



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

## Regular Meeting of the Board of Directors

---

**9:00 a.m.**

Wednesday, September 29, 2021

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](http://www.mobilityauthority.com)*

**Note to members of the public.** Pursuant to Texas Transportation Code Section 370.262, this meeting will be held by telephone conference call. Some Board Members may be present in the Lebermann Board Room while others may participate remotely. In order to maintain safe social distancing, you may view the Board Meeting online via the live stream link on our website. Members of the public that wish to join the conference call to provide comments to the Board remotely must register at least 30 minutes prior to the scheduled start time by contacting the Central Texas Regional Mobility Authority at (844) 287-6220.

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

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

## AGENDA

---

### ***No action on the following:***

---

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

### ***Convene the Audit Committee Meeting***

---

2. Audit Committee Meeting
  - A. Audit Committee meeting called to order by Committee Chairman Singleton.
  - B. Introduction of external auditors from RSM US LLP.

- C. Discuss, consider, and take appropriate action to accept the Fiscal Year 2021 Audit Reports.
- D. Adjourn Audit Committee.

## **Consent Agenda**

---

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

- 3. Approve the minutes from the August 25, 2021 Regular Board Meeting.
- 4. Approve the assignment of the contract for roadway maintenance on 183A Toll and 290E from Angel Brothers Enterprises, Ltd. to Texas Materials Group, Inc.
- 5. Approve a contract with The Levy Company, Inc. for large sign replacement on 183A Phase II (Maintenance Project, 22MAINT-01).
- 6. 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.*

- 7. Accept the financial statements for August 2021.
- 8. Discuss and consider authorizing the Issuance, Sale, and Delivery of Central Texas Regional Mobility Authority Senior Lien Revenue Refunding Bonds in accordance with Specified Parameters.
- 9. Discuss and consider approving a contract with Deloitte Consulting LLP for continued development of the data platform and associated transaction routing and system interfaces to support toll transaction management.

## **Briefings and Reports**

---

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

- 10. Potential options for aesthetic improvements to the Montopolis Bridge.
- 11. Executive Director Board Report
  - A. Resumption of Pay by Mail invoicing related to TxTag processing.

## **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:*

12. Discuss legal issues related to claims by or against the Mobility Authority; pending or contemplated litigation and any related settlement offers; or other matters as authorized by §551.071 (Consultation with Attorney).
13. Discuss legal issues relating to procurement and financing of Mobility Authority transportation projects, as authorized by §551.071 (Consultation with Attorney).
14. Discuss personnel matters as authorized by §551.074 (Personnel Matters).

## **Reconvene in Open Session.**

---

## **Regular Items**

---

*Items to discuss, consider, and take appropriate action.*

15. 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.

*Mobility Authority Board Meeting Agenda  
Wednesday, September 29, 2021*

**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.

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.

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

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

~~(1) an emergency or public necessity exists within the meaning of Section 551.045 of this chapter; and~~

~~(2) the convening at one location of a quorum of the governmental body is difficult or impossible; or~~

~~(3) the meeting is held by an advisory board.~~

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

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

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

(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 29, 2021  
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 29, 2021  
**AGENDA ITEM #2**

---

Accept the Independent Audit Reports  
from RSM US LLP for the Fiscal Year  
Ending June 30, 2021

Strategic Plan Relevance: Regional Mobility  
Department: Finance  
Contact: Bill Chapman, Chief Financial Officer  
Associated Costs: N/A  
Action Requested: Consider and act on the draft resolution

**Background:** Each year the Mobility Authority engages an independent CPA firm to conduct the Authority's required annual audit and single audit. RSM US LLP has completed the annual audit for FY 2021 and will present those reports to the Audit Committee. The draft Resolution accepts the annual audits for FY 2021.

**Audit Committee - Agenda:**

- A. Audit Committee meeting called to order by Committee Chairman Singleton.
- B. Introduction of external auditors from RSM US LLP.
- C. Discuss, consider, and take appropriate action to accept the Fiscal Year 2021 Audit Reports.
- D. Adjourn Audit Committee.

**Action requested/Staff Recommendation:** Staff recommends the Board accept the annual audits for FY 2021.

**Backup provided:** Draft Resolution  
FY 2020 Audit Reports to be provided at the Board Meeting

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

**RESOLUTION NO. 21-0XX**

**ACCEPTING THE INDEPENDENT AUDIT REPORTS FROM RSM US LLP  
FOR THE FISCAL YEAR ENDING JUNE 30, 2021**

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

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

WHEREAS, the firm of RSM US LLP, has been engaged to provide an independent audit of the finances of the Central Texas Regional Mobility Authority for the fiscal year ending on June 30, 2021, and has presented that audit to the Audit Committee; and

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

NOW THEREFORE, BE IT RESOLVED, that the Audit Committee accepts the independent audit reports of the Central Texas Regional Mobility Authority prepared by RSM US LLP for the fiscal year ending on June 30, 2021; and

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

Adopted by the Audit Committee of the Board of Directors of the Central Texas Regional Mobility Authority on the 29<sup>th</sup> day of September 2021.

Submitted and reviewed by:

Approved:

---

Geoffrey Petrov, General Counsel

---

David Singleton  
Chairman, Audit Committee

**Exhibit A**

**Report to the Board of Directors**

(To be provided at the Board Meeting)

**Exhibit B**

**Basic Financial Statements**

(To be provided at the Board Meeting)

**Exhibit C**

**State Awards Compliance Report**

(To be provided at the Board Meeting)



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
AGENDA ITEM #3

---

Approve the minutes from the August  
25, 2021 Regular Board Meeting

Strategic Plan Relevance: Regional Mobility  
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 25, 2021 Regular Board Meeting.

**Backup provided:** Draft minutes

## MINUTES

### Regular Meeting of the Board of

### Directors of the

### CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY

Wednesday, August 25, 2021

9:00 a.m.

This was a video conference meeting. Notice of the meeting was posted August 20, 2021 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 was present on the video conference meeting as were Vice Chair Meade\*, Board Members David Singleton, David Armbrust, John Langmore, Mike Doss and Heather Gaddes.

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

<https://mobilityauthority.swagit.com/play/08252021-953>

After noting that a quorum of the Board was present, Chairman Jenkins called the meeting to order at 9:04 a.m. and had each Board Member who attended via video conference state their name for the record and confirm that they could both hear and be heard by all other attendees that were present in-person or live streaming.

1. Welcome and opportunity for public comment.

Sharon Blythe, Director, Austin Rescue Austin Memorial Park Cemetery, spoke in favor of the proposed memorandum of agreement for tree planting and other improvements at the Austin Memorial Park Cemetery that was presented in Item 12, below.

#### **Consent Agenda**

2. Approve the minutes from the June 30, 2021 Regular Board Meeting.
3. Approve the purchase of Google Looker and Apigee software subscriptions from Carahsoft Technology Corporation for the Data Platform Project.

**ADOPTED AS: RESOLUTION NO. 21-043**



4. Prohibit the operation of certain vehicles on Mobility Authority toll facilities pursuant to the Habitual violator Program.

**ADOPTED AS:**                   **RESOLUTION NO. 21-044**

**MOTION:**                        Approve Item Nos. 2 thru 4 under the Consent Agenda.

**RESULT:**                         Approved (Unanimous); 6-0

**MOTION:**                         Heather Gaddes

**SECONDED BY:**                 John Langmore

**AYE:**                             Armbrust, Doss, Gaddes, Jenkins, Langmore, Singleton

**NAY:**                             None.

**Regular Items**

5. Accept the unaudited financial statements through June 2021.

Presentation by Bill Chapman, Chief Financial Officer and Mary Temple, Controller. Tracie Brown, Director of Operations answered questions.

**MOTION:**                         Accept the unaudited financial statements through June 2021.

**RESULT:**                         Approved (Unanimous); 6-0

**MOTION:**                         Heather Gaddes

**SECONDED BY:**                 John Langmore

**AYE:**                             Armbrust, Doss, Gaddes, Jenkins, Langmore, Singleton

**NAY:**                             None.

**ADOPTED AS:**                   **RESOLUTION NO. 21-045**

6. Accept the financial statements through July 2021.

Presentation by Bill Chapman, Chief Financial Officer and Mary Temple, Controller.

**MOTION:**                         Accept the financial statements through July 2021.

**RESULT:**                         Approved (Unanimous); 6-0

**MOTION:**                         David Armbrust

**SECONDED BY:**                 Mike Doss

**AYE:**                             Armbrust, Doss, Gaddes, Jenkins, Langmore, Singleton

**NAY:**                             None.

**ADOPTED AS:**                   **RESOLUTION NO. 21-046**

7. Discuss and consider authorizing the execution and delivery of a TIFIA Loan Agreement with the United States Department of Transportation relating to the 183 North Mobility Project in accordance with specified parameters.

Presentation by Bill Chapman, Chief Financial Officer. Glenn Opel, Partner, Bracewell, LLP answered questions.

**MOTION:** Approve the execution and delivery of a TIFIA Loan Agreement with the United States Department of Transportation relating to the 183 North Mobility Project in accordance with specified parameters.

**RESULT:** Approved (Unanimous); 6-0

**MOTION:** David Singleton

**SECONDED BY:** John Langmore

**AYE:** Armbrust, Doss, Gaddes, Jenkins, Langmore, Singleton

**NAY:** None.

**ADOPTED AS:** **RESOLUTION NO. 21-047**

**\*NOTE:** Nikelle Meade joined the meeting at 9:36 a.m.

8. Discuss and consider adopting a resolution authorizing the redemption of the Mobility Authority's Subordinate Lien Revenue Bond Anticipation Notes, Series 2018.

Presentation Bill Chapman, Chief Financial Officer.

**MOTION:** Approve the redemption of the Mobility Authority's Subordinate Lien Revenue Bond Anticipation Notes, Series 2018.

**RESULT:** Approved (Unanimous); 7-0

**MOTION:** David Singleton

**SECONDED BY:** Heather Gaddes

**AYE:** Armbrust, Doss, Gaddes, Jenkins, Langmore, Meade, Singleton

**NAY:** None.

**ADOPTED AS:** **RESOLUTION NO. 21-048**

9. Discuss and consider approving a contract with The Goodman Corporation for feasibility analyses, funding consultation, and grant assistance for Park and Ride facility development.

Presentation by Steve Pustelnyk, Director of Community Relations.

**MOTION:** Approve a contract with The Goodman Corporation for feasibility analyses, funding consultation, and grant assistance for Park and Ride facility development.

**RESULT:** Failed; 4-3

**MOTION:** John Langmore

**SECONDED BY:** David Armbrust

**AYE:** Armbrust, Jenkins, Langmore,

**NAY:** Doss, Gaddes, Meade, Singleton

**ADOPTED AS:** Not adopted.

10. Discuss and consider approving Amendment No. 3 to the contract with RS&H Inc. for construction inspection services for the 183 South Project.

Presentation by Mike Sexton, Acting Director of Engineering.

**MOTION:** Approve Amendment No. 3 to the contract with RS&H Inc. for construction inspection services for the 183 South Project.

**RESULT:** Approved (Unanimous); 7-0

**MOTION:** Heather Gaddes

**SECONDED BY:** Nikelle Meade

**AYE:** Armbrust, Doss, Gaddes, Jenkins, Langmore, Meade, Singleton

**NAY:** None.

**ADOPTED AS:** **RESOLUTION NO. 21-049**

11. Discuss and consider approving Supplemental Work Authorization No. 6 to Work Authorization No. 2 with Atkins North America, Inc. for general engineering services for the 183 South Project.

