPPORT, AND CUSTOMER SERVICES**

WHEREAS, by Resolution No. 18-005, dated February 28, 2018, the Board approved an agreement with Cofiroute USA, LLC (now known as ViaPlus by VINCI Highways or “ViaPlus”) for pay by mail, violations processing, collections and customer services (the “ViaPlus Agreement”); and

WHEREAS, in anticipation of the March 8, 2027 expiration of the ViaPlus Agreement, the Mobility Authority issued a request for qualifications (RFQ) from firms interested in providing video tolling, payment processing, collections, enforcement support, and customer services to the Mobility Authority on May 1, 2024;

WHEREAS, the Mobility Authority received eleven responses by the June 28, 2024 deadline which were evaluated and ranked in accordance with the terms of the RFQ; and

WHEREAS, an evaluation committee analyzed and scored each submittal based on the criteria set forth in the RFQ in order to develop a short-list of the most qualified firms to participate in the request for proposals phase of the procurement process; and

WHEREAS, the Executive Director reviewed the evaluation committee’s findings and recommends that the Board approve the short-list of firms identified by the evaluation committee which is set forth in Exhibit A hereto.

NOW THEREFORE, BE IT RESOLVED, that the Board hereby approves the short-list of firms identified and listed on Exhibit A to receive the Request for Proposals for Video Tolling, Payment Processing, Collections, Enforcement Support, and Customer Services to support the Mobility Authority’s Pay By Mail Program.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of September 2024.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

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

Exhibit A

(To be provided at the Board Meeting)



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024
AGENDA ITEM #13

Discuss and consider approving an amendment to the contract with H2O Partners, Inc. to add services for asset data collection on the 183A Phase III Project and data extraction for curb and gutter on all Mobility Authority corridors

Strategic Plan Relevance: Service
Department: Engineering
Contact: Mike Sexton, P.E., Director of Engineering
Associated Costs: \$42,856.00
Funding Source: 183A PHIII Project Funds
Action Requested: Consider and act on draft resolution

Project Description/Background: As part of the Transportation Asset Management Plan (TAMP) implemented by Central Texas Regional Mobility Authority in 2018, pavement condition data is to be collected to support the pavement management program. This data is utilized within the web-enabled Integrated GIS, Enterprise Asset Management software, VUEWorks, and is key in evaluation of routine maintenance and restoration and replacement (R&R) needs.

Previous Actions/Brief History of the Project/Program – Along with pavement condition data, the equipment captures asset imagery and is utilized for capturing the asset inventory to support the VUEWorks software as described. This method for data collection was used on the other CTRMA corridors through the Houston-Galveston Area Council Cooperative Purchasing Program (HGACbuy).

Financing: 183A PH III Project Funds

Action Requested/Staff Recommendation – Staff recommends executing an amendment to the existing 5-year contract with H2O Partners, Inc., providing pavement collection services through the HGACbuy Program. Under this proposed amendment, H2O Partners, Inc. will perform asset data collection services on 183A PH III, and data extraction for curb and gutter on all Mobility Authority corridors for an amount not to

exceed \$36,856.00. Staff also recommends establishing a contingency amount for this amendment to the contract of an amount not to exceed \$6,000.00 for a total contract NTE amount of \$567,856.00.

Backup provided:

Draft Resolution

Proposed amendment

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

RESOLUTION NO. 24-0XX

**APPROVING AN AMENDMENT TO THE CONTRACT WITH H2O PARTNERS, INC.
FOR ASSET DATA COLLECTION FOR THE 183A PHASE III PROJECT AND DATA
EXTRACTION FOR CURB AND GUTTER ON ALL ON MOBILITY AUTHORITY
FACILITIES**

WHEREAS, the Mobility Authority has established a Transportation Asset Management Program to collect and record asset and pavement condition data on Mobility Authority facilities to be utilized in evaluating routine maintenance and restoration and replacement needs; and

WHEREAS, it is necessary to regularly collect pavement condition data for Mobility Authority facilities to support on-going decision making for determining the best approach to pavement management; and

WHEREAS, in accordance with Article 15 of the Mobility Authority Policy Code, purchases made through a cooperative program such as the Houston-Galveston Area Council Cooperative Purchasing Program (HGACbuy) are deemed to have satisfied Mobility Authority procurement requirements; and

WHEREAS, by Resolution No. 22-004 dated January 26, 2022, the Board approved a contract with H2O Partners, Inc. for the collection of pavement condition data to be utilized in evaluating routine maintenance and restoration and replacement needs on Mobility Authority facilities in an amount not to exceed \$525,000 through HGACbuy for; and

WHEREAS, the Mobility Authority requires asset data collection services on the 183A Phase III project and data extraction for curb and gutter on all Mobility Authority corridors; and

WHEREAS, the Executive Director has negotiated an amendment to the contract with H2O Partners, Inc. for these additional services in the amount of \$42,856; and

WHEREAS, the Executive Director recommends approving the proposed amendment to the contract with H2O Partners, Inc. for asset data collection services on the 183A Phase III project and data extraction for curb and gutter on all Mobility Authority corridors which is attached hereto as Exhibit A.

NOW, THEREFORE, BE IT RESOLVED that the Board of Directors approves the amendment to the contract with H2O Partners, Inc. for asset data collection services on the 183A Phase III project and data extraction for curb and gutter on all Mobility Authority corridors in an amount not to exceed \$42,856 and in the form or substantially the same form attached hereto as Exhibit A; and

BE IT FURTHER RESOLVED that the Executive Director is authorized to finalize and execute the amendment to the contract with H2O Partners, Inc. on behalf of the Mobility Authority.
Submitted and reviewed by: Approved:

James M. Bass
Executive Director

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

Exhibit A



September 20, 2024

Central Texas Regional Mobility Authority
300 N. IH 35, Suite 300
Austin, TX 78705

Attn: Lisa Pohlmeier
Senior Project Manager
CTRMA - Asset Management

Subject: Central Texas Mobility Authority Amendment #1
HGACBuy Contract (No. HP08-21) for Pavement Data Collection Services

Dear Ms. Pohlmeier,

This Amendment #1 between H2O Partners, Inc., (H2O) having offices at 260 Addie Roy Road, Suite 150, Austin, TX 78746, and the Central Texas Mobility Authority (CTRMA), having offices at 300 N. IH 35, Suite 300, Austin, TX 78705 is for Pavement Data Collection Services. H2O via our subcontractor, Roadway Asset Services, LLC (RAS) shall provide to CTRMA the requested professional services as described herein the following documents attached as part of this agreement:

- Attachment A: CTRMA ROW Asset Data Collection Services Amendment #1 Scope of Work
- Attachment B: CTRMA HGACBuy Quote Amendment #1 v2
- Attachment C: Contract HP08-21 with Amendments and Extensions between HGAC and H2O

H2O will provide monthly invoices for completed services to CTRMA.

If you have any questions, please do not hesitate to contact Melissa Trent at (512) 740-5014 or mtrent@h2opartnersusa.com.

Sincerely,

A handwritten signature in blue ink, appearing to read "Eric Howard", is written over the typed name.

Eric Howard
Vice President

H2O Partners, Inc.

E Howard

(Signature)

Eric Howard

(Printed name)

Vice President

(Title)

9-20-2024

Date

CENTRAL TEXAS MOBILITY AUTHORITY

(Signature)

(Printed name)

(Title)

Date

Attachment A

Central Texas Regional Mobility Authority ROW Asset Data Collection Services

Amendment #1

Section I - Scope of Work:

Roadway Asset Services, LLC. (CONSULTANT) understands that the Central Texas Regional Mobility Authority (OWNER) desires to conduct a field survey of the right of way assets on 53 lane miles on 183A PHIII.

The CONSULTANT (Roadway Asset Services, LLC.) shall provide the following services to the OWNER:

- Mobile data collection of roadway imagery
- Right of way asset extraction consisting of:
 - Guardrails (Barrier) Inventory
 - Pavement Striping Inventory (Yellow Striping)
 - Pavement Striping Inventory (White Striping)
 - Pavement Markings Inventory (Graphics)
 - Sign & Support Inventory
 - Sign Panel
 - Sign Structure Ground
 - Sign Structure Overhead
 - Street Lights Inventory (Illumination Structure)
 - Retaining Walls Inventory
 - Curb and Gutter Inventory
 - Attenuators Inventory
 - Delineators/Object Markers Inventory

Description of the tasks to be performed.

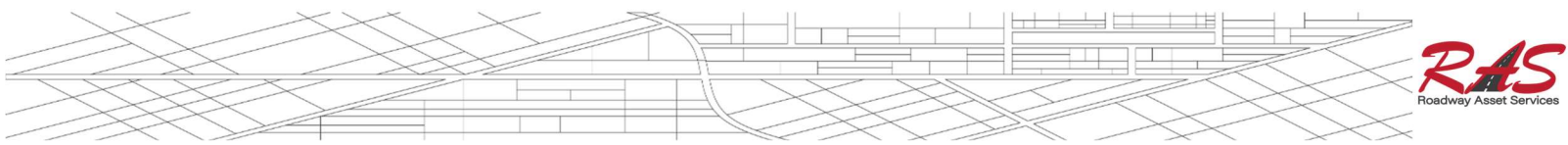
Task 1 - Project Setup

1.1 Project Initiation

Upon notice to proceed the CONSULTANT will arrange a kick-off meeting to confirm the project requirements and scheduling. The kick-off meeting will include proposed key personnel and the OWNER's project members. During the meeting, CONSULTANT will present the proposed Project Approach, which includes project equipment, software, methodology, schedules, and deliverables. The proposed approach will be finalized based on the OWNER requirements and decisions during the meeting. CONSULTANT will request that the OWNER provide any existing database, road centerlines, Geographic Information System (GIS) layers, and aerial imagery for project use. CONSULTANT will use the existing centerline data provided by the OWNER for routing of the 53 lane miles by the RAS collection vehicle. Project communication protocol, documentation, accounting methodologies, data format, and will be confirmed during the meeting.

1.2 Project Management

CONSULTANT will provide project management, including coordinating and attending meetings via web meetings or in person with OWNER, data research and collection efforts as required, preparing weekly



progress reports, and schedule updates. Weekly progress reports will include the total days collected and lost due to weather or mechanical issues for the current reporting period as well as cumulative totals. An exhibit displaying the roads collected and not yet collected will also be included.

CONSULTANT will report any data collection equipment problems, failures, or repairs within 24 hours to the OWNER Project Manager. Provide any information regarding equipment problems, calibration issues, equipment failures, and the ensuing solution to the OWNER Project Manager.

Task 1 Deliverables:

1. The CONSULTANT will deliver weekly progress reports and schedule updates.
2. The CONSULTANT will provide the OWNER with a centerline assessment document for review and approval.

Task 2 - Image Capture

The CONSULTANT will collect roadway data and images in accordance with Amendment #1 and NTP provided by the OWNER using a Roadway Asset Collection (RAC) vehicle in FY 2025.

2.1 *System Setup and Mobilization*

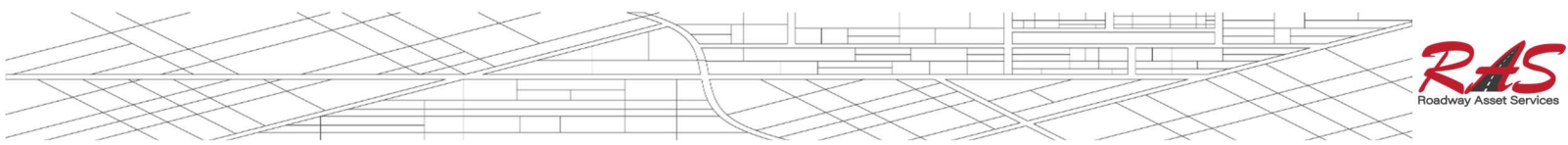
CONSULTANT will work with the OWNER to review and verify that the data is ready to proceed. CONSULTANT will set up the data collection system so that all GIS and database system data are integrated and properly configured.

CONSULTANT will collect data during clear weather conditions and during daylight hours (30 minutes after sunrise and 30 minutes before sunset). Data collection shall not occur when weather condition inhibits visibility, alters sensor measurements, or obscures the Right-of-Way (ROW) images.

CONSULTANT will not impede the flow of traffic at any time. Data collection will be allowed between 10:00 AM and 4:00 PM, Monday through Friday. This can be modified at OWNER's approval.

CONSULTANT will collect noted assets on all lanes in accordance with the geodatabase provided by the OWNER. Field Data and Image Capture

The CONSULTANT team consists of a driver and operator who will systematically drive the automated data collection vehicle on the road segment listings provided by the OWNER. The CONSULTANT will collect noted assets on shown on the geodatabase provided by the OWNER. CONSULTANT proposes to use its collection vehicle line scan camera with laser illumination and right-of-way cameras to capture ROW imagery to be used for asset extraction. Unpaved roads, shoulders and medians will not be surveyed.





A Roadway Asset Services, LLC automated data collection vehicle

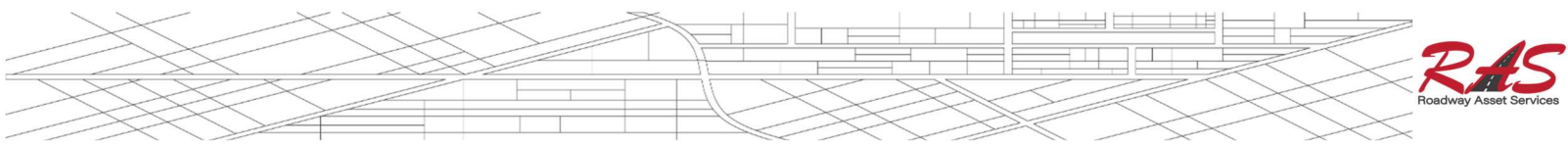
CONSULTANT will perform data field collection on paved travel lanes using a state-of-the-art International Cybernetics Corporation (ICC) data collection vehicle with following systems mounted:

- Right-of-way georeferenced images with Ladybug 5+ camera: Forward, Left, Right, and 360-degree spherical images.
- LCMS-2 pavement 2D/3D imaging.
- Longitudinal profile with 2-line lasers (left and right wheelpaths) Distance measuring instrument (DMI) with an accuracy of $\pm 0.1\%$.
- Differentially corrected GPS (DGPS) with an accuracy of ± 2 feet.
- Applanix POS/LV 220 to compensate for difficult GPS conditions in urban environments.

The CONSULTANT system collects all pavement and right-of-way images, Inertial Measurement Unit (IMU), DMI, and profiler data concurrently.

- 1) Submit a list of equipment and collection methods required to perform the service. If the vendor uses multiple vehicles to collect the data, all vehicles and equipment shall employ the identical hardware and software technologies for data collection and analysis.
- 2) Submit current TTI certification documentation. No data collection will occur without current and verified certification.