Presentation by Mike Sexton, Acting Director of Engineering.

**MOTION:** Approve Supplemental Work Authorization No. 6 to Work Authorization No. 2 with Atkins North America, Inc. for general engineering services for the 183 South Project.

**RESULT:** Approved (Unanimous); 7-0

**MOTION:** Mike Doss

**SECONDED BY:** Heather Gaddes  
**AYE:** Armbrust, Doss, Gaddes, Jenkins, Langmore, Meade, Singleton  
**NAY:** None.

**ADOPTED AS:** **RESOLUTION NO. 21-050**

- 12.** Discuss and consider approving a memorandum of agreement with the Texas Department of Transportation, the State of Texas Historic Preservation Officer, and the City of Austin regarding the MoPac Improvement Project for the planting of trees and other improvements at Austin Memorial Park Cemetery.

Presentation by Mike Sexton, Acting Director of Engineering.

**MOTION:** Approve a memorandum of agreement with the Texas Department of Transportation, the State of Texas Historic Preservation Officer, and the City of Austin regarding the MoPac Improvement Project for the planting of trees and other improvements at Austin Memorial Park Cemetery.

**RESULT:** Approved; 6-1  
**MOTION:** David Armbrust  
**SECONDED BY:** Heather Gaddes  
**AYE:** Armbrust, Doss, Gaddes, Jenkins, Meade, Singleton  
**NAY:** Langmore.

**ADOPTED AS:** **RESOLUTION NO. 21-051**

- 13.** Discuss and consider (a) amending the Policy Code to exempt agreements for road enforcement services from competitive bidding or competitive proposal requirements and (b) authorizing agreements with the Travis County Sheriff's Office for habitual violator road enforcement services.

Presentation by Tracie Brown, Director of Operations.

**MOTION:** Approve (a) amending the Policy Code to exempt agreements for road enforcement services from competitive bidding or competitive proposal requirements and (b) authorizing agreements with the Travis County Sheriff's Office for habitual violator road enforcement services.

**RESULT:** Approved (Unanimous); 7-0  
**MOTION:** John Langmore

**SECONDED BY:** David Singleton  
**AYE:** Armbrust, Doss, Gaddes, Jenkins, Langmore, Meade, Singleton  
**NAY:** None.  
**ADOPTED AS:** **RESOLUTION NO. 21-052**

### **Briefings and Reports**

**14.** Quarterly update on Projects under construction.

Presentation by Mike Sexton, Acting Director of Engineering.

- A. Bergstrom Expressway (183 South)
- B. 183A Phase III
- C. 183 North Mobility Project

**15.** Executive Director Board Report.

Presentation by James Bass, Executive Director.

- A. Strategic Plan Update
- B. Update on the MoPac South Project
- C. Performance Metrics Dashboard

### **Executive Session**

Chairman Jenkins announced in open session at 11:51 a.m. that the Board would recess the meeting and reconvene in Executive Session to deliberate the following items:

- 16.** 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).
- 17.** Discuss legal issues relating to procurement and financing of Mobility Authority transportation projects, as authorized by §551.071 (Consultation with Attorney).
- 18.** Discuss personnel matters as authorized by §551.074 (Personnel Matters).

After completing the executive session, the Board reconvened in open meeting at 12:13 p.m.

### **Regular Items**

After confirming that no member of the public wished to address the Board, Chairman Jenkins declared the meeting adjourned at 12:13 p.m.

**19.** Adjourn Meeting.



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
**AGENDA ITEM #4**

---

Approve the assignment of the contract for roadway maintenance on 183A Toll and 290E from Angel Brothers Holdings Corp. to Texas Materials Group, Inc.

Strategic Plan Relevance: Regional Mobility  
Department: Engineering  
Contact: Mike Sexton, P.E., Acting Director of Engineering  
Associated Costs: \$0  
Funding Source: N/A  
Action Requested: Consider and act on draft resolution

**Project Description/Background:** The FY20-1 Maintenance Project includes an asphalt overlay and pavement structure repairs, edge milling, and pavement markings on the 183A corridor from Hero Way to Avery Ranch Blvd and on the 290E corridor from Parmer Lane to Gilleland Creek. The FY20-1 Maintenance Project began design in February 2021 as part of the Authority's maintenance program. This project will preserve the existing asphalt pavement structure and extend the pavement life along the 183A Frontage Roads and the east end of 290E.

**Previous Actions & Brief History of the Program/Project:** The FY20-1 Maintenance Project was advertised for bids in May of 2021. In June of 2021, the Authority awarded the FY20-1 Maintenance Project construction contract to Angel Brothers Holdings Corp. In July Angel Brothers Holdings Corp. was acquired by Texas Materials Group, Inc.

Texas Materials Group, Inc. was fully prequalified to bid on the project during the original procurement process. Texas Materials Group, Inc. was one of three contractors to submit a responsive and responsible bid for the project in June 2021.

**Financing:** N/A

**Action requested/Staff Recommendation:** Staff recommends approving the assignment of the FY20-1 Maintenance Project contract to Texas Materials Group, Inc.

**Backup provided:** Draft Resolution

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

**RESOLUTION NO. 21-0XX**

**APPROVING THE ASSIGNMENT OF A CONTRACT FOR THE FY20-1  
MAINTENANCE PROJECT FROM ANGEL BROTHERS HOLDINGS CORP. TO  
TEXAS MATERIALS GROUP, INC.**

WHEREAS, in order to preserve the existing asphalt pavement structure and extend the pavement life along the 183A Frontage Roads and the east end of 290E, the Mobility Authority has planned an asphalt overlay, pavement structure repairs, edge milling, and pavement markings on the 183A corridor from Hero Way to Avery Ranch Blvd and on the 290E corridor from Parmer Lane to Gilleland Creek (the “FY20-1 Maintenance Project”); and

WHEREAS, by Resolution No. 21-042, dated June 30, 2021, the Board approved a contract with Angel Brothers Holding Corp. for the FY-20-1 Maintenance Project; and

WHEREAS, on July 30, 2021, Angel Brothers Holding Corp. was acquired by Texas Materials Group, Inc.; and

WHEREAS, on August 10, 2021, Angel Brothers Holding Corp. submitted a request for the Mobility Authority’s consent to assign the contract for the FY-20-1 Maintenance Project to Texas Materials Group, Inc. which is attached hereto as Exhibit A; and

WHEREAS, Texas Materials Group, Inc. participated in the original procurement for the FY-20-1 Maintenance Project and was determined by staff to be fully qualified to perform the work; and

WHEREAS, the Executive Director recommends that the Board approve the assignment of the contract for FY20-1 Maintenance Project from Angel Brothers Holding Corp. to Texas Materials Group, Inc.

NOW, THEREFORE, BE IT RESOLVED, that the Board hereby approves the assignment of the contract for the FY20-1 Maintenance Project from Angel Brothers Holding Corp. to Texas Materials Group, Inc.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 29<sup>th</sup> day of September 2021.

Submitted and reviewed by:

Approved:

---

Geoffrey Petrov, General Counsel

---

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



**Exhibit A**

Angel Brothers Enterprises, Ltd.

3003 Kilgore Parkway, Bldg. A  
Baytown, Texas 77523-9917 P.O. Box 570  
Baytown, Texas 77522-0570



281.421.5721  
Fax 281.421.2344  
[www.angelbrothers.com](http://www.angelbrothers.com)

TO: **Central Texas Regional Mobility Authority**  
FROM: Angel Brothers Enterprises, Ltd.  
Date: August 10, 2021  
RE: Acquisition of Angel Brothers Enterprises, Ltd. by Texas Materials Group, Inc.

Dear Sir or Madam:

As of July 30th, 2021, certain assets of Angel Brothers Enterprises, Ltd. and its affiliates were acquired by Texas Materials Group, Inc. (FEIN 58-1401466). The acquisition contemplates the assignment of all **Central Texas Regional Mobility Authority** contracts held by Angel Brothers Enterprises, Ltd., subject to receipt of consent to assignment. This letter serves as our request for your consent to the assignment of the attached contracts to Texas Materials Group, Inc. Once your consent is provided, please forward all future payments associated with these contracts to Texas Materials Group, Inc.

After the assignment contemplated by this letter, Angel Brothers Enterprises, Ltd. will maintain its existence; however, it will have no further dealings with **Central Texas Regional Mobility Authority**.

Attached please find the following documents:

1. Assignment and Assumption Agreement
2. Listing of current contracts

If you have any questions, please feel free to contact us at any time, as we are working closely with Texas Materials Group, Inc. to ensure that the transition is as seamless as possible. We appreciate your review of this request and look forward to receipt of your response.

Yours sincerely,

**ANGEL BROTHERS ENTERPRISES, LTD.,**

By:  \_\_\_\_\_

**ASSIGNMENT AND ASSUMPTION AGREEMENT**

THIS ASSIGNMENT AND ASSUMPTION AGREEMENT (this “**Agreement**”) is dated as of July 30, 2021 by and between ANGEL BROTHERS ENTERPRISES, LTD., a Texas limited partnership (“**Asset Seller**”), ANGEL BROTHERS HOLDINGS CORP., a Texas corporation (“**Seller Parent**”), and CENTURY ASPHALT, LTD., a Texas limited partnership (“**Century Asphalt, Ltd.**”, and together with Asset Seller and Seller Parent, the “**Sellers**”) and TEXAS MATERIALS GROUP, INC., a Delaware corporation (the “**Buyer**”). Terms used but not defined herein have the meanings assigned to them in the Purchase Agreement, as defined below.

WHEREAS, the Sellers, the Buyer and the Partnership Interest Sellers are parties to that certain Sale and Purchase Agreement dated as of July 30, 2021 (the “**Purchase Agreement**”); and

WHEREAS, pursuant to and in accordance with the Purchase Agreement, the Sellers desire to sell, transfer, convey, assign and deliver all of their respective rights, title and interest in and to each Purchased Asset, including the Assigned Contracts, to the Buyer, and the Buyer desires to accept and assume, and pay, perform, discharge and satisfy, as and when due, from the Sellers the Assumed Liabilities and perform all of the Sellers’ liabilities, obligations and duties under each Assigned Contract, in each case, as and to the extent provided in the Purchase Agreement.

NOW, THEREFORE, for and in consideration of the terms, conditions and mutual agreements contained in the Purchase Agreement, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

1. Assignment and Assumption of Purchased Assets. Upon the terms and subject to the conditions set forth in the Purchase Agreement, each Seller hereby sells, transfers, conveys, assigns and delivers to the Buyer, all of such Seller’s rights, title and interest in and to each Purchased Asset, including each Assigned Contract, as the case may be, free and clear of all Encumbrances, other than Permitted Encumbrances (the “**Assignment**”), and the Buyer hereby accepts the Assignment. The Buyer hereby assumes from the Sellers and agrees to pay, perform, discharge and satisfy, as and when due, the Assumed Liabilities, including all of the Sellers’ liabilities, obligations and duties under each Assigned Contract, upon the terms and subject to the conditions set forth in the Purchase Agreement. Notwithstanding the foregoing, the Buyer does not assume and shall have no obligation in respect of any of the Excluded Liabilities. The Sellers hereby covenant and agree that they will arrange and defend such sale, transfer, conveyance and delivery against each and every person or persons whomsoever claiming or asserting any claim against any or all of the same.