Task 2 Deliverables:



1. CONSULTANT will provide Right-of-Way imagery for all segments collected in a JPEG format.

Task 3 – Asset Data Collection Services

CONSULTANT’s Roadway Asset Collection (RAC) vehicles will capture images within 183A PHIII ROW limits at an interval of approximately 10 to 15 feet for both forward and side-facing directions and geo-referenced to the pavement inventory by segment. Each asset class will be provided as a file geodatabase. CONSULTANT will collect ROW assets with the following attributes:

3.1 Guardrails (Barrier) Inventory (Line Feature) Per OWNER Geodatabase

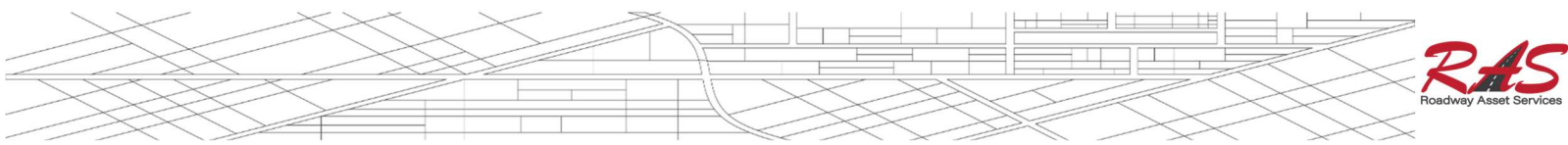
Feature class name – Barrier

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- BARRIER_TYPE
- DELINEATOR
- DATE_INSTALLED
- OWNER
- BEGIN_RM
- END_RM
- LENGTH
- BARRIER_UNITS

3.2 Pavement Striping Inventory (Yellow) (Line Feature) Per OWNER Geodatabase

Feature class name - Yellow Striping

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- STRIPING_COLOR
- DATE_INSTALLED
- OWNER
- BEGIN_RM
- END_RM
- Striping_Line_Type
- QTY
- STRIPINGYELLOW_UNITS



3.3 Pavement Striping Inventory (White) (Line Feature) Per OWNER Geodatabase

Feature class name – White Striping

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- STRIPING_COLOR
- DATE_INSTALLED
- OWNER
- BEGIN_RM
- END_RM
- Striping_Line_Type
- QTY
- STRIPINGWHITE_UNITS

3.4 Pavement Markings Inventory (Point Feature) Per OWNER Geodatabase

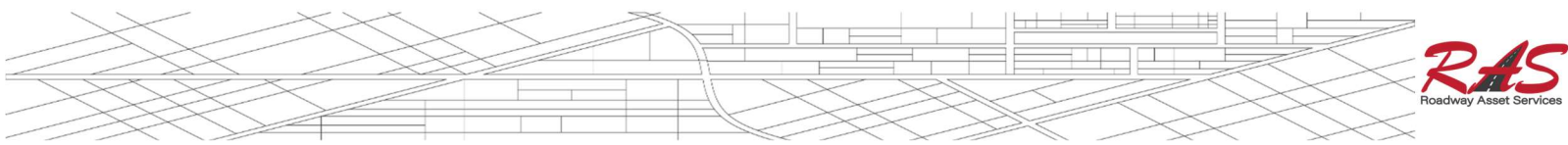
Feature class name – Graphics

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- GRAPHIC_TYPE
- GRAPHIC_COLOR
- DATE_INSTALLED
- OWNER
- RM
- GRAPHIC_UNITS

3.5 Sign & Support Inventory (Panel) (Point Feature) Per OWNER Geodatabase

Feature class name – Sign Panel

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE



- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- PANEL_MUTCD_CAT
- PANEL_MUTCD_CODE
- PANEL_SUPPORT_STRUCT
- PANEL_MATERIAL
- PANEL_SHEETING_TYPE
- DATE_INSTALLED
- PANEL_ORIENTATION
- PANEL_TEXT
- OWNER
- PANEL_PHOTO
- RM
- PANEL_UNITS

3.6 Sign & Support Inventory (Sign Structure Ground) (Point Feature) Per OWNER Geodatabase

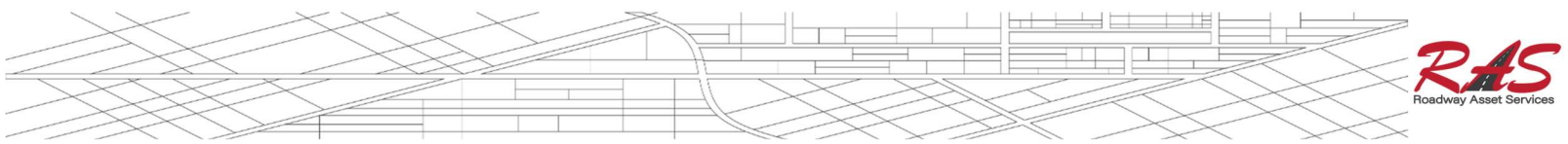
Feature class name – Sign Structure Ground

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- DATE_INSTALLED
- SS_TYPE
- POST_QTY
- BASE_TYPE
- OWNER
- RM
- SS_UNITS

3.7 Sign & Support Inventory (Sign Structure Overhead) (Point Feature) Per OWNER Geodatabase

Feature class name – Sign Structure Overhead

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME



- OSS_TYPE
- LENGTH
- RM
- DATE_INSTALLED
- OWNER
- OSS_PHOTO_1
- OSS_UNITS

3.8 Street Lights (Illuminated Structures) (Line Feature) Per OWNER Geodatabase

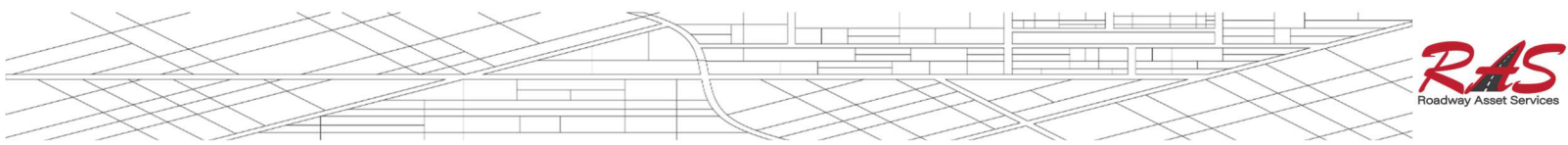
Feature class name – Illumination Structure

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- DATE_INSTALLED
- I_POST_TYPE
- I_POST_BASE
- I_POST_MA_LENGTH
- I_POST_MA_LENGTH2
- I_POST_MA_QUANTITY
- I_POST_LUMINAIRE
- I_POST_HM_CONFIG
- I_POST_HM_LUMINAIRE_QTY
- I_POST_OFFSET_PVMT
- OWNER
- I_POST_PHOTO
- RM
- I_POST_UNITS

3.9 Retaining Walls Inventory (Line Feature) Per OWNER Geodatabase

Feature class name – Walls

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- WALL_TYPE



- BEGIN_RM
- END_RM
- LENGTH
- OWNER
- DATE_INSTALLED
- WALL_UNITS

3.10 Curb and Gutter Inventory (Line Feature) Per OWNER Geodatabase

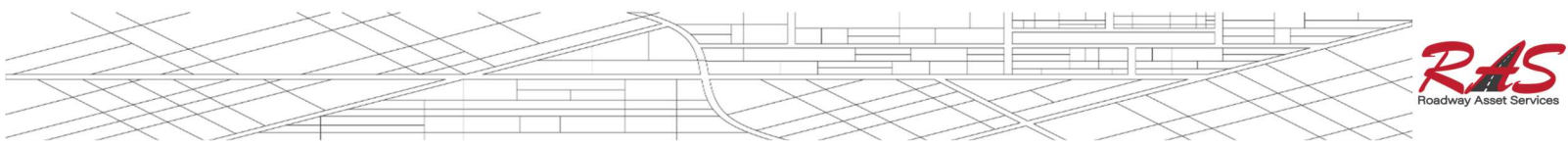
Feature class name – Curb and Gutter

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- CURB_TYPE
- LENGTH
- DATE_INSTALLED
- OWNER
- CURB_PHOTO
- BEGIN_RM
- END_RM
- CURB_UNITS

3.11 Attenuators Inventory (Point Feature) Per OWNER Geodatabase

Feature class name - Attenuator

- CORRIDOR_NAME
- CROSS_ST_NAME
- TRAVEL_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- ATTENUATOR_TYPE
- ATTENUATOR_STANDARD
- BARRIER_ATTEN_STANDARD
- MBGF_END_TREATMENT
- DATE_INSTALLED
- OWNER
- ATTENUATOR_PHOTO
- RM
- ATTENUATOR_BEGIN



- ATTENUATOR_END
- ATTEN_BEGIN_STANDARD
- ATTEN_END_STANDARD
- ATTENUATOR_UNITS

3.12 Delineators/Object Markers Inventory (Point Feature) Per OWNER Geodatabase

Feature class name – Delineators & Object Marker

- CORRIDOR_NAME
- TRAVEL_DIRECTION
- CONNECT_DIRECTION
- LANE_TYPE
- Branded_Corridor_Name
- POSTED_CORRIDOR_NAME
- DELINEATOR_TYPE
- RM
- DATE_INSTALLED
- OWNER
- DOM_UNITS

TASK 3 Deliverables:

- CONSULTANT will deliver a GIS layer with attributes identified above in a linear or point GIS file geodatabase for each of the outlined right of way assets.

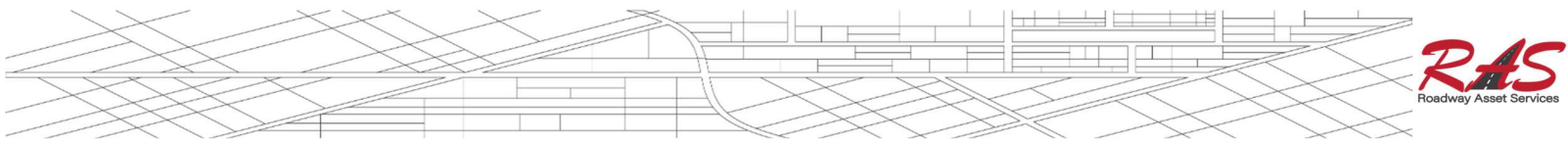
Task 4 Quality Assurance and Quality Control

The CONSULTANT will perform quality assurance and quality control on all data collected.

CONSULTANT has a proven Quality Assurance (QA)/Quality Control (QC) procedure for all mobile data collection projects. CONSULTANTS QC procedures begin with the collection vehicle collection process.

The technician will check each camera's exposure rate, image quality, GPS, and IMU operation to ensure the data collection system is recording appropriate data and that the GPS location is within the stated project tolerance. Each collection day's calibration collection will be documented in the collection logbook. The collection logbook also contains information such as date, location, technician's name, drivers name, any issue that developed during the collection day, and DMI calibration runs. CONSULTANT will maintain a Microsoft Access database of any collection or other project issues. All project team personnel including OWNER personnel will have access to the database to log comments, check the status of issues, and have one central repository to track project issues and resolutions. The OWNER will provide the location of the central repository.

During image collection, the technician reviews the images collected on-screen as they are collected and any issue with image clarity requires the collection run to end and the image quality issue to be resolved. Once resolved, the collection run begins from the beginning for the road segment collected. The technician also monitors GPS reception during collection. If GPS reception is lost (measured using PDOP – positional dilution of precision), the technician stops the collection and resolves the GPS reception issue. Collection begins again once the GPS reception issue is resolved. All issues resulting in the collection run being stopped will be recorded in the collection logbook along with the resolution.



With a completed collection drive delivered to CONSULTANT offices, images are post processed and provided to the image QC Officer who will perform quality control checks on each delivery provided. The QC Officer will visually review the collection routes for image quality. All collection runs that are considered of low quality will be marked for recollection before the data collection vehicle(s) is allowed to demobilize.

Additionally, CONSULTANT will provide independent quality checks via field verification to confirm accuracy of automated data collection.

TASK 4 Deliverables:

- CONSULTANT will review a select sample size of ROW asset imagery condition ratings to verify the accuracy of technicians

Acceptance Criteria

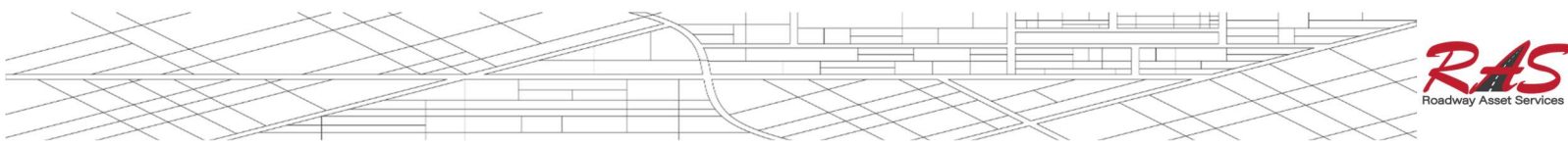
The results of the data collection shall be quality checked for rating consistency by CONSULTANT to ensure the accuracy and quality of deliverables. Additionally, deliverables will be checked for missing and/or duplicate assets. A 97% accuracy rate is expected, and Quality Control checks will be based on the batch/sample size of the delivery (see Table A below to determine sample size for the appropriate accuracy rate).

For any measurement that is needed it must be accurate to the nearest foot. If the data has more errors than allowable the set of data will be corrected. This process will be repeated until each set of data is within the allowable limits.

Method of measurement of acceptable quality level (AQL)

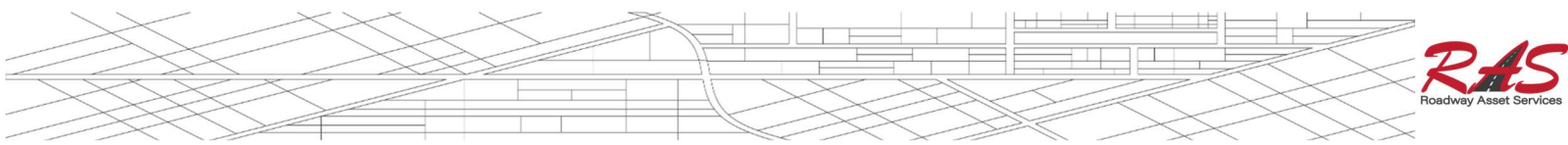
Each attribute captured for an asset counts as one unit of measure. Each physical measurement required for an asset location counts as one attribute or unit of measure. The following location information also counts as an attribute or unit of measure for each asset: Physical presence (when captured as per source = correct, not captured or missed = incorrect) In the event of a duplicate capture of an asset, the total number of attributes or units of measure for the duplicate asset(s) will be deducted from the total units of the sample set, and one error or unit of measure (incorrect physical presence) is charged.