2. Further Assurance. Each Seller hereby covenants and agrees that it will arrange and defend the sale of the Purchased Assets against each and every person or persons whomsoever claiming or asserting any claim against any or all of the same. In addition, each Seller covenants that it will from time to time at its expense make, execute and deliver, or cause to be made, executed and delivered, such instruments, acts, consents and assurances as the Buyer may reasonably request to sell, convey, transfer to and vest in the Buyer all of the Purchased Assets and to put the Buyer in possession of all of the Purchased Assets.

3. Purchase Agreement. Nothing in this Agreement shall be deemed to supersede, enlarge or modify any of the provisions of the Purchase Agreement, all of which survive the execution and delivery of this Agreement in accordance with the terms set forth in the Purchase Agreement. If any conflict exists between the terms of this Agreement and the Purchase Agreement, the terms of the Purchase Agreement shall govern and control.

4. Binding Effect. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective successors and permitted assigns.

5. Governing Law. All matters arising out of or relating to this Agreement shall be governed by and construed in accordance with the internal laws of the State of Texas without giving effect to the conflict of law provisions thereof to the extent such provisions would require or permit the application of the laws of any jurisdiction other than the State of Texas.

6. Amendment. This Agreement may only be amended, modified or supplemented by an agreement in writing signed by each party hereto.

7. Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. A signed copy of this Agreement delivered by facsimile, email or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

*[Remainder of page intentionally left blank – signature page follows]*

IN WITNESS WHEREOF, the parties hereto have executed this Assignment and Assumption Agreement as of the date first written above.

**Sellers:**

**ANGEL BROTHERS HOLDINGS CORP.,**  
a Texas corporation

By:   
Name: Greg L. Angel  
Title: President

**ANGEL BROTHERS ENTERPRISES, LTD.,**  
a Texas limited partnership

By: **Angel Brothers Holding Corp.,**  
a Texas corporation, as general partner

By:   
Name: Greg L. Angel  
Title: President

By: **Angel Brothers Construction Holding Company, LLC,**  
a Texas limited liability company, as sole limited partner

By: **Angel Brothers Holding Corp.,**  
a Texas corporation, as sole member

By:   
Name: Greg L. Angel  
Title: President

**CENTURY ASPHALT, LTD.,**  
a Texas limited partnership

By: **Century Asphalt Partners Management, L.L.C.,**  
a Texas limited liability company, as general partner  
of Century Asphalt, Ltd.

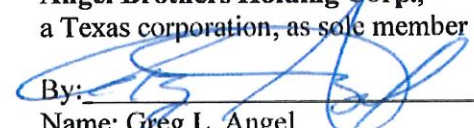
By: **Century Asphalt Holding Company, LLC,**  
a Texas limited liability company, as sole member

By: **Angel Brothers Holding Corp.,**  
a Texas corporation, as sole member

By:   
Name: Greg L. Angel  
Title: President

By: **Century Asphalt Holding Company, LLC,** a Texas  
limited liability company, as sole limited partner of Century  
Asphalt, Ltd.

By: **Angel Brothers Holding Corp.,**  
a Texas corporation, as sole member

By:   
Name: Greg L. Angel  
Title: President

[Signature Page Follows]

**Buyer:**

**TEXAS MATERIALS GROUP, INC.**

By:    
Name: Aaron Price   
Title: President

<u>ABE Job Number</u>	<u>Project Number</u>	<u>Control Number</u>	<u>Job Description</u>	<u>Original Contract Amount</u>
2124	20VARI24601M	N/A	CTRMA-US-189A(FY20-1 MAINTENANCE PROJECT)	\$3,968,858.29





CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
AGENDA ITEM #5

---

Approve a contract with The Levy  
Company, Inc. for large sign  
replacement on 183A Phase II  
(Maintenance Project, 22MAINT-01)

Strategic Plan Relevance:	Regional Mobility
Department:	Engineering
Contact:	Mike Sexton, P.E., Acting Director of Engineering
Associated Costs:	\$447,083.33
Funding Source:	FY22 Operating Budget R&R Funds
Action Requested:	Consider and act on draft resolution

**Project Description/Background:** The 22-MAINT-01 Maintenance Project includes the replacement of large signs along the 183A corridor from RM 2243 to Brushy Creek Rd. The project began design in February 2021 as part of the Authority's maintenance program. This project will restore sign visibility & readability by replacing large overhead and ground mounted signs that have reached the end of their operational life.

**Previous Actions & Brief History of the Program/Project:** In June of 2021, the Authority approved the adoption of the FY2022 Operating Budget which included renewal and replacement funds to maintain the Mobility Authorities existing assets. Final Plans were completed in July 2021 and the project was advertised for bids in August 2021.

Construction Contract Procurement Timeline:

- August 18<sup>th</sup>, 2021: Advertised Project
- August 20<sup>th</sup>, 2021: Pre-Bid Meeting
- September 15<sup>th</sup>, 2021: Bid Opening

Bids: A total of 2 bids were received and came in as shown below.

<b>Contractor</b>	<b>Bid Price</b>	<b>Responsive Bid</b>
The Levy Company, Inc.	\$447,083.33	Yes
DBi Services, LLC	\$484,825.00	Yes

The lowest responsive and responsible bidder is The Levy Company, Inc. at \$447,083.33. The Engineer's Estimate was \$594,107.50

The bid has been reviewed by the Authority staff and the lowest responsive and responsible bidder is The Levy Company, Inc.

**Financing:** FY2022 Operating Budget: Renewal and Replacement Funds

**Action requested/Staff Recommendation:** Staff recommends that the Board award the contract for construction of the 22-MAINT-01 Maintenance Project to The Levy Company, Inc. and authorize the Executive Director to execute a contract with The Levy Company, Inc. in an amount not to exceed \$447,083.33 for construction of the 22-MAINT-01 Maintenance Project.

**Backup provided:** Draft Resolution  
Draft Contract

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

**RESOLUTION NO. 21-0XX**

**AWARDING A CONTRACT WITH THE LEVY COMPANY, INC.  
FOR LARGE SIGN REPLACEMENT ON 183A PHASE II**

WHEREAS, to restore sign visibility and readability along the 183A Phase II corridor from RM 2243 to Brushy Creek Rd, the Mobility Authority seeks to replace large overhead and ground mounted signs that have reached the end of their operational life (the “22-MAINT-01 Project”); and

WHEREAS, the Mobility Authority advertised the 22-MAINT-01 Project on May 6, 2021, and received two bids by the bid opening on June 8, 2021; and

WHEREAS, the Mobility Authority bids were reviewed by engineering staff who determined the lowest responsive and responsible bidder to be The Levy Company; and

WHEREAS, the Executive Director recommends that the Board approve a contract with The Levy Company, Inc. for the 22-MAINT-01 Project in an amount not to exceed \$447,083.33 and in the form published in the bid documents attached hereto as Exhibit A.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Directors approves a contract with The Levy Company, Inc. for the 22-MAINT-01 Project in an amount not to exceed \$447,083.33 and hereby authorizes the Executive Director to finalize and execute the contract in the form published in the bid documents attached hereto as Exhibit A.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 29<sup>th</sup> day of September 2021.

Submitted and reviewed by:

Approved:

\_\_\_\_\_  
Geoffrey Petrov, General Counsel

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

**Exhibit A**



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

**22-MAINT-01**  
**Maintenance Project**

CTRMA Contract No.: 22183A24601M

Bid Documents

Advertisement: August 18, 2021

Pre-Qualification Deadline: 12:00 PM September 1, 2021

Bid Date: 2:00 PM September 15, 2021

Central Texas Regional Mobility Authority

---

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

BID DOCUMENTS  
CONTRACT AND CONTRACT BOND  
SPECIAL PROVISIONS  
SPECIAL SPECIFICATIONS  
PLANS

---

August 18, 2021

Central Texas Regional Mobility Authority

---

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

TABLE OF CONTENTS

	<u>Page</u>
Invitation to Bid .....	1
Bid Document Checklist.....	3
Unofficial Bid Form (To receive Official Bid Form, request via the project’s CivCast website ( <a href="https://www.civcastusa.com/project/605a4be50654de51f38f4e26/summary">https://www.civcastusa.com/project/605a4be50654de51f38f4e26/summary</a> ) .....	5
Bid for 22-MAINT-01 Maintenance Contract.....	6
Non-Collusion Affidavit.....	8
Debarment Affidavit.....	10
Child Support Statement.....	12
Certification To Not Boycott Israel.....	14
Bid Bond .....	15
Contract Agreement.....	17
Information About Proposer Organization .....	20
Performance Bond .....	23
Payment Bond.....	26
Receipt of Addenda .....	28
Engineer’s Seal .....	29

TABLE OF CONTENTS

Page

General Notes.....Section A

Specifications List, Special Provisions & Special Specifications..... Section B

Attachments

Plan Sheets



# CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY

---

## 22-MAINT-01 MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

### INVITATION TO BID

Electronic proposal forms for the above project shall be submitted via the project's CivCast <https://www.civcastusa.com/project/605a4be50654de51f38f4e26/summary> to the Central Texas Regional Mobility Authority (Authority), by **2:00 PM local time, September 15, 2021**. The bids will be publicly posted via the project's CivCast website within 48 hours after the bids are opened.

The contractor will have thirty (30) working days after the date stated in the written Full Notice to Proceed to achieve full completion of all work. The Authority reserves the right to make changes in the work to complete the contract, as defined in the specifications.

Upon execution of the contract, a Partial Notice to Proceed (NTP) may be issued at the sole discretion of the Authority to allow the Contractor to perform such tasks as secure materials on hand, place the field office, produce shop drawings for approval, etc. No time charges will be incurred until a Full NTP is issued.

A Full NTP will be issued no later than 180 calendar days after award for the Contractor to begin work. Time charges will begin accruing upon issuance of the Full NTP.

The complete list of quantities is located in the Bid Form. The principal items of work are as follows:

- Aluminum Signs (TY O)
- Replace Existing Aluminum Signs (TY O)
- Replace Existing Aluminum Signs (TY A)
- Replace Existing Aluminum Signs (TY G)
- Lane Closures

The Official Bid Form for this Contract will be made available to prospective bidders who have met all prequalification requirements on or before 5:00 PM local time, on September 2, 2021 via the project's CivCastUSA website <https://www.civcastusa.com/project/605a4be50654de51f38f4e26/summary>.

Prequalification requirements:

- Be registered with State of Texas,
- Be fully prequalified by Texas Department of Transportation (TxDOT),
- Have a bidding capacity per TxDOT prequalification system of \$1,000,000
- Submit a valid Non-Collusion Affidavit, Debarment Affidavit, Certification to Not Boycott Israel, and Child Support Statement.

The deadline for meeting the prequalification requirements and still obtaining an Official Bid Form is September 1, 2021 at Noon.

The Authority cannot be held liable in the event a party is unable to submit a valid bid due to delay in the prequalification procedure. Securing prequalification through TxDOT and the timing thereof, shall at all times be the sole responsibility of the Prospective Bidder.

Complete Contract documents will be available on August 18, 2021 for potential bidders and others through the Authority's website ([www.mobilityauthority.com](http://www.mobilityauthority.com)) and CivCast's website <https://www.civcastusa.com/project/605a4be50654de51f38f4e26/summary>.

Standard Specifications (Texas Department of Transportation "Standard Specifications for Construction and Maintenance of Highways, Streets and Bridges", November 1, 2014) which form an integral part of this Contract, are available on line at the Texas Department of Transportation (TxDOT) website (<https://www.txdot.gov/business/resources/txdot-specifications.html>).