Batch size			Sample Size (Normal)	Acceptance Rate (%)				
				99.0	98.5	97.5	96.0	93.5
2	to	8	2	≤ 0	≤ 0	≤ 0	≤ 0	≤ 0
9	to	15	3	≤ 0	≤ 0	≤ 0	≤ 0	≤ 0
16	to	25	5	≤ 0	≤ 0	≤ 0	≤ 0	≤ 1
26	to	50	8	≤ 0	≤ 0	≤ 0	≤ 1	≤ 1
51	to	90	13	≤ 0	≤ 0	≤ 1	≤ 1	≤ 2
91	to	150	20	≤ 0	≤ 1	≤ 1	≤ 2	≤ 3
151	to	280	32	≤ 1	≤ 1	≤ 2	≤ 3	≤ 5
281	to	500	50	≤ 1	≤ 2	≤ 3	≤ 5	≤ 7



501	to	1,200	80	≤ 2	≤ 3	≤ 5	≤ 7	≤ 10
1,201	to	3,200	125	≤ 3	≤ 5	≤ 7	≤ 10	≤ 14
3,201	to	10,000	200	≤ 5	≤ 7	≤ 10	≤ 14	≤ 21
10,001	to	35,000	315	≤ 7	≤ 10	≤ 14	≤ 21	≤ 21
35,001	to	150,000	500	≤ 10	≤ 14	≤ 21	≤ 21	≤ 21
150,001	to	500,000	800	≤ 14	≤ 21	≤ 21	≤ 21	≤ 21
500,001	and over		1250	≤ 21	≤ 21	≤ 21	≤ 21	≤ 21

Example: a delivery results in 100 assets – each asset has been determined to have 10 attributes to be captured (including the physical presence “attribute” for each asset) – thus total units of measure for the Batch size = 1,000 (100 x 10). Based on Table A, a Quality Control using a sample size of 80 units should be assessed for quality. With an expected accuracy of 97%, the allowable number of errors ≤ 5.




CONTRACT PRICING WORKSHEET
 For Catalog & Price Sheet Type Purchases

Contract No.:

HP08-21

Date Prepared:

9/20/2024

This Worksheet is prepared by Contractor and given to End User. If a PO is issued, both documents MUST be faxed to H-GAC @ 713-993-4548. Therefore please type or print legibly.

Buying Agency:	Central Texas Regional Mobility Authority	Contractor:	H2O Partners
Contact Person:	Lisa Pohlmeier	Prepared By:	Melissa Trent
Phone:		Phone:	512-740-5014
Fax:		Fax:	
Email:	lpohlmeier@ctrma.org	Email:	mtrent@h2opartnersusa.com

Catalog / Price Sheet Name:	
General Description of Product:	Year - Amendment #1 - 2025

A. Catalog / Price Sheet Items being purchased - Itemize Below - Attach Additional Sheet If Necessary

Quan	Description	Unit Pr	Total
1	Centerline Identification, Field Set-up, GPS Network Creation & Mobilization (lump sum) (183A PHIII Asset) A#1	\$ 7,450.00	\$ 7,450.00
53	Collect Street Network (test mile)(183A PHIII Asset) A#1	\$ 112.00	\$ 5,936.00
36	Guardrails (Barriers) Inventory (lane mile)(183A PHIII Asset) A#1	\$ 25.00	\$ 900.00
53	Pavement Striping Inventory (Yellow) (lane mile)(183A PHIII Asset) A#1	\$ 40.00	\$ 2,120.00
53	Pavement Striping Inventory (White) (lane mile) (183A PHIII Asset)A#1	\$ 40.00	\$ 2,120.00
53	Pavement Markings Inventory (lane mile)(183A PHIII Asset) A#1	\$ 30.00	\$ 1,590.00
36	Sign & Support Inventory with Condition (lane mile)(183A PHIII Asset) A#1	\$ 60.00	\$ 2,160.00
36	Street Lights (Illuminated Structures) Inventory (lane mile)(183A PHIII Asset) A#1	\$ 30.00	\$ 1,080.00
36	Retaining Walls Inventory (lane mile)(183A PHIII Asset) A#1	\$ 40.00	\$ 1,440.00
36	Curb and Gutter Inventory (lane mile)(183A PHIII Asset) A#1	\$ 45.00	\$ 1,620.00
184	Curb and Gutter Inventory (lane mile) - (DTS data) A#1	\$ 45.00	\$ 8,280.00
	*Based on 100% coverage of lanes driven		
	**Assumes Client will import database into PMS software		
Total From Other Sheets, If Any:			
H2O/RAS will bill lump sum based on percent complete for each task item			Subtotal A: \$ 34,696.00

B. Unpublished Options, Accessory or Service items - Itemize Below - Attach Additional Sheet If Necessary

(Note: Unpublished Items are any which were not submitted and priced in contractor's bid.)

Quan	Description	Unit Pr	Total
36	Attenuators Inventory (lane mile) (183A PHIII Asset) A#1	\$ 30.00	\$ 1,080.00
36	Delineators/Object Markers Inventory (lane mile)(183A PHIII Asset) A#1	\$ 30.00	\$ 1,080.00
Total From Other Sheets, If Any:			
Subtotal B:			\$ 2,160.00
Check: Total cost of Unpublished Options (B) cannot exceed 25% of the total of the Base Unit Price plus Published Options (A+B).		For this transaction the percentage is:	6%

C. Other Allowances, Discounts, Trade-Ins, Freight, Make Ready or Miscellaneous Charges

Subtotal C:			\$ -

Delivery Date:
D. Total Purchase Price (A+B+C): \$ 36,856.00

H-GAC

Houston-Galveston Area Council

P.O. Box 22777 · 3555 Timmons · Houston, Texas 77227-2777

Cooperative Agreement - Contract - H2O Partners, Inc. - Public Services - ID: 7252

MASTER GENERAL PROVISIONS

This Master Agreement is made and entered into, by and between the Houston-Galveston Area Council hereinafter referred to as H-GAC having its principal place of business at 3555 Timmons Lane, Suite 120, Houston, Texas 77027 and H2O Partners, Inc., hereinafter referred to as the Contractor, having its principal place of business at 260 Addie Roy Road, Suite 150, Austin, TX 78746.

WITNESSETH:

WHEREAS, H-GAC hereby engages the Contractor to perform certain services in accordance with the specifications of the Master Agreement; and

WHEREAS, the Contractor has agreed to perform such services in accordance with the specifications of the Master Agreement;

NOW, THEREFORE, H-GAC and the Contractor do hereby agree as follows:

ARTICLE 1: LEGAL AUTHORITY

The Contractor warrants and assures H-GAC that it possesses adequate legal authority to enter into this Master Agreement. The Contractor's governing body, where applicable, has authorized the signatory official(s) to enter into this Master Agreement and bind the Contractor to the terms of this Master Agreement and any subsequent amendments hereto.

ARTICLE 2: APPLICABLE LAWS

The Contractor agrees to conduct all activities under this Master Agreement in accordance with all federal laws, executive orders, policies, procedures, applicable rules, regulations, directives, standards, ordinances, and laws, in effect or promulgated during the term of this Master Agreement, including without limitation, workers' compensation laws, minimum and maximum salary and wage statutes and regulations, and licensing laws and regulations. When required, the Contractor shall furnish H-GAC with satisfactory proof of its compliance therewith.

ARTICLE 3: PUBLIC INFORMATION

Except as stated below, all materials submitted to H-GAC, including any attachments, appendices, or other information submitted as a part of a submission or Master Agreement, are considered public information, and become the property of H-GAC upon submission and may be reprinted, published, or distributed in any manner by H-GAC according to open records laws, requirements of the US Department of Labor and the State of Texas, and H-GAC policies and procedures. In the event the Contractor wishes to claim portions of the response are not subject to the Texas Public Information Act, it shall so; however, the determination of the Texas Attorney General as to whether such information must be disclosed upon a public request shall be binding on the Contractor. H-GAC will request such a determination only if Contractor bears all costs for preparation of the submission. H-GAC is not responsible for the return of creative examples of work submitted. H-GAC will not be held accountable if material from submissions is obtained without the written consent of the contractor by parties other than H-GAC, at any time during the evaluation process.

ARTICLE 4: INDEPENDENT CONTRACTOR

The execution of this Master Agreement and the rendering of services prescribed by this Master Agreement do not change the independent status of H-GAC or the Contractor. No provision of this Master Agreement or act of H-GAC in performance of the Master Agreement shall be construed as making the Contractor the agent, servant, or employee of H-GAC, the State of Texas, or the United States Government. Employees of the Contractor are subject to the exclusive control and supervision of the Contractor. The Contractor is solely responsible for employee related disputes and discrepancies, including employee payrolls and any claims arising therefrom.

ARTICLE 5: ANTI-COMPETITIVE BEHAVIOR

Contractor will not collude, in any manner, or engage in any practice which may restrict or eliminate competition or otherwise restrain trade.

ARTICLE 6: SUSPENSION AND DEBARMENT

Debarment and Suspension (Executive Orders 12549 and 12689) – A contract award (2 CFR 180.220) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3 CFR Part 1989 Comp. p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Pursuant to the Federal Rule above, Respondent certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency or by the State of Texas and at all times during the term of the Contract neither it nor its principals will be debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency or by the State of Texas Respondent shall immediately provide the written notice to H-GAC if at any time the Respondent learns that this certification was erroneous when submitted or has become erroneous by reason of changed circumstances. H-GAC may rely upon a certification of the Respondent that the Respondent is not debarred, suspended, ineligible, or voluntarily excluded from the covered contract, unless the H-GAC knows the certification is erroneous.

ARTICLE 7: GOAL FOR CONTRACTING WITH SMALL AND MINORITY BUSINESSES, WOMEN’S BUSINESS ENTERPRISES, AND LABOR SURPLUS AREA FIRMS (if subcontracts are to be let)

H-GAC’s goal is to assure that small and minority businesses, women’s business enterprises, and labor surplus area firms are used when possible in providing services under a contract. In accordance with federal procurements requirements of 2 CFR §200.321, if subcontracts are to be let, the prime contractor must take the affirmative steps listed below:

1. Placing qualified small and minority businesses and women’s business enterprises on solicitation lists;
2. Assuring that small and minority businesses and women’s business enterprises are solicited whenever they are potential sources;
3. Dividing total requirements, when economically feasible, into smaller task or quantities to permit maximum participation by small and minority businesses, and women’s business enterprises;
4. Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women’s business enterprises;
5. Using the services and assistance as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce.
- 6.

Nothing in this provision will be construed to require the utilization of any firm that is either unqualified or unavailable. The Small Business Administration (SBA) is the primary reference and database for information on requirements related to Federal Subcontracting <https://www.sba.gov/federal-contracting/contracting-guide/prime-subcontracting>

NOTE: The term DBE as used in this solicitation is understood to encompass all programs/business enterprises

such as: Small Disadvantaged Business (SDB), Historically Underutilized Business (HUB), Minority Owned Business Enterprise (MBE), Women Owned Business Enterprise (WBE) and Disabled Veteran Business Enterprise (DVBE) or other designation as issued by a certifying agency.

Contractor agrees to work with and assist HGACBuy customer in meeting any DBE targets and goals, as may be required by any rules, processes, or programs they might have in place. Assistance may include compliance with reporting requirements, provision of documentation, consideration of Certified/Listed subcontractors, provision of documented evidence that an active participatory role for a DBE entity was considered in a procurement transaction, etc.

ARTICLE 8: SCOPE OF SERVICES

The services to be performed by the Contractor are outlined in an Attachment to this Master Agreement.

ARTICLE 9: PERFORMANCE PERIOD

This Master Agreement shall be performed during the period which begins Aug 01 2021 and ends Jul 31 2023. All services under this Master Agreement must be rendered within this performance period, unless directly specified under a written change or extension provisioned under Article 21, which shall be fully executed by both parties to this Master Agreement.

ARTICLE 10: PAYMENT OR FUNDING

Payment provisions under this Master Agreement are outlined in the Special Provisions. H-GAC will not pay for any expenses incurred prior to the execution date of a contract, or any expenses incurred after the termination date of the contract.

ARTICLE 11: PAYMENT FOR WORK

The H-GAC Customer is responsible for making payment to the Contractor upon delivery and acceptance of the goods or completion of the services and submission of the subsequent invoice.

ARTICLE 12: PAYMENT TERMS/PRE-PAYMENT/QUANTITY DISCOUNTS

If discounts for accelerated payment, pre-payment, progress payment, or quantity discounts are offered, they must be clearly indicated in the Contractor's submission prior to contract award. The applicability or acceptance of these terms is at the discretion of the Customer.

ARTICLE 13: REPORTING REQUIREMENTS

If the Contractor fails to submit to H-GAC in a timely and satisfactory manner any report required by this Master Agreement, or otherwise fails to satisfactorily render performances hereunder, H-GAC may terminate this Master Agreement with notice as identified in Article 29 of these General Provisions. H-GAC has final determination of the adequacy of performance and reporting by Contractor. Termination of this Master Agreement for failure to perform may affect Contractor's ability to participate in future opportunities with H-GAC. The Contractor's failure to timely submit any report may also be considered cause for termination of this Master Agreement. Any additional reporting requirements shall be set forth in the Special Provisions of this Master Agreement.

ARTICLE 14: INSURANCE

Contractor shall maintain insurance coverage for work performed or services rendered under this Master Agreement as outlined and defined in the attached Special Provisions.

ARTICLE 15: SUBCONTRACTS AND ASSIGNMENTS

Except as may be set forth in the Special Provisions, the Contractor agrees not to assign, transfer, convey, sublet, or otherwise dispose of this Master Agreement or any right, title, obligation, or interest it may have therein to any third party without prior written approval of H-GAC. The Contractor acknowledges that H-GAC is not liable to any subcontractor or assignee of the Contractor. The Contractor shall ensure that the performance rendered under

all subcontracts shall result in compliance with all the terms and provisions of this Master Agreement as if the performance rendered was rendered by the Contractor. Contractor shall give all required notices, and comply with all laws and regulations applicable to furnishing and performance of the work. Except where otherwise expressly required by applicable law or regulation, H-GAC shall not be responsible for monitoring Contractor's compliance, or that of Contractor's subcontractors, with any laws or regulations.

ARTICLE 16: AUDIT

Notwithstanding any other audit requirement, H-GAC reserves the right to conduct or cause to be conducted an independent audit of any transaction under this Master Agreement, such audit may be performed by the H-GAC local government audit staff, a certified public accountant firm, or other auditors designated by H-GAC and will be conducted in accordance with applicable professional standards and practices. The Contractor understands and agrees that the Contractor shall be liable to the H-GAC for any findings that result in monetary obligations to H-GAC.

ARTICLE 17: TAX EXEMPT STATUS

H-GAC and Customer members are either units of government or qualified non-profit agencies, and are generally exempt from Federal and State sales, excise or use taxes. Respondent must not include taxes in its Response. It is the responsibility of Contractor to determine the applicability of any taxes to an order and act accordingly. Exemption certificates will be provided upon request.

ARTICLE 18: EXAMINATION OF RECORDS

The Contractor shall maintain during the course of the work complete and accurate records of all of the Contractor's costs and documentation of items which are chargeable to H-GAC under this Master Agreement. H-GAC, through its staff or designated public accounting firm, the State of Texas, and United States Government, shall have the right at any reasonable time to inspect, copy and audit those records on or off the premises by authorized representatives of its own or any public accounting firm selected by H-GAC. The right of access to records is not limited to the required retention period, but shall last as long as the records are retained. Failure to provide access to records may be cause for termination of the Master Agreement. The records to be thus maintained and retained by the Contractor shall include (without limitation): (1) personnel and payroll records, including social security numbers and labor classifications, accounting for total time distribution of the Contractor's employees working full or part time on the work, as well as cancelled payroll checks, signed receipts for payroll payments in cash, or other evidence of disbursement of payroll payments; (2) invoices for purchases, receiving and issuing documents, and all other unit inventory records for the Contractor's stocks or capital items; and (3) paid invoices and cancelled checks for materials purchased and for subcontractors' and any other third parties' charges.