The contract will be awarded in accordance with the Authority's Procurement policy. A copy of the Procurement Policy is available online at the Authority website: ([https://www.mobilityauthority.com/upload/files/resources/Policy%20Code/32\\_Policy\\_Code\\_Novemeber\\_18,\\_2020.pdf](https://www.mobilityauthority.com/upload/files/resources/Policy%20Code/32_Policy_Code_Novemeber_18,_2020.pdf)).

For more information, please submit a question to the project team through CivCast.com.

Each bid must be accompanied by a Bid Guaranty consisting of a Bid Bond (on the form provided) in the amount of at least five percent (5%) of the Total Bid Amount. The apparent low bidder shall deliver the original sealed Bid Bond to CTRMA within five (5) calendar days of such notification.

CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY  
James Bass, Executive Director  
Austin, Texas

# Central Texas Regional Mobility Authority

---

## 22-MAINT-01 MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

### BID DOCUMENT CHECKLIST

Prior to submitting a bid, prospective bidders should review the checklist below to ensure that the bid is accepted and not declared nonresponsive. No joint venture participants will be allowed.

#### Bid Document:

- Are you aware if your affiliates are bidding on the same project?
- Are you pre-qualified by TxDOT through the Confidential Questionnaire process and have a bidding capacity of \$1,000,000.
- Have you submitted a valid Non-Collusion Affidavit, Debarment Affidavit, and Child Support Statement in order to receive an Official Bid Form?

#### Bid Document Preparation:

- Is the bid being submitted on the Official Bid Form via the CivCast website?
- Are you submitting only one bid for this project?
- Is the bid signed by your company representative or each joint venture participant?
- Have you entered prices for all bid items?
- Does the bid document contain all items included in the Official Bid Form?
- Does the bid document contain a total bid value?
- Is the bid free of any additional conditions not included in the bid document provided to you?
- Have you electronically submitted a complete and executed Bid Bond?
- Have you acknowledged each Addendum on CivCast?

Bid Bonds:

- Is the bid bond signed by the surety?
- Is the bid bond signed by the company representative?
- Is the exact name of the contractor(s) listed as the principal?
- Is the impressed surety seal affixed to the bid bond?
- Does the name on the surety seal match the name of the surety on the bond?
- Is the bond dated on or earlier than the letting date of the project?
- Is the signer for the surety listed on the power of attorney attached to the bond?
- Is the surety authorized to issue the bond?

Bid Document Submission:

- Are you aware of the time and date deadline for submission for the bid document?
- Are you submitting a complete bid document?



**Central Texas Regional Mobility Authority**

---

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

BID FOR 22-MAINT-01 MAINTENANCE PROJECT MAINTENANCE CONTRACT

To the Central Texas Regional Authority  
3300 N I-35, Suite 300  
Austin, Texas 78705

Gentlemen:

I/we, the undersigned, declare: that no other person, firm or corporation is interested in this Bid; that I/we have carefully examined the Plans, Standard Specifications, Special Provisions, and all other documents pertaining to this Contract which form a part of this Bid as if set forth at length herein; that I/we understand that the quantities of items shown herein below are approximate only; that I/we have examined the location of the proposed work; that I/we agree to bind myself/ourselves, upon award to me/us by the Central Texas Regional Authority under this Bid, to enter into and execute a Contract, for the project named above; that I/we agree to start work within thirty (30) calendar days after the date stated in the written Notice-to-Proceed (Item 8.1 of the Specifications), to furnish all necessary materials, provide all necessary labor, equipment, tools and plant, pay for all required insurance, bonds, permits, fees and service, and do all required work in strict compliance with the terms of all documents comprising said Contract, and to fully complete the entire project within thirty (30) working days after Notice-to-Proceed; and that I/we agree to accept as full compensation for the satisfactory prosecution of this project the contractual bid amount after it is adjusted based on the terms and conditions specified in the contract.

The quantities shown in the above schedule of items are considered to be approximate only and are given as the basis for comparison of bids. The Authority may increase or decrease the amount of any item or portion of the work as may be deemed necessary or expedient. Any increase or decrease in the amount of any item or portion of work will be added or deducted from the total Contract bid price based on the terms and conditions specified in TxDOT Specification Item 4. It is understood that payment for this project will be by unit prices bid.

The cost of any work performed, materials furnished, services provided, or expenses incurred, whether or not specifically delineated in the Contract documents but which are incidental to the scope and plans, intent, and completion of this Contract, have been included in the price bid for the various items scheduled hereinabove.

Accompanying this Bid is a bid guaranty consisting of a Bid Bond (on the form provided) in the amount of at least five percent (5%) of the Official Total Bid Amount. It is hereby understood and agreed that said Bid Bond is to be forfeited as liquidated damages in the event that, on the basis of this Bid, the Authority should award this Contract to me/us and that I/we should fail to execute and deliver said Contract and the prescribed Contract Bond, together with the proof of proper insurance coverage and other necessary documents, all within fifteen (15) calendar days after award of the Contract; otherwise, said check or bond is to be returned to the undersigned.

Business Name of Bidder \_\_\_\_\_

Type of Organization            Individual          
   Partnership         
   Corporation     

Address of Bidder: \_\_\_\_\_

\_\_\_\_\_

Signature of Owner,  
Partner or Corp. Officer: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Central Texas Regional Mobility Authority**

\_\_\_\_\_  
22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

NON-COLLUSION AFFIDAVIT

STATE OF \_\_\_\_\_)

COUNTY OF \_\_\_\_\_)

I, \_\_\_\_\_, of the  
City of \_\_\_\_\_, County of \_\_\_\_\_ and State of  
\_\_\_\_\_, being of full age and duly sworn according to law on my oath  
depose and say:

That I am \_\_\_\_\_ (Title) of  
\_\_\_\_\_, the Bidder making  
the Bid submitted to the Central Texas Regional Mobility Authority, on the 15<sup>th</sup> day of  
September, 2021, for Contract No. 22183A24601M in connection with the 22-MAINT-01  
Maintenance Project; that I executed the said Bid with full authority to do so;

The said Bidder has not, directly or indirectly, entered into any combination or  
arrangement with any person, firm or corporation or entered into any agreement, participated in  
any collusion, or otherwise taken any action in restraint of free, competitive bidding or which  
would increase the cost of construction or maintenance in connection with the said Contract; that  
no person or selling agency has been employed or retained to solicit or secure the said Contract  
upon an agreement or understanding for a commission, percentage, brokerage or contingent fee,  
except bona fide full-time employees;



And that said Bidder is or has been a member of the following highway contractors' association during the preceding twelve months:

Name of Association	Location of Principal Office
_____	_____
_____	_____
_____	_____

I further warrant that all statements contained in said Bid and in this Affidavit are true and correct and made with full knowledge that the said Authority relies upon the truth of the statements contained in said Bid and in this Affidavit in awarding the said Contract.

Sworn to and subscribed  
before me this \_\_\_\_\_  
day of \_\_\_\_\_,  
20\_\_.

By: \_\_\_\_\_  
Person Signing Bid

Print Name: \_\_\_\_\_  
Title: \_\_\_\_\_

\_\_\_\_\_  
Notary Public

My commission expires: \_\_\_\_\_

**Central Texas Regional Mobility Authority**

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

DEBARMENT AFFIDAVIT

STATE OF \_\_\_\_\_)

COUNTY OF \_\_\_\_\_)

I, \_\_\_\_\_, of the City  
of \_\_\_\_\_, County of \_\_\_\_\_ and State of  
\_\_\_\_\_, being of full age and duly sworn according to law on my oath  
depose and say:

That I am \_\_\_\_\_ (Title) of  
\_\_\_\_\_, the Bidder making  
the Bid submitted to the Central Texas Regional Mobility Authority, on the 15<sup>th</sup> day of September,  
2021, for Contract No. 22183A24601M in connection with the 22-MAINT-01 Maintenance  
Project; that I executed the said Bid with full authority to do so;

The said Bidder has not been excluded or disqualified from doing business on State or  
Federal projects;

And that said Bidder is or has been a member of the following highway contractors'  
association during the preceding twelve months:

Name of Association	Location of Principal Office
_____	_____
_____	_____
_____	_____

I further warrant that all statements contained in said Bid and in this Affidavit are true and correct and made with full knowledge that the said Authority relies upon the truth of the statements contained in said Bid and in this Affidavit in awarding the said Contract.

Sworn to and subscribed  
before me this \_\_\_\_\_  
day of \_\_\_\_\_,  
20\_\_.

By: \_\_\_\_\_  
Person Signing Bid

Print Name: \_\_\_\_\_  
Title: \_\_\_\_\_

\_\_\_\_\_  
Notary Public

My commission expires: \_\_\_\_\_

## **CHILD SUPPORT STATEMENT**

**Under section 231.006, Family Code, the vendor or applicant certifies that the individual or business entities named in this contract, bid, or application is not ineligible to receive the specified grant, loan, or payment and acknowledges that this contract may be terminated, and payment may be withheld if this certification is inaccurate.**



## CHILD SUPPORT STATEMENT FOR NEGOTIATED CONTRACTS AND GRANTS

Under Family Code, Section 231.006, \_\_\_\_\_  
 Certifies that \_\_\_\_\_,  
 as of \_\_\_\_\_ is eligible to receive a grant, loan or payment and acknowledges  
 that any contract may be terminated and payment may be withheld if this certification is inaccurate.

List below the name and social security number of the individual or sole proprietor and each partner, shareholder, or owner with an ownership interest of at least 25% of the business entity submitting the bid or application. This form must be updated whenever any party obtains a 25% ownership interest in the business entity.

NAME <i>(please print legibly, if handwritten)</i>	SOCIAL SECURITY NUMBER

Family Code, Section 231.006, specifies that a child support obligor who is more than thirty (30) days delinquent in paying child support and a business entity in which the obligor is a sole proprietor, partner, shareholder, or owner with an ownership interest of at least 25% is not eligible to receive payments from state funds under a contract to provide property, materials, or services; or receive a state-funded grant or loan.

A child support obligor or business entity ineligible to receive payments described above remains ineligible until all arrearage have been paid or the obligor is in compliance with a written repayment agreement or court order as to any existing delinquency.

Except as provided in Family Code, Section 231.302(d), a social security number is confidential and may be disclosed only for the purposes of responding to a request for information from an agency operating under the provisions of Subchapters A and D of Title IV of the federal Social Security Act (42 U.S.C. Sections 601 et seq. and 651 et seq.)

## **CERTIFICATION TO NOT BOYCOTT ISRAEL**

Pursuant to Texas Government Code 2271.002, the Mobility Authority must include a provision requiring a written verification that the Contractor does not boycott Israel and will not boycott Israel during the term of the Contract. By signing the contract, the Contractor certifies that it does not boycott Israel and will not boycott Israel during the term of this contract.

Violation of this certification may result in action by the Mobility Authority.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**Central Texas Regional Mobility Authority**

---

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

BID BOND

KNOW ALL PERSONS MEN BY THESE PRESENTS,  
that \_\_\_\_\_, as Principal/Contractor, and  
\_\_\_\_\_, as Surety, legally authorized to do  
business in the State of Texas, are held and firmly bounded unto the Central Texas Regional  
Mobility Authority, as Authority, in the amount of at least five percent (5%) percent of the Total  
Bid amount, on which the Contract is awarded lawful money of the United States of America, for  
the payment of which, well and truly to be made, we bind ourselves, our heirs, executors,  
administrators, successors and assigns, jointly and severally and firmly by these presents:

WHEREAS, the Contractor is herewith submitting its Bid for Contract No.  
22183A24601M, entitled 22-MAINT-01 Maintenance Project, and

NOW, THEREFORE, the condition of this obligation is such, that if the Contractor shall be  
awarded the Contract upon said Bid and shall, within fifteen (15) calendar days after the date of  
written notice of such award, enter into and deliver a signed Contract and the prescribed  
Performance Bond for the faithful performance of the Contract, together with the required proof of  
proper insurance coverage and other necessary documents, then this obligation shall be null and  
void; otherwise, to remain in full force and effect, and the Contractor and Surety will pay unto the  
Authority the difference in money between the amount of the Total Amount written in the Bid of  
said Contractor and the amount for which the Authority may legally contract with another party to  
perform the said work, if the latter amount be in excess of the former; but in no event shall the  
Surety's liability exceed the penal sum hereof.