Contractor agrees that H-GAC will have the right, with reasonable notice, to inspect its records pertaining to purchase orders processed and the accuracy of the fees payable to H-GAC. The Contractor further agrees that the examination of records outlined in this article shall be included in all subcontractor or third-party Master Agreements.

ARTICLE 19: RETENTION OF RECORDS

The Contractor and its subcontractors shall maintain all records pertinent to this Master Agreement, and all other financial, statistical, property, participant records, and supporting documentation for a period of no less than seven (7) years from the later of the date of acceptance of the final payment or until all audit findings have been resolved. If any litigation, claim, negotiation, audit or other action involving the records has been started before the expiration of the retention period, the records shall be retained until completion of the action and resolution of all issues which arise from it, or until the end of the seven (7) years, whichever is later, and until any outstanding litigation, audit, or claim has been fully resolved.

ARTICLE 20: DISTRIBUTORS, VENDORS, RESELLERS

Contractor agrees and acknowledges that any such designations of distributors, vendors, resellers or the like are for the convenience of the Contractor only and the awarded Contractor will remain responsible and liable for all obligations under the Contract and the performance of any designated distributor, vendor, reseller, etc. Contractor is also responsible for receiving and processing any Customer purchase order in accordance with the Contract and forwarding of the Purchase Order to the designated distributor, vendor, reseller, etc. to complete the sale or service. H-GAC reserves the right to reject any entity acting on the Contractor's behalf or refuse to add entities after a contract is awarded.

ARTICLE 21: CHANGE ORDERS AND AMENDMENTS

- A. Any alterations, additions, or deletions to the terms of this Master Agreement, which are required by changes in federal or state law or by regulations, are automatically incorporated without written amendment hereto, and shall become effective on the date designated by such law or by regulation.
- B. To ensure the legal and effective performance of this Master Agreement, both parties agree that any amendment that affects the performance under this Master Agreement must be mutually agreed upon and that all such amendments must be in writing. After a period of no less than 30 days subsequent to written notice, unless sooner implementation is required by law, such amendments shall have the effect of qualifying the terms of this Master Agreement and shall be binding upon the parties as if written herein.
- C. Customers have the right to issue a change order to any purchase orders issued to the Contractor for the purposes of clarification or inclusion of additional specifications, qualifications, conditions, etc. The change order must be in writing and agreed upon by Contractor and the Customer agency prior to issuance of any Change Order. A copy of the Change Order must be provided by the Contractor to, and acknowledged by, H-GAC.

ARTICLE 22: CONTRACT ITEM CHANGES

- A. If a manufacturer discontinues a contracted item, that item will automatically be considered deleted from the contract with no penalty to Contractor. However, H-GAC may at its sole discretion elect to make a contract award to the next lowest Respondent for the item, or take any other action deemed by H-GAC, at its sole discretion, to be in the best interests of its Customers.
- B. If a manufacturer makes any kind of change in a contracted item which affects the contract price, Contractor must advise H-GAC of the details. H-GAC may allow or reject the change at its sole discretion. If the change is rejected, H-GAC will remove the item from its program and there will be no penalty to Contractor. However, H-GAC may at its sole discretion elect to make a contract award to the next lowest Respondent for the item, or take any other action deemed by H-GAC, at its sole discretion, to be in the best interests of its Customers.
- C. If a manufacturer makes any change in a contracted item which does not affect the contract price, Contractor shall advise H-GAC of the details. If the 'new' item is equal to or better than the originally contracted item, the 'new' item shall be approved as a replacement. If the change is rejected H-GAC will remove the item from its program and there will be no penalty to Contractor. However, H-GAC may at its sole discretion elect to make a contract award to the next lowest Respondent for the item or may take any other action deemed by H-GAC at its sole discretion, to be in the best interests of its Customers.
- D. In the case of specifically identified catalogs or price sheets which have been contracted as base bid items or as published options, routine published changes to products and pricing will be automatically incorporated into the contract. However, Contractor must still provide thirty (30) calendar days written

notice and an explanation of the changes to products and pricing. H-GAC will respond with written approval.

ARTICLE 23: CONTRACT PRICE ADJUSTMENTS

Price Decreases

If Contractor's Direct Cost decreases at any time during the full term of this award, Contractor must immediately pass the decrease on to H-GAC and lower its prices by the amount of the decrease in Direct Cost. (Direct Cost means Contractor's cost from the manufacturer of any item or if Contractor is the manufacturer, the cost of raw materials required to manufacture the item, plus costs of transportation from manufacturer to Contractor and Contractor to H-GAC. Contractor must notify H-GAC of price decreases in the same way as for price increases set out below. The price decrease shall become effective upon H-GAC's receipt of Contractor's notice. If Contractor routinely offers discounted contract pricing, H-GAC may request Contractor accept amended contract pricing equivalent to the routinely discounted pricing

Price Increases

Contractors may request a price increase for items priced as Base Bid items and Published Options after twelve (12) months from the bid opening date of the bid received by H-GAC. The amount of any increase will not exceed actual documented increase in Contractor's Direct Cost and will not exceed 10% of the previous bid price. Considerations on the percentage limit will be given if the price increase is the result of increased tariff charges, or other economic factors.

Price Changes

Any permanent increase or decrease in offered pricing for a base contract item or published option is considered a price change. Temporary increases in pricing by whatever name (e.g. 'surcharge', 'adjustment', 'equalization charge', 'compliance charge', 'recovery charge', etc.), are also considered to be price changes. For published catalogs and price sheets as part of an H-GAC contract, requests to amend the contract to reflect any new published catalog or price sheet must be submitted whenever the manufacturer publishes a new document. The request must include the new catalog or price sheet.

All Products shall, at time of sale, be equipped as required under any then current applicable local, state, and federal government requirements. If, during the course of any contract, changes are made to any government requirements which cause a manufacturer's costs of production to increase, Contractor may increase pricing to the extent of Contractor's actual cost increase. The increase must be substantiated with support documentation acceptable to H-GAC prior to taking effect. Modifications to a Product required to comply with such requirements which become effective after the date of any sale are the responsibility of the Customer.

Requesting Price Increase/Required Documentation

Contractor must submit a written notification at least thirty (30) calendar days prior to the requested effective date of the change, setting the amount of the increase, along with an itemized list of any increased prices, showing the Contractor's current price, revised price, the actual dollar difference and the percentage of the price increase by line item. Price change requests must include H-GAC Forms D Offered Item Pricing and E Options Pricing, or the documentation used to submit pricing in the original Response and be supported with substantive documentation (e.g. manufacturer's price increase notices, copies of invoices from suppliers, etc.) clearly showing that Contractor's actual costs have increased per the applicable line-item bid. The Producer Price Index (PPI) may be used as partial justification, subject to approval by H-GAC, but no price increase based solely on an increase in the PPI will be allowed. This documentation should be submitted in Excel format to facilitate analysis and updating of the website. The letter and documentation must be sent to the Bids and Specifications manager, William Burton, at William.Burton@h-gac.com

Review/Approval of Requests

If H-GAC approves the price increase, Contractor will be notified in writing; no price increase will be effective until Contractor receives this notice. If H-GAC does not approve Contractor's price increase, Contractor may terminate its performance upon sixty (60) days advance written notice to H-GAC, however Contractor must fulfill any outstanding Purchase Orders. Termination of performance is Contractor's only remedy if H-GAC does not approve the price increase. H-GAC reserves the right to accept or reject any price change request.

ARTICLE 24: DELIVERIES AND SHIPPING TERMS

The Contractor agrees to make deliveries only upon receipt of authorized Customer Purchase Order acknowledged by H-GAC. Delivery made without such Purchase Order will be at Contractor's risk and will leave H-GAC the option of canceling any contract awarded to the Contractor. The Contractor must secure and deliver any item within five (5) working days, or as agreed to on any corresponding customer Purchase Order.

Shipping must be Freight On Board Destination to the delivery location designated on the Customer purchase order. The Contractor will retain title and control of all goods until delivery is completed and the Customer has accepted the delivery. All risk of transportation and all related charges are the responsibility of the Contractor. The Customer will notify the Contractor and H-GAC promptly of any damaged goods and will assist the Contractor in arranging for inspection. The Contractor must file all claims for visible or concealed damage. Unless otherwise stated in the Master Agreement, deliveries must consist only of new and unused merchandise.

ARTICLE 25: RESTOCKING (EXCHANGES AND RETURNS)

There will be no restocking charge to the Customer for return or exchange of any item purchased under the terms of any award. If the Customer wishes to return items purchased under an awarded contract, the Contractor agrees to exchange, these items for other items, with no additional charge incurred. Items must be returned to Contractor within thirty (30) days from date of delivery. If there is a difference in price in the items exchanged, the Contractor must notify H-GAC and invoice Customer for increase price or provide the Customer with a credit or refund for any decrease in price per Customer's preference. On items returned, a credit or cash refund will be issued by the Contractor to Customer. This return and exchange option will extend for thirty (30) days following the expiration of the term of the Contract. All items returned by the Customer must be unused and in the same merchantable condition as when received. Items that are special ordered may be returned only upon approval of the Contractor.

ARTICLE 26: MANUALS

Each product delivered under contract to any Customer must be delivered with at least one (1) copy of a safety and operating manual and any other technical or maintenance manual. The cost of the manual(s) must be included in the price for the Product offered.

ARTICLE 27: OUT OF STOCK, PRODUCT RECALLS, AND DISCONTINUED PRODUCTS

H-GAC does NOT purchase the products sold pursuant to a Solicitation or Master Agreement. Contractor is responsible for ensuring that notices and mailings, such as Out of Stock or Discontinued Notices, Safety Alerts, Safety Recall Notices, and customer surveys, are sent directly to the Customer with a copy sent to H-GAC. Customer will have the option of accepting any equivalent product or canceling the item from Customer's Purchase Order. Contractor is not authorized to make substitutions without prior approval.

ARTICLE 28: WARRANTIES, SALES, AND SERVICE

Warranties must be the manufacturer's standard and inclusive of any other warranty requirements stated in the Master Agreement; any warranties offered by a dealer will be in addition to the manufacturer's standard warranty and will not be a substitute for such. Pricing for any product must be inclusive of the standard warranty.

Contractor is responsible for the execution and effectiveness of all product warranty requests and any claims, Contractor agrees to respond directly to correct warranty claims and to ensure reconciliation of warranty claims that have been assigned to a third party.

ARTICLE 29: TERMINATION PROCEDURES

The Contractor acknowledges that this Master Agreement may be terminated for Convenience or Default. H-GAC will not pay for any expenses incurred after the termination date of the contract.

A. *Convenience*

H-GAC may terminate this Master Agreement at any time, in whole or in part, with or without cause, whenever H-GAC determines that for any reason such termination is in the best interest of H-GAC, by providing written notice by certified mail to the Contractor. Upon receipt of notice of termination, all services hereunder of the Contractor and its employees and subcontractors shall cease to the extent specified in the notice of termination.

The Contractor may cancel or terminate this Master Agreement upon submission of thirty (30) days written notice, presented to H-GAC via certified mail. The Contractor may not give notice of cancellation after it has received notice of default from H-GAC.

B. *Default*

H-GAC may, by written notice of default to the Contractor, terminate the whole or any part of the Master Agreement, in any one of the following circumstances:

- (1) If the Contractor fails to perform the services herein specified within the time specified herein or any extension thereof; or
- (2) If the Contractor fails to perform any of the other provisions of this Master Agreement for any reason whatsoever, or so fails to make progress or otherwise violates the Master Agreements that completion of services herein specified within the Master Agreement term is significantly endangered, and in either of these two instances does not cure such failure within a period often (10) days (or such longer period of time as may be authorized by H-GAC in writing) after receiving written notice by certified mail of default from H-GAC.
- (3) In the event of such termination, Contractor will notify H-GAC of any outstanding Purchase Orders and H-GAC will consult with the End User and notify the Contractor to what extent the End User wishes the Contractor to complete the Purchase Order. If Contractor is unable to do so, Contractor may be subject to a claim for damages from H-GAC and/or the End User.

ARTICLE 30: SEVERABILITY

H-GAC and Contractor agree that should any provision of this Master Agreement be determined to be invalid or unenforceable, such determination shall not affect any other term of this Master Agreement, which shall continue in full force and effect.

ARTICLE 31: FORCE MAJEURE

To the extent that either party to this Master Agreement shall be wholly or partially prevented from the performance of any obligation or duty placed on such party by reason of or through strikes, stoppage of labor, riot, fire, flood, acts of war, insurrection, accident, order of any court, act of God, or specific cause reasonably beyond the party's control and not attributable to its neglect or nonfeasance, in such event, the time for the performance of such obligation or duty shall be suspended until such disability to perform is removed. Determination of force majeure shall rest solely with H-GAC.

ARTICLE 32: CONFLICT OF INTEREST

No officer, member or employee of the Contractor or Contractors subcontractor, no member of the governing body of the Contractor, and no other public officials of the Contractor who exercise any functions or responsibilities in the review or Contractor approval of this Master Agreement, shall participate in any decision relating to this Master Agreement which affects his or her personal interest, or shall have any personal or pecuniary interest, direct or indirect, in this Master Agreement.

- A. **Conflict of Interest Questionnaire:** Chapter 176 of the Texas Local Government Code requires contractors contracting or seeking to contract with H-GAC to file a conflict-of-interest questionnaire (CIQ) if they have an employment or other business relationship with an H-GAC officer or an officer's close family member. The required questionnaire and instructions are located on the H-GAC website or at the Texas Ethics Commission website <https://www.ethics.state.tx.us/forms/CIQ.pdf>. H-GAC officers include its Board of Directors and Executive Director, who are listed on this website. Respondent must complete and file a CIQ with the Texas Ethics Commission if an employment or business relationship with H-GAC office or an officer's close family member as defined in the law exists.
- B. **Certificate of Interested Parties Form – Form 1295:** As required by Section 2252.908 of the Texas Government Code. H-GAC will not enter a Contract with Contractor unless (i) the Contractor submits a disclosure of interested parties form to H-GAC at the time the Contractor submits the contract H-GAC, or (ii) the Contractor is exempt from such requirement. The required form and instructions are located at the Texas Ethics Commission website https://www.ethics.state.tx.us/whatsnew/elf_info_form1295.htm. Respondents who are awarded a Contract must submit their Form 1295 with the signed Contract to H-GAC.