SIGNED AND SEALED this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_.

**PRINCIPAL/CONTRACTOR**

\_\_\_\_\_  
Business Name

\_\_\_\_\_  
Address

Witness or Attest:

\_\_\_\_\_

By: \_\_\_\_\_

Title:

(Affix Corporate Seal Here)

**SURETY:**

\_\_\_\_\_  
Business Name

\_\_\_\_\_  
Address

Witness or Attest:

\_\_\_\_\_

By: \_\_\_\_\_

Title:

(Attach evidence of Power of Attorney)

(Affix Corporate Seal Here)



**Central Texas Regional Mobility Authority**

---

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

CONTRACT AGREEMENT

THIS AGREEMENT, made this \_\_\_\_ day of \_\_\_\_\_, 20\_\_, between the Central Texas Regional Mobility Authority, 3300 N. I-35, Suite 300, Austin, Texas, 78705, hereinafter called the "Authority" and \_\_\_\_\_, or his, its or their successors, executors, administrators and assigns, hereinafter called the Contractor.

WITNESSETH, that the Contractor agrees with the Authority for the consideration herein mentioned, and at his, its or their own proper cost and expense, to do all the work and furnish all the materials, equipment, teams and labor necessary to prosecute and complete and to extinguish all liens therefore, Contract No. 22183A24601M, entitled 22-MAINT-01 Maintenance Project, in the manner and to the full extent as set forth in the Plans, Standard Specifications, Special Provisions, Bid (for the basis of award stated herein below) and other documents related to said Contract which are on file at the office of the Authority and which are hereby adopted and made part of this Agreement as completely as if incorporated herein, and to the satisfaction of the Authority or its duly authorized representative who shall have at all times full opportunity to inspect the materials to be furnished and the work to be done under this Agreement.

This Contract is awarded on the basis of the official total Bid Amount based on the unit prices bid of \_\_\_\_\_ dollars and \_\_\_\_\_ Cents (\$ \_\_\_\_\_).

In consideration of the foregoing premise, the Authority agrees to pay the Contractor for all items of work performed and materials furnished at the amount of the unit prices bid therefore in the Bid submitted for this Contract, subject to any percentage reductions in the total Contract amount that may be named in the Bid corresponding to the basis of award stated in the above paragraph, and subject to the conditions set forth in the Specifications.

The Contractor agrees as follows:

- a. I/WE will not discriminate against any employee or applicant for employment because of race, religion, color, sex or national origin, except where religion, sex or national origin is a bona fide occupational qualification reasonably necessary to the normal operation of the Contractor.

- b. I/WE agree it is the policy of the Company to assure that applicants are employed, and that employees are treated during employment, without regard to their race, religion, sex, color or national origin, age or disability. Such action shall include: Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship, pre-apprenticeship, and on-the-job training.
- c. I/WE agree to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.
- d. I/WE in any solicitations or advertising for employees placed by or on behalf of itself, will state that it is an equal opportunity employer.
- e. I/WE agree to adhere to all federal/state regulations including, but not limited to, American Disabilities Act, Equal Employment Opportunity, submitting certified payrolls, and participating in Contractor/Subcontractor labor standard reviews.
- f. Notices and advertisements and solicitations placed in accordance with applicable state and federal law, rule or regulation, shall be deemed sufficient for the purposes of meeting the requirements of this section.
- g. Contract Time - The contractor will have thirty (30) working days after the date stated in the written Full Notice-to-Proceed to Fully complete the project.
- h. Failure by Contractor to fulfill these requirements is a material breach of the Contract, which may result in the termination of this Contract, or such other remedy, as the Authority deems appropriate.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement the day and year written above.

Sworn to and Subscribed

CENTRAL TEXAS REGIONAL MOBILITY  
AUTHORITY

before me this \_\_\_\_\_  
day of \_\_\_\_\_, 20\_\_.

By: \_\_\_\_\_

James Bass  
Executive Director

\_\_\_\_\_  
Notary Public

My commission expires:  
\_\_\_\_\_

CONTRACTOR:

\_\_\_\_\_  
Business Name

\_\_\_\_\_  
Address

Sworn to and subscribed  
before me this \_\_\_\_\_  
day of \_\_\_\_\_, 20\_\_\_\_.

\_\_\_\_\_  
by: \_\_\_\_\_  
Notary Public

\_\_\_\_\_  
Title

My commission expires:  
\_\_\_\_\_

(Affix Corporate Seal Here)

**INFORMATION ABOUT PROPOSER ORGANIZATION**

Proposer's business address:

---

(No.) (Street) (Floor or Suite)

---

(City) (State or Providence) (ZIP or Postal Code) (Country)

State or County of Incorporation/Formation/Organization: \_\_\_\_\_

Signature block for a corporation or limited liability company:

Company: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Additional Requirements:

- A. If the proposer is a corporation, enter state or country of incorporation in addition to the business address. If the proposer is a partnership, enter state or country of formation. If the proposer is a limited liability company, enter state or country of organization.
- B. Describe in detail the legal structure of the entity making the Bid. If the proposer is a partnership, attach full name and addresses of all partners and the equity ownership interest of each entity, provide the aforementioned incorporation, formation and organization information for each general partner and attach a letter from each general partner stating that the respective partner agrees to be held jointly and severally liable for any and all of the duties and obligations of the proposer under the Bid and under any contract arising therefrom. If the proposer is a limited liability entity, attach full names and addresses of all equity holders and other financially responsible entities and the equity ownership interest of each entity. If the proposer is a limited liability company, include an incumbency certificate executed by a Secretary thereof in the form set on the following page listing each officer with signing authority and its corresponding office. Attach evidence to the Bid and to each letter that the person signing has authority to do so.
- C. With respect to authorization of execution and delivery of the Bid and the Agreements and validity thereof, if any signature is provided pursuant to a power of attorney, a copy of the power of attorney shall be provided as well as a certified copy of corporate or other appropriate resolutions authorizing said power of attorney. If the Proposer is a corporation, it shall provide evidence of corporate authorization in the form of a resolution of its governing body certified by an appropriate officer of the corporation. If the Proposer is a limited liability company, evidence of authorization would be in the form of a limited company resolution and a managing member resolution providing such authorization, certified by an appropriate officer of the managing member. If the Proposer is a partnership, evidence of authorization shall be provided for the governing body of the Proposer and for the governing bodies of each of its general partners, at all tiers, and in all cases certified by an appropriate officer.
- D. The Proposer must also identify those persons authorized to enter discussions on its behalf with the Authority in connection with this Bid, the Project, and The Agreement. The Proposer shall submit with its Bid a power of attorney executed by the Proposer and each member, partner of the Proposer, appointing and designating one or more individuals to act for and bind the Proposer in all matters relating to the Bid.

INCUMBENCY CERTIFICATE

The undersigned hereby certifies to the Central Texas Regional Mobility Authority that he/she is the duly elected and acting \_\_\_\_\_ Secretary of \_\_\_\_\_ (the "Company"), and that, as such, he/she is authorized to execute this Incumbency Certificate on behalf of the Company, and further certifies that the persons named below are duly elected, qualified and acting officers of the Company, holding on the date hereof the offices set forth opposite their names.

NAME:

OFFICE:

---

---

---

---

---

---

---

---

---

---

---

---

---

---

IN WITNESS WHEREOF, the undersigned has executed this Incumbency Certificate this \_\_\_\_\_ day of \_\_\_\_\_.

---

---

Secretary

**Central Texas Regional Mobility Authority**

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

PERFORMANCE BOND

STATE OF TEXAS  
COUNTY OF \_\_\_\_\_

KNOW ALL MEN BY THESE PRESENTS: That \_\_\_\_\_

\_\_\_\_\_ of the City of \_\_\_\_\_

County of \_\_\_\_\_, and State of \_\_\_\_\_, as principal,  
and

\_\_\_\_\_ authorized under the laws of the State of Texas to act as surety on bonds for principals, are held and firmly bound unto the Central Texas Regional Mobility Authority (Authority), in the penal sum of

\_\_\_\_\_ Dollars

(\$ \_\_\_\_\_) for the payment whereof, the said Principal and Surety bind themselves, their heirs, administrators, executors, successors, jointly and severally, by these presents:

WHEREAS, the Principal has entered into a certain written contract with the Authority, dated the \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_ (the "Contract"), to which the said Contract, along with the Contract Documents referenced therein are hereby referred to and made a part hereof as fully and to the same extent as if copied at length herein.

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION IS SUCH, that if the said Principal shall faithfully perform said Agreement and shall in all respects duly and faithfully observe and perform all and singular the covenants, conditions and agreements in and by the Contract agreed and covenanted by the Principal to be observed and performed, and according to the true intent and meaning of said Contract and the Contract Documents hereto annexed, then this obligation shall be void; otherwise to remain in full force and effect.

PROVIDED, HOWEVER, that this bond is executed pursuant to the provisions of Chapter 2253 of the Texas Government Code, as amended and all liabilities on this bond shall be determined in accordance with the provisions of said Chapter to the same extent as if it were copied at length herein.

SURETY, for value received, stipulates and agrees that no change, extension of time, alteration or addition to the terms of the Agreement or to the work performed thereunder, or to the Contract Documents referenced therein, shall in anyway affect the obligations on this bond, and it does hereby waive notice of such change, extension of time, alteration or addition to the terms on the Agreement, or to the work to be performed thereunder.

IN WITNESS WHEREOF, the said Principal and Surety have signed and sealed this instrument this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_.

\_\_\_\_\_  
PRINCIPAL

\_\_\_\_\_  
SURETY

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
NAME & TITLE

\_\_\_\_\_  
NAME & TITLE

\_\_\_\_\_  
ADDRESS

\_\_\_\_\_  
ADDRESS

(\_\_\_\_\_) \_\_\_\_\_  
PHONE NUMBER

(\_\_\_\_\_) \_\_\_\_\_  
PHONE NUMBER

The name and address of the Resident Agency of Surety is:

\_\_\_\_\_  
\_\_\_\_\_

(\_\_\_\_\_) \_\_\_\_\_  
PHONE NUMBER

\_\_\_\_\_  
SIGNATURE OF LICENSED LOCAL  
RECORDING AGENT appointed to countersign  
on behalf of Surety (Required by Art. 21.09 of the  
Insurance Code)



\*\*\*\*\*

I, \_\_\_\_\_, having executed Bonds  
SIGNATURE

for \_\_\_\_\_ do hereby affirm I have  
NAME OF SURETY

verified that said Surety is now certified with Authority from either: (a) the Secretary of the Treasury of the United States if the project funding includes Federal monies; or (b) the State of Texas if none of the project funding is from Federal sources; and further, said Surety is in no way limited or restricted from furnishing Bond in the State of Texas for the amount and under conditions stated herein.

**Central Texas Regional Mobility Authority**

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

PAYMENT BOND

STATE OF TEXAS  
COUNTY OF \_\_\_\_\_

KNOW ALL MEN BY THESE PRESENTS: That \_\_\_\_\_

\_\_\_\_\_ of the City of \_\_\_\_\_

County of \_\_\_\_\_, and State of \_\_\_\_\_, as Principal  
(hereinafter referred to as the "Principal"), and

\_\_\_\_\_ authorized under the laws of the State of Texas to act as Surety on bonds for principals (hereinafter referred to as the "Surety"), are held and firmly bound unto Central Texas Regional Mobility Authority, (hereinafter referred to as the "Authority"), in the penal sum of

\_\_\_\_\_ Dollars

(\$\_\_\_\_\_) for the payment whereof, the said Principal and Surety bind themselves, their heirs, administrators, executors, successors and assigns, jointly and severally, by these presents:

WHEREAS, the Principal has entered into a certain written contract with the Authority, dated the \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_ (the "Contract"), to which the said Contract, along with the Contract Documents referenced therein are hereby referred to and made a part hereof as fully and to the same extent as if copied at length herein.

NOW, THEREFORE, THE CONDITION OF THIS OBLIGATION IS SUCH, that if the said Principal shall pay all claimants supplying labor and material to him or a subcontractor in the prosecution of the Work provided for in said Contract, then, this obligation shall be void; otherwise to remain in full force and effect.

PROVIDED, HOWEVER, that this bond is executed pursuant to the provisions of Chapter 2253 of the Texas Government Code, as amended and all liabilities on this bond shall be determined in accordance with the provisions of said Chapter to the same extent as if it were copied at length herein.

SURETY, for value received, stipulates and agrees that no change, extension of time, alteration or addition to the terms of the Contract or to the Work performed thereunder, or to the other Contract Documents accompanying the same, shall in anyway affect its obligation on this bond, and it does hereby waive notice of such change, extension of time, alteration or addition to the terms of the Contract, or to the work to be performed thereunder or to the other Contract Documents accompanying the same.

IN WITNESS WHEREOF, the said Principal and Surety have signed and sealed this instrument this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_.

\_\_\_\_\_  
PRINCIPAL

\_\_\_\_\_  
SURETY

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
NAME & TITLE

\_\_\_\_\_  
NAME & TITLE

\_\_\_\_\_  
ADDRESS

\_\_\_\_\_  
ADDRESS

(\_\_\_\_\_) \_\_\_\_\_  
PHONE NUMBER

(\_\_\_\_\_) \_\_\_\_\_  
PHONE NUMBER

The name and address of the Resident Agency of Surety is:

\_\_\_\_\_  
\_\_\_\_\_

(\_\_\_\_\_) \_\_\_\_\_  
PHONE NUMBER

\_\_\_\_\_  
SIGNATURE OF LICENSED LOCAL  
RECORDING AGENT appointed to countersign  
on behalf of Surety (Required by Art. 21.09 of the  
Insurance Code)

**Central Texas Regional Mobility Authority**

---

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

RECEIPT OF ADDENDA

Receipt of addendum, if issued, must be acknowledged electronically on the CivCast website.

Failure to confirm receipt of all addenda issued will result in the bid being deemed non-responsive.

---

Signature

---

Date

Central Texas Regional Mobility Authority

---

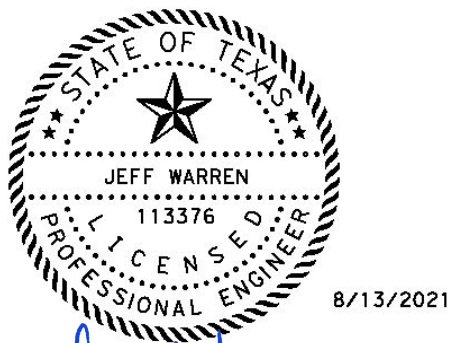
22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

SEALS

The enclosed Specifications, Special Provisions, General Notes, and Specification Data in this document have been selected by me, or under my responsible supervision as being applicable to this project.



Atkins North America, Inc.  
Firm #474

Alteration of a sealed document without proper notification to the responsible engineer is an offence under the Texas Engineering Practice Act.

**Project Number:** 22183A24601M

**County:** Williamson

**Highway:** 183A

**Sheet:**

**Control:**

## **GENERAL NOTES:**

### **GENERAL**

Perform work during good weather. If work is damaged by a weather event, the Contractor is responsible for all costs associated with replacing damaged work.

Remove and replace, at the Contractor's expense, and as directed, all defective work, which was caused by the Contractor's workforce, materials, or equipment.

The "Engineer" shall be the Mobility Authority's consultant identified by the Mobility Authority at the pre-construction meeting.

References to manufacturer's trade name or catalog numbers are for the purpose of identification only. Similar materials from other manufacturers are permitted if they are of equal quality, comply with the specifications for this project, and are approved.

If work is performed at Contractor's option, when inclement weather is impending, and the work is damaged by subsequent precipitation, the Contractor is responsible for all costs associated with replacing the work, if required.

Equip all construction equipment used in roadway work with highly visible omnidirectional flashing warning lights.

Intelligent Transportation Systems (ITS) Infrastructure and Toll Collection System Infrastructure exists within the limits of this project and the system must remain operational throughout construction. Backbone and hub communication fiber links are critical and must be maintained during the duration of the project. Use caution if working in these areas to avoid damaging or interfering with existing facilities and infrastructure. In the event of TxDOT system damage, notify TxDOT at (512) 974-0883 and the Toll Operations Division at (512) 874-9177 within one hour of occurrence. In the event of Mobility Authority Toll system or ITS system damage, notify the Mobility Authority Director of Operations at (512) 996-9778 within one hour of occurrence. Failure of the Contractor to repair damage within 8 hours of occurrence to any infrastructure that conveys any corridor information to TxDOT/Mobility Authority will result in the Contractor being billed for the full cost of emergency repairs performed by others. Damage to any toll collection system infrastructure impacting the ability of the TxDOT/Authority to collect, process or transmit transactions will result in the Contractor being billed for lost revenue damages. Revenue damages will be based on historical revenue collected from the affected gantries.

Use a self-contained vacuum broom to sweep the roadway and keep it free of sediment as directed. The contractor will be responsible for any sweeping above and beyond the normal maintenance required to keep fugitive sediment off the roadway as directed by the Engineer.

Protect all areas of the right of way (ROW), which are not included in the actual limits of the proposed construction areas, from disturbance. Restore any area disturbed because of the Contractor's operations to a condition as good as, or better than, before the beginning of work at no cost to the Mobility Authority.

Remove all loose Formwork and other Materials from the Floodplain or drainage areas, daily, which could float off in a Stormwater Event, as directed.

**Project Number:** 22183A24601M  
**County:** Williamson  
**Highway:** 183A

**Sheet:**  
**Control:**

Damage to existing pipes and SETs due to Contractor operations will be repaired at Contractor's expense.

All locations used for storing construction equipment, materials, and stockpiles of any type, within the ROW, will be as directed. Use of ROW for these purposes will be restricted to those locations where driver sight distance to businesses and side street intersections is not obstructed and at other locations where an unsightly appearance will not exist. The Contractor will not have exclusive use of ROW but will cooperate in the use of the ROW with the city/county, various public utility companies and other contractors as required.

Meet weekly with the Engineer to notify of planned work for the upcoming week. Provide a three-week "look ahead", as well as all work performed over the past week.

Coordinate and obtain approval for all work over existing roadways.

The Project Superintendent will always be available to contact when work is being performed, including subcontractor work. The Superintendent will be available and on-call 24 hours a day.

During evacuation periods for Hurricane events the Contractor will cooperate with the Mobility Authority and TxDOT for the restricting of Lane Closures and arranging for Traffic Control to facilitate Coastal Evacuation Efforts.

Overhead and underground utilities may exist in the vicinity of the project. The exact location of underground utilities may not be known. Refer to ITEM 5 – CONTROL OF THE WORK, for utility rates. If working near power lines, comply with the appropriate sections of Local Legal Requirements, Texas State Law, and Federal Regulations relating to the type of work involved.

Provide vertical clearance for all structures (including overhead sign bridge structures and bridge mounted signs) within the project limits. Submit information and notices to the Mobility Authority.

Contractor is responsible for all toll charges incurred by Contractor vehicles.

#### **ITEM 4 – SCOPE OF WORK**

Final clean up will include the removal of excess material considered detrimental to vegetation growth along the front slope of the ditch. Materials, as specified by the Engineer, will be removed at the Contractor's expense.

#### **ITEM 5 – CONTROL OF THE WORK**

Provide a 48-hour advance email notice to [AUS\\_Locate@txdot.gov](mailto:AUS_Locate@txdot.gov) to request illumination, traffic signal, ITS, or toll equipment utility locates on TxDOT's system (US 183, 183A frontage roads between Brushy Creek and SH 45N). Provide a 48-hour advance notice to the Engineer to request locates on the Mobility Authority's system (183A in areas not mentioned above).

Before the Authority or its contractor begins work on State right of way, the entity performing the work shall provide TxDOT with a fully executed copy of TxDOT's Form 1560 Certificate of Insurance verifying the existence of coverage in the amounts and types specified on the Certificate of Insurance for all persons and entities working on State right of way. This coverage shall be maintained until all work on TxDOT right of way is complete. If coverage is not maintained, all

**Project Number:** 22183A24601M

**County:** Williamson

**Highway:** 183A

**Sheet:**

**Control:**

work on State right of way shall cease immediately, and TxDOT may recover damages and all costs of completing the work.

**Electronic Shop Drawing Submittals:**

Submit electronic shop drawing submittals according using the Mobility Authority's Electronic Data Management System (EDMS), which will be established for the Project prior to commencing construction. Submittals will be addressed to the Engineer and additional staff, as appropriate.

**ITEM 7 – LEGAL RELATIONS AND RESPONSIBILITIES**

Refer to the Environmental Permits, Issues and Commitments (EPIC) plan sheets for additional requirements and permits.

Erosion control and stabilization measures must be initiated immediately in portions of the site where construction activities have temporarily ceased and will not resume for a period of time exceeding 14 calendar days. Track all exposed soil, stockpiles and slopes. Tracking consists of operating 2 tracked vehicles or equipment up and down the slope, leaving track marks perpendicular to the direction of the slope. Re-track slopes and stockpiles after each rain event or every 14 days, whichever occurs first. This work is subsidiary.

Do not park equipment where driver sight distance to businesses and side street intersections is obstructed, especially after work hours. If it is necessary to park where drivers' views are blocked, make every effort to flag traffic accordingly. Give the traveling public first priority.

Perform maintenance of vehicles or equipment at designated maintenance sites. Keep a spill kit on-site during fueling and maintenance. This work is subsidiary.

**Migratory Birds and Bats.**

Migratory birds and bats may be nesting within the project limits and concentrated on roadway structures such as bridges and culverts. Remove all old and unoccupied migratory bird nests from any structures, trees, etc. between September 16 and February 28. Prevent migratory birds from re-nesting or perform construction activities between March 1 and September 15. All methods used for the removal of old nesting areas and the prevention of re-nesting must be submitted to the Mobility Authority 30 business days prior to begin work. This work is subsidiary.

If active nests are encountered on-site during construction, all construction activity within 50 ft. of the nest must stop. Contact the Engineer to determine how to proceed.

No extension of time or compensation payment will be granted for a delay or suspension of work due to the above bird and bat requirements.

**Law Enforcement Personnel.**

A maximum combined rate of \$70 per hour for the law enforcement personnel and the patrol vehicle will be allowed. Any scheduling fee is subsidiary per Standard Specification 502.4.2.