ARTICLE 33: FEDERAL COMPLIANCE

Contractor agrees to comply with all federal statutes relating to nondiscrimination, labor standards, and environmental compliance. With regards to "Rights to Inventions Made Under a Contract or Master Agreement," If the Federal award meets the definition of "funding Master Agreement" under 37 CFR § 401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding Master Agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Master Agreements," and any implementing regulations issued by the awarding agency. Contractor agrees to be wholly compliant with the provisions of 2 CFR 200, Appendix II. Additionally, for work to be performed under the Master Agreement or subcontract thereof, including procurement of materials or leases of equipment, Contractor shall notify each potential subcontractor or supplier of the Contractor's federal compliance obligations. These may include, but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§ 1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) the Fair Labor Standards Act of 1938 (29 USC 676 et. seq.), (d) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794), which prohibits discrimination on the basis of handicaps and the Americans with Disabilities Act of 1990; (e) the Age Discrimination in Employment Act of 1967 (29 USC 621 et. seq.) and the Age Discrimination Act of 1974, as amended (42 U.S.C. §§ 6101-6107), which prohibits discrimination on the basis of age; (f) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (g) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to the nondiscrimination on the basis of alcohol abuse or alcoholism; (h) §§ 523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. 290 dd-3 and 290 ee-3), as amended, relating to confidentiality of alcohol and drug abuse patient records; (i) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. § 3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (j) any other nondiscrimination provisions in any specific statute(s) applicable to any Federal funding for this Master Agreement; (k) the requirements of any other nondiscrimination statute(s) which may apply to this Master Agreement; (l) applicable provisions of the Clean Air Act (42 U.S.C. §7401 et seq.), the Federal Water Pollution Control Act, as amended (33 U.S.C. §1251 et seq.), Section 508 of the Clean Water Act (33 U.S.C. 1368), Executive Order 11738, and the Environmental Protection Agency regulations at 40 CFR Part 15; (m) applicable provisions of the Davis- Bacon Act (40 U.S.C. 276a - 276a-7), the Copeland Act (40 U.S.C. 276c), and the Contract Work Hours and Safety Standards Act (40 U.S.C. 327-332), as set forth in Department of Labor Regulations at 20 CFR 5.5a; (n) the mandatory standards and policies relating to energy efficiency which are

contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (P.L. 94-163).

ARTICLE 34: PROHIBITION ON CONTRACTING WITH ENTITIES USING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE EQUIPMENT (EFFECTIVE AUG. 13, 2020 AND AS AMENDED OCTOBER 26, 2020)

Pursuant to 2 CFR 200.216, Contractor shall not offer equipment, services, or system that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Covered telecommunications equipment or services means 1) telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities); 2) for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities); 3) telecommunications or video surveillance services provided by such entities or using such equipment; or 4) telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country. Respondent must comply with requirements for certifications. The provision at 48 C.F.R Section 52.204-26 requires that offerors review SAM prior to completing their required representations. This rule applies to all acquisitions, including acquisitions at or below the simplified acquisition threshold and to acquisitions of commercial items, including commercially available off the-shelf items.

ARTICLE 35: DOMESTIC PREFERENCE

In accordance with 2 CFR 200.322, as appropriate and to the extent consistent with law, when using federal grant award funds H-GAC should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). H-GAC must include this requirement in all subawards including all contracts and purchase orders for work or products under the federal grant award. If Contractor intends to qualify for Purchase Orders using federal grant money, then it shall work with H-GAC to provide all required certifications and other documentation needed to show compliance.

ARTICLE 36: CRIMINAL PROVISIONS AND SANCTIONS

The Contractor agrees to perform the Master Agreement in conformance with safeguards against fraud and abuse as set forth by the H-GAC, the State of Texas, and the acts and regulations of any related state or federal agency. The Contractor agrees to promptly notify H-GAC of any actual or suspected fraud, abuse, or other criminal activity through the filing of a written report within twenty-four (24) hours of knowledge thereof. Contractor shall notify H-GAC of any accident or incident requiring medical attention arising from its activities under this Master Agreement within twenty-four (24) hours of such occurrence. Theft or willful damage to property on loan to the Contractor from H-GAC, if any, shall be reported to local law enforcement agencies and H-GAC within two (2) hours of discovery of any such act.

The Contractor further agrees to cooperate fully with H-GAC, local law enforcement agencies, the State of Texas, the Federal Bureau of Investigation, and any other duly authorized investigative unit, in carrying out a full investigation of all such incidents.

The Contractor shall notify H-GAC of the threat of lawsuit or of any actual suit filed against the Contractor pertaining to this Master Agreement or which would adversely affect the Contractor's ability to perform services under this Master Agreement.

ARTICLE 37: INDEMNIFICATION AND RECOVERY

H-GAC's liability under this Master Agreement, whether for breach of contract, warranty, negligence, strict liability, in tort or otherwise, is limited to its order processing charge. In no event will H-GAC be liable for any loss of use, loss of time, inconvenience, commercial loss, lost profits, or savings or other incidental, special or consequential damages to the full extent such use may be disclaimed by law. Contractor agrees, to the extent permitted by law, to defend and hold harmless H-GAC, its board members, officers, agents, officials, employees, and indemnities from any and all claims, costs, expenses (including reasonable attorney fees), actions, causes of action, judgements, and liens arising as a result of Contractor's negligent act or omission under this Master Agreement. Contractor shall notify H-GAC of the threat of lawsuit or of any actual suit filed against Contractor relating to this Master Agreement.

ARTICLE 38: LIMITATION OF CONTRACTOR'S LIABILITY

Except as specified in any separate writing between the Contractor and an END USER, Contractor's total liability under this Master Agreement, whether for breach of contract, warranty, negligence, strict liability, in tort or otherwise, but excluding its obligation to indemnify H-GAC, is limited to the price of the particular products/services sold hereunder, and Contractor agrees either to refund the purchase price or to repair or replace product(s) that are not as warranted. In no event will Contractor be liable for any loss of use, loss of time, inconvenience, commercial loss, loss of profits or savings or other incidental, special or consequential damages to the full extent such use may be disclaimed by law. Contractor understands and agrees that it shall be liable to repay and shall repay upon demand to END USER any amounts determined by H-GAC, its independent auditors, or any agency of State or Federal government to have been paid in violation of the terms of this Master Agreement.

ARTICLE 39: TITLES NOT RESTRICTIVE

The titles assigned to the various Articles of this Master Agreement are for convenience only. Titles shall not be considered restrictive of the subject matter of any Article, or part of this Master Agreement.

ARTICLE 40: JOINT WORK PRODUCT

This Master Agreement is the joint work product of H-GAC and the Contractor. This Master Agreement has been negotiated by H-GAC and the Contractor and their respective counsel and shall be fairly interpreted in accordance with its terms and, in the event of any ambiguities, no inferences shall be drawn against any party.

ARTICLE 41: PROCUREMENT OF RECOVERED MATERIAL

H-GAC and the Respondent must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include: (1) procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; (2) procuring solid waste management services in a manner that maximizes energy and resource recovery; and (3) establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines. Pursuant to the Federal Rule above, as required by the Resource Conservation and Recovery Act of 1976 (42 U.S.C. § 6962(c)(3)(A)(i)), Respondent certifies that the percentage of recovered materials content for EPA-designated items to be delivered or used in the performance of the Contract will be at least the amount required by the applicable contract specifications or other contractual requirements.

ARTICLE 42: COPELAND "ANTI-KICKBACK" ACT

Contractor shall comply with 18 U.S.C. § 874, 40 U.S.C. § 3145, and the requirements of 29 C.F.R. pt. 3 as may be applicable, which are incorporated by reference into the contract. The contractor or subcontractor shall insert in any subcontracts the clause above and such other clauses as appropriate agency instructions require, and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for the compliance by any subcontractor or lower tier subcontractor with all of these contract

clauses. A breach of the contract clauses above may be grounds for termination of the Contract, and for debarment as a contractor and subcontractor as provided in 29 C.F.R. § 5.12.

ARTICLE 43: DISCRIMINATION

Respondent and any potential subcontractors shall comply with all Federal statutes relating to nondiscrimination. These include, but are not limited to:

- a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352), which prohibits discrimination on the basis of race, color, or national origin;
- b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex;
- c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps;
- d) The Age Discrimination Act of 1975, as amended (42 U.S.C. §§6101- 6107), which prohibits discrimination on the basis of age;
- e) The Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse;
- f) The Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism;
- g) Sections 523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee-3), as amended, relating to confidentiality of alcohol and drug abuse patient records;
- h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental, or financing of housing;
- i) Any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and
- j) The requirements of any other nondiscrimination statute(s) that may apply to the application.

ARTICLE 44: DRUG FREE WORKPLACE

Contractor must provide a drug-free workplace in accordance with the Drug-Free Workplace Act, as applicable. For the purposes of this Section, “drug-free” means a worksite at which employees are prohibited from engaging in the unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance. H-GAC may request a copy of this policy.

ARTICLE 45: APPLICABILITY TO SUBCONTRACTORS

Respondent agrees that all contracts it awards pursuant to the contract awarded as a result of this Master Agreement will be bound by the foregoing terms and conditions.

ARTICLE 46: WARRANTY AND COPYRIGHT

Submissions must include all warranty information, including items covered, items excluded, duration, and renewability. Submissions must include proof of licensing if using third party code for programming.

ARTICLE 47: DATA HANDLING AND SECURITY

It will always be the responsibility of the selected Contractor to manage data transfer and to secure all data appropriately during the project to prevent unauthorized access to all data, products, and deliverables.

ARTICLE 48: DISPUTES

All disputes concerning questions of fact or of law arising under this Master Agreement, which are not addressed within the Whole Master Agreement as defined pursuant to Article 4 hereof, shall be decided by the Executive Director of H-GAC or his designee, who shall reduce his decision to writing and provide notice thereof to the Contractor. The decision of the Executive Director or his designee shall be final and conclusive unless, within

thirty (30) days from the date of receipt of such notice, the Contractor requests a rehearing from the Executive Director of H-GAC. In connection with any rehearing under this Article, the Contractor shall be afforded an opportunity to be heard and offer evidence in support of its position. The decision of the Executive Director after any such rehearing shall be final and conclusive. The Contractor may, if it elects to do so, appeal the final and conclusive decision of the Executive Director to a court of competent jurisdiction. Pending final decision of a dispute hereunder, the Contractor shall proceed diligently with the performance of the Master Agreement and in accordance with H-GAC's final decision.

ARTICLE 49: CHOICE OF LAW: VENUE

This Master Agreement shall be governed by the laws of the State of Texas. Venue and jurisdiction of any suit or cause of action arising under or in connection with the Master Agreement shall lie exclusively in Harris County, Texas. Disputes between END USER and Contractor are to be resolved in accordance with the law and venue rules of the state of purchase. Contractor shall immediately notify H-GAC of such disputes.

ARTICLE 50: ORDER OF PRIORITY

In the case of any conflict between or within this Master Agreement, the following order of priority shall be utilized: 1) General Provisions, 2) Special Provisions, 3) Scope of Work, and 4) Other Attachments.

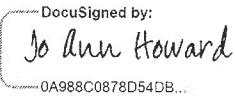
ARTICLE 51: WHOLE MASTER AGREEMENT

Please note, this is an H-GAC Master Agreement template and is used for all products and services offered in H-GAC Cooperative Purchasing. Any redlines to this Master Agreement may not be reviewed. If this Master Agreement has not been signed by the Contractor within 30 calendar days, this Master Agreement will be automatically voided. The Master General Provisions, Master Special Provisions, and Attachments, as provided herein, constitute the complete Master Agreement between the parties hereto, and supersede any and all oral and written Master Agreements between the parties relating to matters herein. Except as otherwise provided herein, this Master Agreement cannot be modified without written consent of the parties.

SIGNATURES:

H-GAC and the Contractor have read, agreed, and executed the whole Master Agreement as of the date first written above, as accepted by:

H2O Partners, Inc.

Signature  DocuSigned by:
0A988C0878D54DB...

Name Jo Ann Howard

Title President

Date 8/18/2021

H-GAC

Signature  DocuSigned by:
82EC270D5D61423...

Name Chuck Wemple

Title Executive Director

Date 8/23/2021

H-GAC

Houston-Galveston Area Council

P.O. Box 22777 · 3555 Timmons · Houston, Texas 77227-2777

Cooperative Agreement - Contract - H2O Partners, Inc. - Public Services - 7252

MASTER SPECIAL PROVISIONS

Please note, this is an H-GAC Master Agreement template and is used for all products and services offered in H-GAC Cooperative Purchasing. Any redlines to this Master Agreement may not be reviewed. Incorporated by attachment, as part of the whole Master Agreement, H-GAC and the Contractor do, hereby agree to the Master Special Provisions as follows:

ARTICLE 1: BIDS/PROPOSALS INCORPORATED

In addition to the whole Master Agreement, the following documents listed in order of priority are incorporated into the Master Agreement by reference: Bid/Proposal Specifications and Contractor's Response to the Bid/Proposal.

ARTICLE 2: END USER MASTER AGREEMENTS ("EUA")

H-GAC acknowledges that the END USER may choose to enter into an End User Master Agreement ("EUA") with the Contractor through this Master Agreement, and that the term of the EUA may exceed the term of the current H-GAC Master Agreement. H-GAC's acknowledgement is not an endorsement or approval of the End User Master Agreement's terms and conditions. Contractor agrees not to offer, agree to or accept from the END USER, any terms or conditions that conflict with those in Contractor's Master Agreement with H-GAC. Contractor affirms that termination of its Master Agreement with H-GAC for any reason shall not result in the termination of any underlying EUA, which shall in each instance, continue pursuant to the EUA's stated terms and duration. Pursuant to the terms of this Master Agreement, termination of this Master Agreement will disallow the Contractor from entering into any new EUA with END USERS. Applicable H-GAC order processing charges will be due and payable to H-GAC on any EUAs, surviving termination of this Master Agreement between H-GAC and Contractor.

ARTICLE 3: MOST FAVORED CUSTOMER CLAUSE

Contractor shall provide its most favorable pricing and terms to H-GAC. If at any time during this Master Agreement, Contractor develops a regularly followed standard procedure of entering into Master Agreements with other governmental customers within the State of Texas, and offers the same or substantially the same products/services offered to H-GAC on a basis that provides prices, warranties, benefits, and or terms more favorable than those provided to H-GAC, Contractor shall notify H-GAC within ten (10) business days thereafter, and this Master Agreement shall be deemed to be automatically retroactively amended, to the effective date of Contractor's most favorable past Master Agreement with another entity. Contractor shall provide the same prices, warranties, benefits, or terms to H-GAC and its END USER as provided in its most favorable past Master Agreement. H-GAC shall have the right and option at any time to decline to accept any such change, in which case the amendment shall be deemed null and void. If Contractor claims that a more favorable price, warranty, benefit, or term that was charged or offered to another entity during the term of this Master Agreement, does not constitute more favorable treatment, than Contractor shall, within ten (10) business days, notify H-GAC in writing, setting forth the detailed reasons Contractor believes the aforesaid offer is not in fact most favored treatment. H-GAC, after due consideration of Contractor's written explanation, may decline to accept such explanation and thereupon this Master Agreement between H-GAC and Contractor shall be automatically amended, effective retroactively, to the effective date of the most favored Master Agreement, to provide the same prices, warranties, benefits, or terms to H-GAC and the END USER.

EXCEPTION: This clause shall not be applicable to prices and price adjustments offered by a bidder,

proposer or contractor, which are not within bidder's/proposer's control [example; a manufacturer's bid concession], or to any prices offered to the Federal Government and its agencies.

ARTICLE 4: PARTY LIABILITY

Contractor's total liability under this Master Agreement, whether for breach of contract, warranty, negligence, strict liability, in tort or otherwise, is limited to the price of the particular products/services sold hereunder. Contractor agrees either to refund the purchase price or to repair or replace product(s) that are not as warranted. Contractor accepts liability to repay, and shall repay upon demand to END USER, any amounts determined by H-GAC, its independent auditors, or any state or federal agency, to have been paid in violation of the terms of this Master Agreement.

ARTICLE 5: GOVERNING LAW & VENUE

Contractor and H-GAC agree that Contractor will make every reasonable effort to resolve disputes with the END USER in accord with the law and venue rules of the state of purchase. Contractor shall immediately notify H-GAC of such disputes.

ARTICLE 6: SALES AND ORDER PROCESSING CHARGE

Contractor shall sell its products to END USERS based on the pricing and terms of this Master Agreement. H-GAC will invoice Contractor for the applicable order processing charge when H-GAC receives notification of an END USER order. Contractor shall remit to H-GAC the full amount of the applicable order processing charge, after delivery of any product or service and subsequent END USER acceptance. Payment of the Order Processing Charge shall be remitted from Contractor to H-GAC, within thirty (30) calendar days or ten (10) business days after receipt of an END USER's payment, whichever comes first, notwithstanding Contractor's receipt of invoice. For sales made by Contractor based on this Master Agreement, including sales to entities without Interlocal Master Agreements, Contractor shall pay the applicable order processing charges to H-GAC. Further, Contractor agrees to encourage entities who are not members of H-GAC's Cooperative Purchasing Program to execute an H-GAC Interlocal Master Agreement. H-GAC reserves the right to take appropriate actions including, but not limited to, Master Agreement termination if Contractor fails to promptly remit the appropriate order processing charge to H-GAC. In no event shall H-GAC have any liability to Contractor for any goods or services an END USER procures from Contractor. At all times, Contractor shall remain liable to pay to H-GAC any order processing charges on any portion of the Master Agreement actually performed, and for which compensation was received by Contractor.

ARTICLE 7: LIQUIDATED DAMAGES

Contractor and H-GAC agree that Contractor shall cooperate with the END USER at the time an END USER purchase order is placed, to determine terms for any liquidated damages.

ARTICLE 8: INSURANCE

Unless otherwise stipulated in Section B of the Bid/Proposal Specifications, Contractor must have the following insurance and coverage minimums:

- a. General liability insurance with a Single Occurrence limit of at least \$1,000,000.00, and a General Aggregate limit of at least two times the Single Occurrence limit.
- b. Product liability insurance with a Single Occurrence limit of at least \$1,000,000.00, and a General Aggregate limit of at least two times the Single Occurrence limit for all Products except Automotive Fire Apparatus. For Automotive Fire Apparatus, see Section B of the Bid/Proposal Specifications.
- c. Property Damage or Destruction insurance is required for coverage of End User owned equipment while in Contractor's possession, custody, or control. The minimum Single Occurrence limit is \$500,000.00 and the General Aggregate limit must be at least two times the Single Occurrence limit. This insurance may be carried in several ways, e.g. under an Inland Marine policy, as art of Automobile coverage, or under a

Garage Keepers policy. In any event, this coverage must be specifically and clearly listed on insurance certificate(s) submitted to H-GAC.

- d. Insurance coverage shall be in effect for the length of any contract made pursuant to the Bid/Proposal, and for any extensions thereof, plus the number of days/months required to deliver any outstanding order after the close of the contract period.
- e. Original Insurance Certificates must be furnished to H-GAC on request, showing Contractor as the insured and showing coverage and limits for the insurances listed above.
- f. If any Product(s) or Service(s) will be provided by parties other than Contractor, all such parties are required to carry the minimum insurance coverages specified herein, and if requested by H-GAC, a separate insurance certificate must be submitted for each such party.
- g. H-GAC reserves the right to contact insurance underwriters to confirm policy and certificate issuance and document accuracy.

ARTICLE 9: PERFORMANCE AND PAYMENT BONDS FOR INDIVIDUAL ORDERS

H-GAC's contractual requirements DO NOT include a Performance & Payment Bond (PPB); therefore, Contractor shall offer pricing that reflects this cost savings. Contractor shall remain prepared to offer a PPB to cover any order if so requested by the END USER. Contractor shall quote a price to END USER for provision of any requested PPB, and agrees to furnish the PPB within ten business (10) days of receipt of END USER's purchase order.

ARTICLE 10: ORDER PROCESSING CHARGE

H-GAC will apply an Order Processing Charge for each sale done through the H-GAC contract, with the exception of orders for motor vehicles. Any pricing submitted must include this charge amount per the most current H-GAC schedule. For motor vehicle orders, the Processing Charge is paid by the Customer.

ARTICLE 11: CHANGE OF STATUS

Contractor shall immediately notify H-GAC, in writing, of ANY change in ownership, control, dealership/franchisee status, Motor Vehicle license status, or name. Contractor shall offer written guidance to advise H-GAC if this Master Agreement shall be affected in any way by such change. H-GAC shall have the right to determine whether or not such change is acceptable, and to determine what action shall be warranted, up to and including cancellation of Master Agreement.

ARTICLE 11: REQUIREMENTS TO APPLICABLE PHYSICAL GOODS

In the case of physical goods (e.g. equipment, material, supplies, as opposed to services), all Products offered must comply with any applicable provisions of the Texas Business and Commerce Code, Title 1, Chapter 2 and with at least the following:

- a. Be new, unused, and not refurbished.
- b. Not be a prototype as the general design, operation and performance. This requirement is NOT meant to preclude the Contractor from offering new models or configurations which incorporate improvements in a current design or add functionality, but in which new model or configuration may be new to the marketplace.
- c. Include all accessories which may or may not be specifically mentioned in the Master Agreement, but which are normally furnished or necessary to make the Product ready for its intended use upon delivery. Such accessories shall be assembled, installed and adjusted to allow continuous operation of Product at time of delivery.
- d. Have assemblies, sub-assemblies and component parts that are standard and interchangeable throughout the entire quantity of a Product as may be purchased simultaneously by any Customer.
- e. Be designed and constructed using current industry accepted engineering and safety practices, and materials.

- f. Be available for inspection at any time prior to or after procurement.

ARTICLE 12: TEXAS MOTOR VEHICLE BOARD LICENSING

All Contractors that deal in motor vehicles shall maintain current licenses that are required by the Texas Motor Vehicle Commission Code. If at any time during this Master Agreement term, any required Contractor license is denied, revoked, or not renewed, Contractor shall be in default of this Master Agreement, unless the Texas Motor Vehicle Board issues a stay or waiver. Contractor shall promptly provide copies of all current applicable Texas Motor Vehicle Board documentation to H-GAC upon request.

ARTICLE 13: INSPECTION/TESTING

All Products sold pursuant to this Master Agreement will be subject to inspection/testing by or at the direction of H-GAC and/or the ordering Customer, either at the delivery destination or the place of manufacture. In the event a Product fails to meet or exceed all requirements of this Master Agreement, and unless otherwise agreed in advance, the cost of any inspection and/or testing, will be the responsibility of the Contractor.

ARTICLE 14: ADDITIONAL REPORTING REQUIREMENTS

Contractor agrees to submit written quarterly reports to H-GAC detailing all transactions during the previous three (3) month period. Reports must include, but are not limited, to the following information:

- a. Customer Name
- b. Product/Service purchased, including Product Code if applicable
- c. Customer Purchase Order Number
- d. Purchase Order Date
- e. Product/Service dollar amount
- f. HGACBuy Order Processing Charge amount

ARTICLE 15: BACKGROUND CHECKS

Cooperative customers may request background checks on any awarded contractor's employees who will have direct contact with students, or for any other reason they so choose, any may require contractor to pay the cost of obtaining any background information requested by the Customer.

ARTICLE 16: PROHIBITION ON CONTRACTS WITH COMPANIES BOYCOTTING ISRAEL CERTIFICATION

As required by Chapter 2271 of the Texas Local Government Code the Contractor must verify that it 1) does not boycott Israel; and 2) will not boycott Israel during the term of the Contract. Pursuant to Section 2271.001, Texas Government Code:

1. "Boycott Israel" means refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations specifically with Israel, or with a person or entity doing business in Israel or in an Israeli-controlled territory, but does not include an action made for ordinary business purposes; and

2. "Company" means a for-profit sole proprietorship, organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, or any limited liability company, including a wholly owned subsidiary, majority-owned subsidiary, parent company or affiliate of those entities or business associations that exist to make a profit.

ARTICLE 17: NO EXCLUDED NATION OR TERRORIST ORGANIZATION CERTIFICATION

As required by Chapter 2252 of the Texas Government Code the Contractor must certify that it is not a company engaged in active business operations with Sudan, Iran, or a foreign terrorist organization – specifically, any company identified on a list prepared and maintained by the Texas Comptroller under Texas Government Code §§806.051, 807.051, or 2252.153. (A company that the U.S. Government affirmatively

declares to be excluded from its federal sanctions regime relating to Sudan, Iran, or any federal sanctions regime relating to a foreign terrorist organization is not subject to the contract prohibition.)

ARTICLE 18: PROHIBITION ON CONTRACTING WITH ENTITIES USING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE EQUIPMENT (Effective Aug. 13, 2020 and as amended October 26, 2020)

Pursuant to 2 CFR 200.216, Contractor shall not offer equipment, services, or system that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. "Covered telecommunications equipment or services means 1) telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities); 2) for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities); 3) telecommunications or video surveillance services provided by such entities or using such equipment; or 4) telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Contractor must comply with requirements for certifications. The provision at 48 C.F.R Section 52.204-26 requires that Contractors review SAM prior to completing their required representations. This rule applies to all acquisitions, including acquisitions at or below the simplified acquisition threshold and to acquisitions of commercial items, including commercially available off the-shelf items.

ARTICLE 19: BUY AMERICA ACT (National School Lunch Program and Breakfast Program)

With respect to products purchased by Customers for use in the National School Lunch Program and/or National School Breakfast Program, Contractor shall comply with all federal procurement laws and regulations with respect to such programs, including the Buy American provisions set forth in 7 C.F.R. Part 210.21(d), to the extent applicable. Contractor agrees to provide all certifications required by Customer regarding such programs.

In the event Contractor or Contractor's supplier(s) are unable or unwilling to certify compliance with the Buy American Provision, or the applicability of an exception to the Buy American provision, H-GAC Customers may decide not to purchase from Contractor. Additionally, H-GAC Customers may require country of origin on all products and invoices submitted for payment by Contractor, and Contractor agrees to comply with any such requirement.

ARTICLE 20: BUY AMERICA REQUIREMENT (Applies only to Federally Funded Highway and Transit Projects)

With respect to products purchased by Customer for use in federally funded highway projects, Contractor shall comply with all federal procurement laws and regulations with respect to such projects, including the Buy American provisions set forth in 23 U.S.C. Section 313, 23 C.F.R. Section 635.410, as amended, and the Steel and Iron Preference provisions of Texas Transportation Code Section 223.045, to the extent applicable. Contractor agrees to provide all certifications required by Customer regarding such programs. With respect to products purchased by Customer for use in federally funded transit projects, Contractor shall comply with all federal procurement laws and regulations with respect to such projects, including the Buy American provisions set forth in 49 U.S.C. Section 5323(j)(1), 49 C.F.R. Sections 661.6 or 661.12, to the extent applicable. Contractor agrees to provide all certifications required by Customer regarding such programs.

ARTICLE 21: DOMESTIC PREFERENCE

In accordance with 2 CFR 200.322, as appropriate and to the extent consistent with law, a Customer using federal grant award funds should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). The Customer must include this requirement in all subawards including all contracts and purchase orders for work or products under the federal grant award. If Contractor intends to qualify for Purchase Orders using federal grant money, the it shall work with the Customer to provide all required certifications and other documentation needed to show compliance.

ARTICLE 22: TITLE VI REQUIREMENTS

H-GAC in accordance with the provisions of Title VI of the Civil Rights Act of 1964 (78 Stat. 252, 42 U.S.C. §§ 2000d to 2000d-4) and the Regulations, hereby notifies all bidders that it will affirmatively ensure that any disadvantaged business enterprises will be afforded full and fair opportunity to submit in response to this Master Agreement and will not be discriminated against on the grounds of race, color, or national origin in consideration for an award.

ARTICLE 23: EQUAL EMPLOYMENT OPPORTUNITY

Except as otherwise provided under 41 CFR Part 60, all Contracts and Customer Purchase Orders that meet the definition of “federally assisted construction contract” in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, “Equal Employment Opportunity” (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., pg.339), as amended by Executive Order 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity,” and implementing regulations at 41CFR Part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor.”

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Contractor agrees that such provision applies to any contract that meets the definition of “federally assisted construction contract” in 41 CFR Part 60-1.3 and agrees that it will comply with such provision.

ARTICLE 24: CLEAN AIR AND WATER POLLUTION CONTROL ACT

Customer Purchase Orders using federal funds must contain a provision that requires the Contractor to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

Pursuant to the Federal Rule above, Contractor certifies that it is in compliance with all applicable provisions of the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387) and will remain in compliance during the term of the Contract.

ARTICLE 25: PREVAILING WAGE

Contractor and any potential subcontractors have a duty to and shall pay the prevailing wage rate under the Davis-Bacon Act, 40 U.S.C. 276a – 276a-5, as amended, and the regulations adopted thereunder contained in 29 C.F.R. pt. 1 and 5.

ARTICLE 26: CONTRACT WORK HOURS AND SAFETY STANDARDS

As per the Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708), where applicable, all Customer Purchase Orders in excess of ,000 that involve the employment of mechanics or laborers must include

a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

ARTICLE 27: PROFIT AS A SEPARATE ELEMENT OF PRICE

For purchases using federal funds in excess of ,000, a Customer may be required to negotiate profit as a separate element of the price. See, 2 CFR 200.323(b). Contractor agrees to provide information and negotiate with the Customer regarding profit as a separate element of the price for the purchase. Contractor also agrees that the total price, including profit, charged by Contractor to Customer will not exceed the awarded pricing, including any applicable discount, under any awarded contract.

ARTICLE 28: BYRD ANTI-LOBBYING AMENDMENT

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) – Contractors that apply or bid for an award exceeding ,000 must file the required anti-lobbying certification. Each tier must certify to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the Customer. As applicable, Contractor agrees to file all certifications and disclosures required by, and otherwise comply with, the Byrd Anti-Lobbying Amendment (31 USC 1352). Contractor certifies that it is currently in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) and will continue to be in compliance throughout the term of the Contract and further certifies that:

1. No Federal appropriated funds have been paid or will be paid by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal Grant, the making of a Federal Loan, the entering into a cooperative Master Agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative Master Agreement.
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing, or attempting to influence, an officer or employee of a Member of Congress in connection with a Federal contract, grant, loan, or cooperative Master Agreement, Contractor shall complete and submit Standard Form – LLL, “Disclosure Form to Report Lobbying”, in accordance with its instructions.
3. Contractor shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative Master Agreements) and that all subcontractors shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certificate is a prerequisite for making or entering into this transaction imposed by Section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than ,000 and not more than ,000 for each such failure.

ARTICLE 29: COMPLIANCE WITH EPA REGULATIONS APPLICABLE TO GRANTS, SUBGRANTS, COOPERATIVE MASTER AGREEMENTS, AND CONTRACTS

Contractor certifies compliance with all applicable standards, orders, regulations, and/or requirements issued pursuant to the Clean Air Act of 1970, as amended (42 U.S.C. 1857(h)), Section 508 of the Clean Water Act, as amended (13 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15.