Cancel law enforcement personnel when the event is canceled. Cancellation, minimums or "show up" fees will not be paid when cancellation is made 12 hours prior to beginning of the event. Failure to cancel within 12 hours will not be cause for payment for cancellation, minimums, or "show up" time. Payment of actual "show up" time to the event site due to cancellation will be on



**Project Number:** 22183A24601M  
**County:** Williamson  
**Highway:** 183A

**Sheet:**  
**Control:**

a case by case basis at a maximum of 2 hours per officer. Contractor must use CTRMA provided form to be reimbursed.

Alterations to the cancellation and maximum rate must be approved by the Engineer or pre-determined by official policy of the officers governing authority.

### **Back Up Alarm**

For hours 9 P to 5 A, utilize a non-intrusive, self-adjusting noise level reverse signal alarm. This is not applicable to hot mix or seal coat operations. This is subsidiary.

## **ITEM 8 – PROSECUTION AND PROGRESS**

There will be a 90-calendar day delay start which is to be used for the fabrication of signs starting from written Limited Notice to Proceed provided by the Mobility Authority.

The Contractor will have 30 working days from NTP to have all installations complete.

Electronic versions of schedules will be saved in native format and delivered in native and PDF formats.

Working days will be charged based on a standard workweek. Working days will be charged Monday through Friday, excluding national or state holidays, if weather or other conditions permit the performance of the principal unit of work underway, as determined by the Engineer, for a continuous period of at least 7 hr. between 7:00 A.M. and 6:00 P.M., unless otherwise shown in the Contract. The Contractor has the option of working on Saturdays or state holidays. Provide sufficient advance notice to the Engineer when scheduling work on Saturdays. Work on Sundays and national holidays will not be permitted without written permission of the Engineer. If work requiring an Inspector to be present is performed on a Saturday, Sunday, or holiday, and weather or other conditions permit the performance of work for 7 hr. between 7:00 A.M. and 6:00 P.M., a working day will be charged.

Provide via email a 3-week look-ahead schedule in Gantt chart format. Submit weekly by noon on Friday. Designate each activity as night or day shift and include the name of the foreman or contractor. The chart shall have a specific section dedicated solely to lane closures and detours. Each lane closure and detour shall be an individual item on the schedule.

Lane Closure Assessments will be assessed as shown in the **Table 1** below.

Any unauthorized lane closures will result in an assessment to the Contractor of \$1,000 per lane per hour or the assigned Lane Closure Assessments in the table, whichever is the higher amount.

All Lane Closure Assessments for the Contractor will be subtracted from the value of the payment application for that associated period.

**Table 1: Lane Closure Assessment Rates**

Lane Closure Period	Late Charges (Per Lane)			
	183A		US 183 & 183A FR	
	Lane	Shoulder	Lane	Shoulder
<b>0-15 mins</b>	\$1,000	\$1,000	\$1,000	\$1,000
<b>15-30 mins</b>	\$2,000	\$2,000	\$2,000	\$2,000
<b>30-45 mins</b>	\$3,000	\$3,000	\$3,000	\$3,000
<b>45-60 mins</b>	\$4,000	\$4,000	\$4,000	\$4,000
<b>Every additional 15-minute interval after 1 hour</b>	\$2,000	\$2,000	\$2,000	\$2,000

For example: If the contractor has one lane of traffic closed on US 183 until Monday at 5:32 a.m., the contractor is 32 minutes outside of the allowable lane closure period. The late charges will be accrued as follows:

$$1 \text{ lane closed} \times [\$1,000 + \$1,000 + \$1,000] = \$3000$$

Emergency lane closures are not subject to lane closure assessments. Emergency lane closures are defined as closures caused by circumstances other than those caused by the contractor and shall be approved by the authority.

Refer to Table 2. Allowable Lane Closure of Item 7001-RMA Lane Closures for available lane closure times.

**ITEM 9 – MEASUREMENT AND PAYMENT**

Provide full-time, off-duty, uniformed, certified peace officers in officially marked vehicles, as part of traffic control operations, as directed.

Show proof of certification by the Texas Commission on Law Enforcement Standards.

No payment will be made for peace officers unless the Contractor completes the proper Department tracking form. Submit invoices that agree with the tracking form for payment at the end of each month, when approved services were provided. Request the tracking form from the Department.

No payment for officers used for moving equipment without prior written approval.

Cancel “Off-Duty” Peace Officers and their Motor Vehicle Units when the Scheduled lane closures are canceled. Failure to cancel the Off-Duty Officers and their respective Motor Vehicle Units will not be the cause for payment, by Mobility Authority, for “Show Up” time.

**ITEM 502 – BARRICADES, SIGNS, AND TRAFFIC HANDLING**

Cover, relocate or remove existing signs that conflict with traffic control. Install all permanent signs, delineation, and object markers required for the operation of the roadway before opening to

**Project Number:** 22183A24601M

**County:** Williamson

**Highway:** 183A

**Sheet:**

**Control:**

traffic. Use of temporary mounts is allowed or may be required until the permanent mounts are installed or not impacted by construction. Maintain the temporary mounts. This work is subsidiary.

Do not set up traffic control when the pavement is wet.

Maintain access to all streets and driveways at all times, unless otherwise approved. Considered subsidiary to the pertinent Items.

#### **ITEM 600s – LIGHTING, SIGNING, MARKINGS, AND SIGNALS**

Use materials from Material Producer List as shown on the TxDOT website (TxDOT.gov > Business > Resources). Furnish new material as required per Standard Specification.

Meet the requirements of the NEC, Texas MUTCD, TxDOT standards, and TxDOT Standard Specifications. If existing elements shown to remain do not meet the codes or specifications, provide notice to the Engineer.

#### **ITEM 636 – ALUMINUM SIGNS**

All signs that are to be replaced should have the old sign removed and the new sign placed within the same day and the same operation and setup.

Contractor shall use new hardware to attach new ground mount and overhead signs to existing structure. This work is subsidiary to the various bid items.

Contractor will retain ownership of replaced signs.

#### **ITEM 6001 – PORTABLE CHANGEABLE MESSAGE SIGN**

Provide 2 “Electronic” Portable Changeable Message Sign(s) (EPCMS) as part of the traffic control operation. All EPCMS will be exclusive to this project, unless otherwise approved. Placement location and message as directed.

Place appropriate number of “Electronic” Portable Changeable Message Signs (EPCMS) at locations requiring lane closures for one-week prior to the closures, or as directed. Obtain approval for the actual message that will appear on the boards. If more than two phases of a message are required per board, provide additional EPCMS’s to meet the two-phases-per-board requirement. Provide a replacement within 12 hours. EPCMS will be available for traffic control, event notices, roadway conditions, service announcements, etc.

#### **ITEM 6185 – TRUCK MOUNTED ATTENUATOR AND TRAILER ATTENUATOR**

A TMA/TA shall be used when installing and removing a TCP setup. This work is subsidiary to item 7001-RMA Lane Closures.

The contractor will be responsible for determining if one or more operations will be ongoing at the same time to determine the total number of TMA/TA required for the project.

TMA/TA used to protect damaged attenuators will be paid by the day using the force account item for the repair.

**ITEM 7001-RMA – LANE CLOSURES**

Table 2. Allowable Lane Closure

Roadway	Limits	Allowable Closure Time*
		Weekday
183A	SH 45 to San Gabriel Pkwy	9 P to 5 A
183A Frontage Roads	SH 45 to San Gabriel Pkwy	9 P to 5 A
All	Within 200' of a signalized intersection	9 P to 5 A

\* Allowable Closure Time includes setup and cleanup time.

No closures will be allowed the weekends adjacent to, working day prior, and working day after the National Holidays defined in the Standard Specifications and Easter weekend. No closures will be allowed on Friday and the weekends for Austin City Limits Fest, Formula 1 United States Grand Prix, South by Southwest, UT home football games, Republic of Texas Rally, Rodeo Austin or other special events that could be impacted by the construction. All lanes will be open by noon of the day before these special events. The closure restrictions may be amended by the Engineer.

For any events at the Cedar Park Events Center on 183A Toll, lane closures from the event center to 2 miles south of the event center are not permitted 2 hours preceding the start time of an event, and 2 hours following the end time of an event. Event dates for which this restriction will be warranted will be determined on a monthly basis, as the event calendar is available.

To account for directional traffic volumes, begin and end times of closures may be shifted equally by the Engineer. The closure duration will remain. Added compensation is not allowed.

Submit an emailed request for a lane closure notification (LCN) to the Mobility Authority/TxDOT representative. The email will be submitted in the format provided. Receive concurrence prior to implementation. Submit a cancellation of lane closures a minimum of 18 hours prior to implementation.

Blanket requests for extended periods are not allowed. Max duration of a request is 2 weeks prior to requiring resubmittal. Provide 2-hour notice prior to implementation and immediately upon removal of the closure.

Submit the request a minimum of 48 hours prior to the closure and by the following deadline immediately prior to the closure: 11A on Tuesday or 11A on Friday.

For all roadways: Submit request for traffic detours and full roadway closures 168 hours prior to implementation.

Maintain a minimum of 1 through lane in each direction, unless otherwise directed in plans.

Cancellations of accepted closures (not applicable to full closures or detours) due to weather will not require resubmission in accordance with the above restrictions if the work is completed during the next allowable closure time.

**Project Number:** 22183A24601M

**County:** Williamson

**Highway:** 183A

**Sheet:**

**Control:**

In the case of an unauthorized lane closure, all approved LCNs will be revoked until a meeting is held between the contractor and the Engineer. No lane closure notices will be approved until the meeting is concluded.

Meet with the Engineer prior to lane closures to ensure that sufficient equipment, materials, devices, and workers will be used. Take immediate action to modify traffic control, if at any time backup (queuing) becomes greater than 20 minutes. Have a contingency plan of how modification will occur. Consider inclement weather prior to implementing the lane closures.

In the case of an unauthorized lane closure, all approved LCNs will be revoked until a meeting is held between the contractor and the Engineer. No lane closure notices will be approved until the meeting is concluded.

Coordinate Main Lane closures with adjacent projects including those projects owned by other agencies and departments.

Closures that conflict with adjacent contractor will be prioritized according to critical path work per latest schedule. Conflicting critical path or non-critical work will be approved for first LCN submitted. Denial of a closure due to prioritization or other reasons will not be reason for time suspension, delay, overhead, etc.

Maintain a minimum of **1** through lane in each direction on the 183A frontage roads, during all hours.

Shadow Vehicle with TMA is required for setup/removal of traffic control devices.

TMA(s) shall be subsidiary to Item 7001-RMA - Lane Closure.

**Central Texas Regional Mobility Authority**

---

22-MAINT-01  
MAINTENANCE PROJECT

CONTRACT NO. 22183A24601M

\*\*\*\*\*

SPECIFICATION LIST

PREFACE:

The "Standard Specifications for Construction and Maintenance of Highways, Streets, and Bridges" of the Texas Department of Transportation, 2014, as amended and augmented by the Supplemental Specifications following, shall govern the performance of the Contract. These specifications hereby are made a part of the Contract as fully and with the same effect as if set forth at length herein.

Attention is directed to the fact that any other documents printed by the Texas Department of Transportation modifying or supplementing said "Standard Specifications", such as Standard Supplemental Specifications, Special Provisions (by the Department), Notice to Bidders, etc., do not form a part of this Contract nor govern its performance, unless specifically so-stated in the Supplemental Specifications herein contained.

Attention is directed to the use of "Proposal" in standard TxDOT documents included in this contract (Standard Specifications, Special Provisions, & Special Specifications) is equivalent to "Bid" in the Mobility Authority's documents. This shall be accounted for when working contract documents prepared by the Mobility Authority with those standards prepared by TxDOT.