ARTICLE 30: COMPLIANCE WITH ENERGY POLICY AND CONSERVATION ACT

Contractor certifies that Contractor will be in compliance with mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (Pub. L. 94-163, 89 Stat. 871).

HGACBuy

Attachment A**H2O Partners, Inc.****All Hazards Preparedness, Planning, Consulting & Recovery Services****Contract No.: HP08-21**

H2O Partners Labor Category	Hourly Rates
Project Executive/Principal	\$215.00
Quality Control Officer	\$180.00
Subject Matter Expert	\$160.00
Program Manager	\$185.00
Project Manager	\$160.00
Senior Consultant	\$155.00
Staff Consultant	\$120.00
Associate Consultant	\$110.00
Senior Planner	\$132.00
Associate Planner	\$120.00
Planner	\$110.00
GIS Specialist	\$110.00
Senior Grant Manager	\$132.00
Grant Manager	\$120.00
Senior Closeout Specialist	\$120.00
Closeout Specialist	\$110.00
Cost Estimator	\$110.00
Senior Insurance Specialist	\$155.00
Insurance Specialist	\$135.00
Environmental Specialist	\$135.00
Construction Manager	\$135.00
Construction Inspector	\$120.00
Eligibility Manager	\$155.00
Eligibility Analyst	\$120.00
Eligibility Consultant	\$110.00
Senior Case Manager	\$120.00
Case Manager	\$110.00
Technical Support Specialist	\$110.00

HGACBuy

Support Specialist	\$95.00
Publisher/Graphic Design	\$143.00
Senior Technical Writer	\$147.00
Technical Writer	\$100.00
IT System Management	\$124.00
IT System Support	\$107.00
Education & Outreach Specialist (Master)	\$135.00
Education & Outreach Specialist (Senior)	\$120.00
Education & Outreach Specialist (Mid)	\$110.00
Training Performance Consultant	\$120.00
Continuing Education Coordinator	\$110.00
Editor	\$147.00
Curriculum Development/Designer	\$147.00
Administrative Specialist	\$90.00
Roadway Asset Services (RAS) Management Labor Category	Hourly Rates
Training Services	\$150.00
Data Collection Specialist	\$100.00
Database Administrator	\$120.00
Senior Database Administrator	\$150.00
GIS Technician	\$90.00
GIS Analyst	\$110.00
Senior GIS Analyst	\$150.00
Programmer I	\$100.00
Programmer II / AMS Specialist	\$150.00
Pavement Subject Matter Expert	\$275.00
Transportation Subject Matter Expert	\$200.00
Asset Management Subject Matter Expert	\$200.00
Project Manager	\$160.00
Senior Project Manager	\$200.00
Principal-in-Charge	\$300.00
Pavement Consultant	\$200.00
Senior Pavement Consultant	\$275.00
Arborist	\$200.00
Unmanned Aerial Vehicle (UAV) Pilot in Command	\$210.00
Unmanned Aerial Vehicle (UAV) Pilot	\$185.00
Sensor Operator for Remote UAV	\$185.00
Visual Observer for Remote UAV	\$160.00
Roadway Asset Services (RAS) Inventory	Rates
Centerline Identification (lump sum)	\$1,950.00
Field Set-up & GPS Network Creation (lump sum)	\$5,500.00
Project Calibration Site Survey (lump sum)	\$2,500.00
Collect Street Network (test mile)	\$80.00

HGACBuy

Pavement Condition Index - ASTM D6433 surveys (PCI) (test mile)	\$50.00
Pavement Condition Index-ASTM D6433 (PCI) 100% rating of test mile driven	\$150.00
Pavement Condition Index - Modified ASTM D6433 Artificial Intelligence with 100% rating (PCI) (test mile)	\$40.00
Alley inventory (paved) (lane mile)	\$60.00
Alley inventory (unpaved) (lane mile)	\$70.00
GIS Street Centerline Creation (lane mile)	\$60.00
Pavement Widths (lane mile)	\$12.00
Signs (lane mile)	\$45.00
Signs, with no conditions rating (lane mile)	\$38.00
Signs, Nighttime Retroreflectivity, visual assessment (lane mile)	\$36.00
Sidewalks (lane mile)	\$40.00
Sidewalks, with no condition rating (lane mile)	\$32.00
Sidewalk Obstructions (lane mile)	\$30.00
ADA Ramps (lane mile)	\$30.00
ADA Ramps, with no condition rating (lane mile)	\$25.00
Signals (lane mile)	\$30.00
Inlets (lane mile)	\$30.00
Curb and Gutter (lane mile)	\$45.00
Curb and Gutter, with no condition rating (lane mile)	\$35.00
Pavement Markings (lane mile)	\$30.00
Pavement Striping (lane mile)	\$40.00
Water Valves (lane mile)	\$25.00
Control/vault boxes (lane mile)	\$25.00
Backflow and backflow enclosures (lane mile)	\$25.00
Fire Hydrants (lane mile)	\$25.00
Manholes (lane mile)	\$25.00
Street Lights (lane mile)	\$30.00
Transformers (lane mile)	\$25.00
Parking Meters (lane mile)	\$25.00
Utility Poles (lane mile)	\$30.00
Meter Boxes (lane mile)	\$25.00
Street Trees, location only (no tree species information) (lane mile)	\$90.00
Retaining Walls (lane mile)	\$40.00
Mailboxes (lane mile)	\$25.00
Driveways (Drive path) (lane mile)	\$45.00
Bus Shelters (lane mile)	\$25.00
Guardrails (lane mile)	\$25.00
Bike Lanes and Bike Lane Hazards (lane mile)	\$25.00
Bikeway Bollards (lane mile)	\$20.00
Traffic Calming Devices (lane mile)	\$30.00
ITS Beacons (lane mile)	\$25.00
ITS System Cabinets (lane mile)	\$30.00
ITS Pullboxes (lane mile)	\$35.00
ITS Service Connections (lane mile)	\$30.00
ITS Poles (lane mile)	\$30.00
ITS Dynamic Message Signs (lane mile)	\$20.00
Medians (lane mile)	\$60.00
Bridge Locations (lane mile)	\$30.00
Streetscapes (lane mile)	\$60.00
Parks and Recreation Facilities (unit)	\$60.00
Trail and bike path Inventory (mile)	\$60.00
GIS Delivery and Metadata Documentation (lump sum)	\$10,200.00
Pavement Report with 1 round of multi-year Budget Scenarios (lump sum)	\$25,000.00
Pavement Report without multi-year Budget Scenarios (lump sum)	\$15,000.00
3 additional PCI forecast scenarios (lump sum)	\$5,000.00

HGACBuy

Onsite RAS data reviews (per day)	\$2,500.00
Falling Weight Deflectometer (FWD) and Ground Penetrating Radar (GPR) testing for Arterial and Collector Roads (lane mile)	\$145.00
Falling Weight Deflectometer (FWD) and Ground Penetrating Radar (GPR) testing for Local/Residential Roads (lane mile)	\$170.00
Falling Weight Deflectometer (FWD) analysis and reporting (SCI value in tables) (lane mile)	\$160.00
Falling Weight Deflectometer (FWD) and Ground Penetrating Radar (GPR) analysis and reporting (SCI value in tables and GPR thickness tables) (lane mile)	\$320.00
Mobilization for Falling Weight Deflectometer (FWD) and Ground Penetrating Radar (GPR) testing (lump sum)	\$15,000.00
Traffic Control for Falling Weight Deflectometer (FWD) and Ground Penetrating Radar (GPR) testing (day)	\$2,000.00

Section E: Marketing and Service Plan (Form H)

Prime Proposer: H2O Partners, Inc.



FORM H – MARKETING & SERVICE PLAN

Respondent: H2O Partners, Inc.

H-GAC expects proposer to have the capability and willingness to serve any H-GAC Customers across the nation, and to promote any contract to the best of its ability. Respondent must submit a completed marketing and service plan form and include a detailed written narrative explaining in detail activities that will be undertaken to actively market and promote the awarded contract to H-GAC Customers and provide information on applicable items listed below:

1. Describe types of media to be used, frequency and method of outreach campaigns (social media, ads, sales tools, newsletters, etc.)

Since many of the business opportunities that arise post-disaster are not procured in direct response to traditional forms of marketing and advertising, H2O seeks to maintain high visibility to our past and potential future clients during "blue sky" times prior to disaster needs. We achieve this via a blend of outreach strategies, including social media, enhanced web site resources for clients/visitors, advertising in Texas Emergency Management Magazine, and through our attendance, exhibition, and sponsorship at various industry conferences and trade shows. Below is a list of our recent and current conference registrations. COVID-19 has forced many conferences online again this year, but we anticipate 2022 will be back live, in person.

- Texas Floodplain Managers Conference, (Exhibitor/Sponsor), Online, April 14-17, 2021
- American Society of Floodplain Managers Annual Conference, (Major Sponsor/Exhibitor) Online, May 9-13, 2021
- Florida Governor's Hurricane Conference, West Palm Beach, Florida, May 16-21, 2021
- National Hurricane Conference, New Orleans, Louisiana, June 14-17, 2021
- National Flood Conference, (Major Sponsor/Exhibitor), Online, June 27-30, 2021
- National Association of Flood and Stormwater Management Agencies, (Presenter) Nashville, Tennessee, August 16-19, 2021
- International Association of Emergency Managers, (Exhibitor) Grand Rapids, Michigan, October 5-22, 2021
- Texas-American Public Works Association Conference, Galveston, Texas, October 20-22, 2021 (RAS)
- Texas Association of County Engineers and Road Administrators, Location TBD, October 2021 (RAS)

- Texas Emergency Management Conference, (Exhibitor) San Antonio, Texas, Date TBD
- Texas Floodplain Managers Technical Summit, (Sponsor) Date and Location TBD, usually San Antonio
- FIMA IBHS, Washington D.C., Date TBD
- H-GAC Buy Conference, Date and Location TBD
- American Public Works Association PWX National Conference, 2022 Date and Location TBD (RAS)

When H2O attends conferences and exhibits, we typically rent a 10x10 booth with professionally-designed booth graphics and decorations. Our staff is expected to be at the booth at all times the exhibit hall is open, and we keep ample supply of fact sheets, contact cards, and promotional give-away items (swag) with our logo and website URL. Often, H2O Subject Matter Experts are asked to present at these conferences, and we use that exposure to highlight the services we offer. H2O always displays the H-GAC plexiglass sign and offers information about H-GAC at our booths. Our staff is knowledgeable and can explain how H-GAC contracting works. Our staff always has a supply of cards on hand to direct clients to H-GAC if they have more in-depth questions.

2. A description of the dedicated staff resources anticipated in serving and in promoting any contract.

H2O Partners executive management team participates in the promotion and management of every contract. Our founder and president, Jo Ann Howard, is a former presidentially appointed administrator at FEMA and a major portion of her activities are business-development related. Eric Howard, H2O's Vice President, oversees business operations, including H-GAC contracting and procurement. Pam Hawkins, H2O's Director of Program Operations, provides program oversight and staffing management for all of our contracted work. Julie Wickert has recently joined the H2O team as our Business Development Manager and she oversees the production of all of our proposals and business development materials. Our program staff includes Dorothy Martinez, NFIP Stakeholder Training and Outreach Manager, Heather Ferrara, H2O's Mitigation Programs Manager, and Elizabeth Russell, H2O's Innovation Team Manager. All of our management and program staff are expected to contribute to business development activities in addition to their program duties. H2O currently employs 38 staff members and business development is on every job description.

3. Anticipated marketing strategies to increase sales in awarded service areas or categories.

Though much of our business is directly related to disaster events, we have endeavored to gain pre-positioned clients to avoid the "storm chasing" aspect of the disaster recovery business. H2O Partners seeks to shift the procurement timeline to pre-disaster engagement to reduce the urgency, and often rushed evaluation and decision-making on the part of the client. This model is a good fit with the H-GAC program, and we encourage prospective clients to take this procurement path whenever practical. We have seen an increase in overall contracts at the state and local level, but much of this business has come outside of the H-GAC Buy program due to Texas Division of Emergency Management and FEMA's active discouragement of local municipalities and counties during the last contract cycle. We sincerely hope those agencies' objections have been overcome and our clients are supported in their procurement of disaster services via this vehicle.

4. Anticipated employee representative trainings and frequency.

H2O Partners makes Continuing Education and certification support a priority for every employee. Typically, we focus on professional areas of expertise and certification, but we spend a significant amount of internal time and resources preparing our staff for business development activities. We have an internal, annual “all hands” meeting where we go over all our contracts, proposals, targets, and teaming partners with the staff, so they are prepared to answer questions and direct prospective clients to the proper internal resources. Should H2O be awarded an H-GAC contract in this cycle, we will include training and information on the program and business development strategies for growing our H-GAC line of business.

5. Dedicated webpages or other online presence.



H2O is your partner when you need us. From hazard mitigation to recovery after the worst hits, our team jumps into *difficult* with both feet. We cut through red tape and confusion, harness the power of local, state and national experts, and work tirelessly to solve your overwhelming, often heartbreaking, challenges. And like any strong partner, H2O stands by your side every step of the way. [>>> Learn More](#)

H2O IS AN SBA CERTIFIED WOMAN-OWNED SMALL BUSINESS (WOMB) AND A STATE HISTORICALLY UNDERUTILIZED BUSINESS (HUB).

H2O Partners' web site, www.h2opartnersusa.com, is newly designed, fresh, and informative. We have streamlined the pages and provide visitors with a clear path to contacting our professional staff. Should H2O be awarded a contract under this procurement, we will add the H-GAC Buy logo and link to the appropriate page.

H2O Partners has also developed an online knowledge base tool for our customers. Our PERDIX system is an all-purpose portal to help manage document-heavy and regulatory contracts. The system is available on a seat-license basis and is flexible enough to permit users to configure the resources to fit their use case. We often make this resource available at no extra charge to our disaster recovery clients and in other cases offer the system as a Software-As-Service (SAS) arrangement. We have not priced or offered this knowledge base portal via this procurement, since it does not specifically fit the service area requested, but we include it here as an example of our online presence and customer-facing proprietary tools.



6. Use of dealer or distributor networks.

H2O Partners' service delivery model does not include the use of dealers or distributors since those sales models are better suited to goods or commodities sales.

7. Use of existing company marketing teams and coordination with H-GAC's marketing team.

Over the past contract cycle H2O has coordinated with the H-GAC marketing team to acquire materials for distribution at sales events, conferences, and presentations. Due to the situation with TDEM and FEMA during the last cycle, we were not able to fully realize the potential for collaborative marketing and sincerely hope those agencies' objections have been overcome for the upcoming cycle. We look forward to working closely with the H-GAC marketing team to introduce the organization to our audiences at national conferences and events.

8. Metrics employed to measure outreach and marketing success and measurement of sales.

H2O Partners' sales have grown in all categories: revenue, clients, contracts, and profitability over the past H-GAC contract cycle. Hurricane Harvey drove significant business to us, but we grew at the federal and out-of-Texas levels as well. We use monthly sales reports, quarterly revenue forecast tools, and semi-annual and annual financial reviews from our Chief Financial Officer and Executive Management team, along with our Board of Directors to pinpoint what is and is not working in the business development and procurement areas of operation.

in advance, the cost of any inspection and/or testing, will be the responsibility of the Contractor.

ARTICLE 14: ADDITIONAL REPORTING REQUIREMENTS

Contractor agrees to submit written quarterly reports to H-GAC detailing all transactions during the previous three (3) month period. Reports must include, but are not limited, to the following information:

- a. Customer Name
- b. Product/Service purchased, including Product Code if applicable
- c. Customer Purchase Order Number
- d. Purchase Order Date
- e. Product/Service dollar amount
- f. HGACBuy Order Processing Charge amount

AMENDMENT No. 1 to CONTRACT No. HP08-21

For

All Hazards Preparedness, Planning, Consulting & Recovery Services

Between

HOUSTON-GALVESTON AREA COUNCIL

And

H2O Partners, Inc.

THIS AMENDMENT modifies the above referenced Contract as follows:

Clarifies Articles 26, 27, and 28 in Master Special Provisions of the above referenced Agreement (#7252) should read as follows:

ARTICLE 26: CONTRACT WORK HOURS AND SAFETY STANDARDS

As per the Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708), where applicable, all Customer Purchase Orders in excess of \$100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

ARTICLE 27: PROFIT AS A SEPARATE ELEMENT OF PRICE

For purchases using federal funds in excess of \$150,000, a Customer may be required to negotiate profit as a separate element of the price. See, 2 CFR 200.323(b). Contractor agrees to provide information and negotiate with the Customer regarding profit as a separate element of the price for the purchase. Contractor also agrees that the total price, including profit, charged by Contractor to Customer will not exceed the awarded pricing, including any applicable discount, under any awarded contract.

ARTICLE 28: BYRD ANTI-LOBBYING AMENDMENT

Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) – Contractors that apply or bid for an award exceeding \$100,000 must file the required anti-lobbying certification. Each tier must certify to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the Customer. As applicable, Contractor agrees to file all certifications and disclosures required by, and otherwise comply with, the Byrd Anti-Lobbying Amendment (31 USC 1352). Contractor certifies that it is currently in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) and will continue to be in compliance throughout the term of the Contract and further certifies that:

1. No Federal appropriated funds have been paid or will be paid by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal Grant, the making of a Federal Loan, the entering into a cooperative Master Agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative

Master Agreement.

2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing, or attempting to influence, an officer or employee of a Member of Congress in connection with a Federal contract, grant, loan, or cooperative Master Agreement, Contractor shall complete and submit Standard Form – LLL, “Disclosure Form to Report Lobbying”, in accordance with its instructions.
3. Contractor shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative Master Agreements) and that all subcontractors shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certificate is a prerequisite for making or entering into this transaction imposed by Section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

Unless otherwise noted, this amendment goes into effect on the date signed by **H-GAC**. All other terms and conditions of this Contract shall remain unchanged and in full force and effect.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized representatives.

Signed for **Houston-Galveston Area Council**,
Houston, Texas

DocuSigned by:



62EC270D5C04423

Chuck Wemple, Executive Director

1/5/2022

Date: _____

Signed for: **H2O Partners, Inc.**

DocuSigned by:



70D01848C3E44AD...

Eric Howard

Vice President

1/3/2022

Printed Name & Title:

Date: _____

AMENDMENT No. 2 to CONTRACT No. HP08-21
For
All Hazards Preparedness, Planning, Consulting & Recovery Services
Between
HOUSTON-GALVESTON AREA COUNCIL
And
H2O Partners, Inc.

THIS AMENDMENT modifies the above referenced Contract as follows:

This contract is extended through July, 31, 2024 Midnight CT.

Unless otherwise noted, this amendment goes into effect on the date signed by **H-GAC**. All other terms and conditions of this Contract shall remain unchanged and in full force and effect.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized representatives.

Signed for **Houston-Galveston Area Council**,
Houston, Texas

DocuSigned by:



925C372D5E091423

Chuck Wemple, Executive Director

Date: 7/3/2023

Signed for: **H2O Partners, Inc.**

Printed Name & Title:

DocuSigned by:



70D01B4BC3E44AD...

Eric Howard Vice President

Date: 6/30/2023



HOUSTON-GALVESTON AREA COUNCIL
PROCUREMENT AND CONTRACTS
PROGRAM

CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND
VOLUNTARY EXCLUSION FOR COVERED CONTRACTS

Federal Executive Order 12549 requires the Houston-Galveston Area Council (HGAC) to require each covered potential contractor to determine whether each has a right to obtain a contract in accordance with federal regulations on debarment, suspension, ineligibility, and voluntary exclusion. Each covered contractor must also screen each of its covered subcontractors/providers. In this certification, "contractor" refers to both contractor and subcontractor, "contract" refers to both contract and subcontract.

By signing and submitting this certification the potential contractor accepts the following terms:

1. The certification herein below is a material representation of fact upon which reliance was placed when this contract was entered into. If it is later determined that the potential contractor knowingly rendered an erroneous certification, in addition to other remedies available to the federal government, the Houston-Galveston Area Council or other federal department or agency, may pursue available remedies, including suspension and/or debarment.
2. The potential contractor shall provide immediate written notice to the person to whom this certification is submitted if at any time the potential contractor learns that the certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
3. The words "covered contract," "debarred," "suspended," "ineligible," "participant," "person," "principal," "proposal," and "voluntarily excluded," as used in this certification have meanings based upon materials in the Definitions and Coverage sections of federal rules implementing Executive Order 12549. Usage is as defined in the attachment.
4. The potential contractor agrees by submitting this certification that, should the proposed covered contract be entered into, it shall not knowingly enter into any subcontract with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the Houston-Galveston Area Council or other federal department or agency, as applicable.

Do you have or do you anticipate having subcontractors under this proposed contract? YES NO

5. The potential contractor further agrees by submitting this certification that it will include this certification titled "Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion for Covered Contracts" without modification, in all covered subcontracts and in solicitations for all covered subcontracts.
6. A contractor may rely upon a certification of a potential subcontractor that it is not debarred, suspended, ineligible, or voluntarily excluded from the covered contract, unless it knows that the certification is erroneous. A contractor must, at a minimum, obtain certifications from its covered subcontractors upon each subcontract's initiation and upon each renewal.
7. Nothing contained in all the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this certification document. The knowledge and information of a contractor is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
8. Except for contracts authorized under paragraph 4 of these terms, if a contractor in a covered contract knowingly enters into a covered subcontract with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in the transaction, in addition to other remedies available to the federal government, Houston-Galveston Area Council, or other federal department or agency, as applicable, may pursue available remedies, including suspension and/or debarment.

Indicate which statement applies to the covered potential contractor:

The potential contractor certifies, by submission of this certification, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this contract by any federal department or agency or by the State of Texas.

The potential contractor is unable to certify to one or more of the terms in this certification. In this instance, the potential contractor must attach an explanation for each of the above terms to which he is unable to make certification. Attach the explanation(s) to this certification.

NAME OF POTENTIAL CONTRACTOR H2O Partners, Inc.

VENDOR ID NO./FEDERAL EMPLOYER ID NO. 74-2994685

70D01B4BC3E44A0
Signature of Authorized Representative

Eric Howard
Printed/Typed Name of Authorized Representative

6/30/2023
Date

Vice President
Title of Authorized Representative

H-GAC

Houston-Galveston Area Council

P.O. Box 22777 · 3555 Timmons · Houston, Texas 77227-2777

Cooperative Agreement - Extension - H2O Partners, Inc. - Public Services - ID: 12490

EXTENSION No. 2 to CONTRACT No. HP08-21

For

All Hazards Preparedness, Planning, Consulting & Recovery Services

Between

HOUSTON-GALVESTON AREA COUNCIL

And

H2O Partners, Inc.


THIS AMENDMENT modifies the above referenced Contract as follows:

Contract is extended through Jul 31 2025 Midnight CST or the effective date of the contracts resulting from the most recently awarded Request For Proposal (RFP) for All Hazards Preparedness, Planning, Consulting & Recovery Services, whichever occurs first.

Unless otherwise noted, this amendment goes into effect on the date signed by **H-GAC**. All other terms and conditions of this Contract shall remain unchanged and in full force and effect.

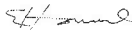
IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized representatives.

Signed for: **Houston-Galveston Area Council**

DocuSigned by:

82EC270D5D61423...

Chuck Wemple
Executive Director
Date: 5/17/2024

Signed for: **H2O Partners, Inc.**

DocuSigned by:

70D91B4BC3E44AD...

Printed Name:
Title:

Eric Howard
Vice President
Date: 5/14/2024



HOUSTON-GALVESTON AREA COUNCIL
PROCUREMENT AND CONTRACTS
PROGRAM

CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND
VOLUNTARY EXCLUSION FOR COVERED CONTRACTS

Federal Executive Order 12549 requires the Houston-Galveston Area Council, under 49 CFR 101-11.9, to determine and document whether each person who enters into a contract in accordance with federal regulations is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the Houston-Galveston Area Council or other federal department or agency, as applicable, may pursue available remedies, including suspension and/or debarment.

By signing and submitting this certification the potential contractor accepts the following terms:

1. The certification herein below is a material representation of fact upon which reliance was placed when this contract was entered into. If it is later determined that the potential contractor knowingly rendered an erroneous certification, in addition to other remedies available to the federal government, the Houston-Galveston Area Council or other federal department or agency, may pursue available remedies, including suspension and/or debarment.
2. The potential contractor shall provide immediate written notice to the person to whom this certification is submitted if at any time the potential contractor learns that the certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
3. The words "covered contract," "debarred," "suspended," "ineligible," "participant," "person," "principal," "proposal," and "voluntarily excluded," as used in this certification have meanings based upon materials in the Definitions and Coverage sections of federal rules implementing Executive Order 12549. Usage is as defined in the attachment.
4. The potential contractor agrees by submitting this certification that, should the proposed covered contract be entered into, it shall not knowingly enter into any subcontract with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the Houston-Galveston Area Council or other federal department or agency, as applicable.

Do you have or do you anticipate having subcontractors under this proposed contract? YES NO

5. The potential contractor further agrees by submitting this certification that it will include this certification titled "Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion for Covered Contracts" without modification, in all covered subcontracts and in solicitations for all covered subcontracts.
6. A contractor may rely upon a certification of a potential subcontractor that it is not debarred, suspended, ineligible, or voluntarily excluded from the covered contract, unless it knows that the certification is erroneous. A contractor must, at a minimum, obtain certifications from its covered subcontractors upon each subcontract's initiation and upon each renewal.
7. Nothing contained in all the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this certification document. The knowledge and information of a contractor is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
8. Except for contracts authorized under paragraph 4 of these terms, if a contractor in a covered contract knowingly enters into a covered subcontract with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in the transaction, in addition to other remedies available to the federal government, Houston-Galveston Area Council, or other federal department or agency, as applicable, may pursue available remedies, including suspension and/or debarment.

Indicate which statement applies to the covered potential contractor:

The potential contractor certifies, by submission of this certification, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this contract by any federal department or agency or by the State of Texas.

The potential contractor is unable to certify to one or more of the terms in this certification. In this instance, the potential contractor must attach an explanation for each of the above terms to which he is unable to make certification. Attach the explanation(s) to this certification.

NAME OF POTENTIAL CONTRACTOR Roadway Asset Services

VENDOR ID NO./FEDERAL EMPLOYER ID NO. 85-1939454

[Signature]
Signature of Authorized Representative

Eric Howard
Printed/Typed Name of Authorized Representative

May 14, 2024
Date

Executive Vice Preseident
Title of Authorized Representative



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024
AGENDA ITEM #14

Discuss and consider approving a
project development agreement with
the Texas Department of
Transportation for the US 183 General
Purpose Lane Project

Strategic Plan Relevance:	Collaboration
Department:	Engineering
Contact:	Mike Sexton, P.E., Director of Engineering
Associated Costs:	No financial liability with executing the Project Development Agreement
Funding Source:	TxDOT
Action Requested:	Consider and act on the draft resolution

Project Description/Background: The Texas Department of Transportation (TxDOT) US 183 general purpose lane project from RM 1431 to Avery Ranch Boulevard will address congestion, enhance safety, and improve mobility along US 183 in Williamson County. The project has two elements: the first being construction of new frontage roads and the second operation and maintenance of the new and existing frontage roads in the corridor.

The first component is an approximate 3-mile project that includes constructing two grade-separated lanes on each side of the Mobility Authority's 183A toll road from Ranch to Market 1431 to Avery Ranch Boulevard and a shared-use path on the northbound side of the roadway, connecting to the existing 183A trailhead. The second component of the project is for TxDOT to assume operating and maintenance of the newly constructed and existing frontage roads adjacent to the Authority's 183A corridor in between Avery Ranch Boulevard and US 183.

The PDA outlines the rights and responsibilities of TxDOT and the Authority for the construction component and subsequent operating and maintenance of the contiguous frontage roads. Additionally, the PDA grants TxDOT the right to operate within the

Authority's right-of-way.

The Authority has loans and loan commitments with United States Department of Transportation (USDOT) and the Transportation Innovation and Infrastructure Finance Act (TIFIA) Office. In accordance with loan covenant provisions, Authority staff has presented the PDA for review and determination on action by TIFIA.

The Indenture of Trust established by the Authority to provide security for investors and lenders requires agreements such as the PDA to be reviewed by the Authority's Board of Directors to ensure that the actions outlined will not be prohibitive to the operation of the Authority or prevent compliance with bond and debt covenants.

Previous Actions & Brief History of the Program/Project: The Authority has informed lenders and investors of this planned TxDOT project since 2018. The project has been disclosed in traffic and revenue studies, bond offering documents and financial models presented to investors and lenders since that time. TxDOT started the schematic design and environmental process in 2018, with environmental clearance achieved in the fall of 2023. TxDOT will finalize design plans in September 2024 and plans to have a construction letting in November 2024 for the project. Construction will start in spring 2025, with completion anticipated in 2028.

Financing: The project, both construction and operating and maintenance of the contiguous frontage roads, will be 100% funded by TxDOT

Action requested/Staff Recommendation: Staff recommends that the Board execute the Project Development Agreement with TxDOT for the US 183 general purpose lane project.

Backup provided:
Development Agreement to be

Draft Resolution and Project
provided at the board meeting



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024
AGENDA ITEM #15

Project Updates

Strategic Plan Relevance: Stewardship, Service & Safety
Department: Engineering
Contact: Mike Sexton, 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

Backup provided: None



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024
AGENDA ITEM #16

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. Recent agency staff activities.
- B. Agency performance metrics.

Backup provided: None



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024
AGENDA ITEM #17

Executive Session

Executive Session:

Discuss the acquisition of one or more parcels or interests in real property need for a Mobility Authority headquarters, including facilities for traffic and incident management and other agency functions, pursuant to §551.071 (Consultation with Attorney) and §551.072 (Deliberation Regarding Real Property; Closed Meeting).



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024
AGENDA ITEM #18

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

September 25, 2024
AGENDA ITEM #19

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

September 25, 2024
AGENDA ITEM #20

Executive Session

Executive Session:

Discuss personnel matters related to the executive director's employment agreement, as authorized by §551.074 (Personnel Matters).



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 25, 2024
AGENDA ITEM #21

Adjourn Meeting

Adjourn Board Meeting.