Attention is directed to the use of "Department" in standard TxDOT documents included in this contract (Standard Specifications, Special Provisions, & Special Specifications) is equivalent to "Mobility Authority" in the Mobility Authority's documents.

References made to specific section numbers in these Special Provisions, or in any of the various documents which constitute the complete Contract Documents, shall, unless otherwise denoted, be construed as referenced to the corresponding section of the "Standard Specifications" issued by the Texas Department of Transportation in 2014.

CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY  
GOVERNING SPECIFICATIONS AND SPECIAL PROVISIONS

(STANDARD SPECIFICATIONS, SPECIAL PROVISIONS, AND SPECIAL SPECIFICATIONS)

WHERE DISCREPANCIES OCCUR BETWEEN THE TECHNICAL SPECIFICATIONS, THE FOLLOWING DESCENDING ORDER OF PRIORITY SHALL GOVERN: (1) SPECIAL CONDITIONS, (2) SPECIAL PROVISIONS TO SPECIAL SPECIFICATIONS, (3) SPECIAL SPECIFICATIONS, (4) SPECIAL PROVISIONS, AND (5) STANDARD SPECIFICATIONS.

ALL SPECIFICATIONS AND SPECIAL PROVISIONS APPLICABLE TO THIS PROJECT ARE IDENTIFIED AS FOLLOWS:

STANDARD SPECIFICATIONS: ADOPTED BY THE TEXAS DEPARTMENT OF TRANSPORTATION NOVEMBER 1, 2014. STANDARD SPECIFICATIONS ARE INCORPORATED INTO THE CONTRACT BY REFERENCE.

ITEMS 1-9 GENERAL REQUIREMENTS AND COVENANTS

ITEM 500 MOBILIZATION

ITEM 502 BARRICADES, SIGNS, AND TRAFFIC HANDLING

ITEM 636 SIGNS (643)

SPECIAL PROVISIONS: SPECIAL PROVISIONS WILL GOVERN AND TAKE PRECEDENCE OVER THE SPECIFICATIONS ENUMERATED HEREON WHEREVER IN CONFLICT THEREWITH.

SPECIAL PROVISION TO ITEM 000 (000---002---RMA)

SPECIAL PROVISION TO ITEM 000 (000---008)

SPECIAL PROVISION TO ITEM 000 (000---009)

SPECIAL PROVISION TO ITEM 000 (000---011---RMA)

SPECIAL PROVISION TO ITEM 000 (000---658)

SPECIAL PROVISION TO ITEM 000 (000---659)

SPECIAL PROVISION TO ITEM 000 (000---954---RMA)

SPECIAL PROVISION TO ITEM 001 (001---001---RMA)

SPECIAL PROVISION TO ITEM 002 (002---005---RMA)

SPECIAL PROVISION TO ITEM 002 (002---011)

SPECIAL PROVISION TO ITEM 003 (003---005---RMA)  
SPECIAL PROVISION TO ITEM 003 (003---011)  
SPECIAL PROVISION TO ITEM 004 (004---001---RMA)  
SPECIAL PROVISION TO ITEM 005 (005---002)  
SPECIAL PROVISION TO ITEM 005 (005---003)  
SPECIAL PROVISION TO ITEM 006 (006---001---RMA)  
SPECIAL PROVISION TO ITEM 006 (006---012)  
SPECIAL PROVISION TO ITEM 007 (007---003---RMA)  
SPECIAL PROVISION TO ITEM 007 (007---004)  
SPECIAL PROVISION TO ITEM 007 (007---011)  
SPECIAL PROVISION TO ITEM 008 (008---002---RMA)  
SPECIAL PROVISION TO ITEM 008 (008---003)  
SPECIAL PROVISION TO ITEM 008 (008---030)  
SPECIAL PROVISION TO ITEM 008 (008---033)  
SPECIAL PROVISION TO ITEM 009 (009---001---RMA)  
SPECIAL PROVISION TO ITEM 009 (009---011)  
SPECIAL PROVISION TO ITEM 502 (502---008)  
SPECIAL PROVISION TO ITEM 636 (636---001)  
SPECIAL PROVISION TO ITEM 643 (643---001)  
SPECIAL PROVISION TO SPECIAL SPECIFICATION ITEM 6185 (6185---002)

SPECIAL SPECIFICATIONS:

ITEM 6001 PORTABLE CHANGEABLE MESSAGE SIGN

ITEM 6185 TRUCK MOUNTED ATTENUATOR (TMA) AND TRAILER ATTENUATOR (TA)

ITEM 7001-RMA LANE CLOSURES (502) (6185)

GENERAL:

THE ABOVE-LISTED SPECIFICATION ITEMS ARE THOSE UNDER WHICH PAYMENT IS TO BE MADE. THESE, TOGETHER WITH SUCH OTHER PERTINENT ITEMS, IF ANY, AS MAY BE REFERRED TO IN THE ABOVE-LISTED SPECIFICATION ITEMS, AND INCLUDING THE SPECIAL PROVISIONS LISTED ABOVE, CONSTITUTE THE COMPLETE SPECIFICATIONS FOR THIS PROJECT.



---

# Special Provision to Item 000

## Nondiscrimination

---

### 1. DESCRIPTION

The Contractor agrees, during the performance of the service under this Agreement, that the Contractor shall provide all services and activities required in a manner that complies with the Civil Rights Act of 1964, as amended, the Rehabilitation Act of 1973, Public Law 93-1122, Section 504, the provisions of the Americans with Disabilities Act of 1990, Public Law 101-336 (S.933), and all other federal and state laws, rules, regulations, and orders pertain to equal opportunity in employment, as if the Contractor were an entity bound to comply with these laws. The Contractor shall not discriminate against any employee or applicant for employment based on race, religion, color, sex, national origin, age or handicapped condition.

---

### 2. DEFINITION OF TERMS

Where the term "Contractor" appears in the following six nondiscrimination clauses, the term "Contractor" is understood to include all parties to Contracts or agreements with the Texas Department of Transportation.

---

### 3. NONDISCRIMINATION PROVISIONS

During the performance of this Contract, the Contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "Contractor") agrees as follows:

- 3.1. **Compliance with Regulations.** The Contractor (hereinafter includes consultants) will comply with the Acts and the Regulations relative to Nondiscrimination in Federally-assisted programs of the U.S. Department of Transportation, the Federal Highway Administration, as they may be amended from time to time, which are herein incorporated by reference and made a part of this Contract.
- 3.2. **Nondiscrimination.** The Contractor, with regard to the work performed by it during the Contract, will not discriminate on the grounds of race, color, or national origin in the selection and retention of subcontractors, including procurements of materials and leases of equipment. The Contractor will not participate directly or indirectly in the discrimination prohibited by the Acts and the Regulations, including employment practices when the Contract covers any activity, project, or program set forth in Appendix B of 49 CFR Part 21.
- 3.3. **Solicitations for Subcontracts, Including Procurements of Materials and Equipment:** In all solicitations, either by competitive bidding, or negotiation made by the Contractor for work to be performed under a subcontract, including procurements of materials, or leases of equipment, each potential subcontractor or supplier will be notified by the Contractor of the Contractor's obligations under this Contract and the Acts and the Regulations relative to Nondiscrimination on the grounds of race, color, or national origin.
- 3.4. **Information and Reports:** The Contractor will provide all information and reports required by the Acts, the Regulations, and directives issued pursuant thereto and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by the Recipient or the Federal Highway Administration to be pertinent to ascertain compliance with such Acts, Regulations, and instructions. Where any information required of a Contractor is in the exclusive possession of another who fails or refuses to furnish the information, the Contractor will so certify to the Recipient or the Federal Highway Administration, as appropriate, and will set forth what efforts it has made to obtain the information.
- 3.5. **Sanctions for Noncompliance.** In the event of a Contractor's noncompliance with the Nondiscrimination provisions of this Contract, the Recipient will impose such Contract sanctions as it or the Federal Highway Administration may determine to be appropriate, including, but not limited to:

- withholding payments to the Contractor under the Contract until the Contractor complies, and/or
- cancelling, terminating, or suspending a Contract, in whole or in part.

3.6. **Incorporation of Provisions.** The Contractor will include the provisions of paragraphs (3.1) through (3.6) in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Acts, the Regulations, and directives issued pursuant thereto. The Contractor will take action with respect to any subcontract or procurement as the Recipient or the Federal Highway Administration may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if the Contractor becomes involved in, or is threatened with litigation by a subcontractor, or supplier because of such direction, the Contractor may request the Recipient to enter into any litigation to protect the interests of the Recipient. In addition, the Contractor may request the United States to enter into the litigation to protect the interests of the United States.

---

#### 4. PERTINENT NONDISCRIMINATION AUTHORITIES:

During the performance of this Contract, the Contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "Contractor") agrees to comply with the following nondiscrimination statutes and authorities; including but not limited to:

- 4.1. Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d et seq., 78 stat. 252), (prohibits discrimination on the basis of race, color, national origin); and 49 CFR Part 21.
- 4.2. The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 U.S.C. § 4601), (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects);
- 4.3. Federal-Aid Highway Act of 1973, (23 U.S.C. § 324 et seq.), (prohibits discrimination on the basis of sex);
- 4.4. Section 504 of the Rehabilitation Act of 1973, (29 U.S.C. § 794 et seq.), as amended, (prohibits discrimination on the basis of disability); and 49 CFR Part 27;
- 4.5. The Age Discrimination Act of 1975, as amended, (42 U.S.C. § 6101 et seq.), (prohibits discrimination on the basis of age);
- 4.6. Airport and Airway Improvement Act of 1982, (49 U.S.C. § 4 71, Section 4 7123), as amended, (prohibits discrimination based on race, creed, color, national origin, or sex);
- 4.7. The Civil Rights Restoration Act of 1987, (PL 100-209), (Broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, The Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms "programs or activities" to include all of the programs or activities of the Federal-aid recipients, subrecipients and Contractors, whether such programs or activities are Federally funded or not);
- 4.8. Titles II and III of the Americans with Disabilities Act, which prohibit discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities (42 U.S.C. §§ 12131-12189) as implemented by Department of Transportation regulations at 49 C.F.R. parts 37 and 38;
- 4.9. The Federal Aviation Administration's Nondiscrimination statute (49 U.S.C. § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex);
- 4.10. Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, which ensures discrimination against minority populations by discouraging programs,

policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations;

- 4.11. Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, you must take reasonable steps to ensure that LEP persons have meaningful access to your programs (70 Fed. Reg. at 74087 to 74100);
- 4.12. Title IX of the Education Amendments of 1972, as amended, which prohibits you from discriminating because of sex in education programs or activities (20 U.S.C. 1681 et seq).

# Special Provision to Item 000

## Special Labor Provisions for State Projects



### 1. GENERAL

This is a "Public Works" Project, as provided under Government Code Title 10, Chapter 2258, "Prevailing Wage Rates," and is subject to the provisions of the Statute. No provisions in the Contract are intended to be in conflict with the provisions of the Statute.

The Texas Transportation Commission has ascertained and indicated in the special provisions the regular rate of per diem wages prevailing in each locality for each craft or type of worker. Apply the wage rates contained in the specifications as minimum wage rates for the Contract.

### 2. MINIMUM WAGES, HOURS AND CONDITIONS OF EMPLOYMENT

All workers necessary for the satisfactory completion of the work are within the purview of the Contract.

Whenever and wherever practical, give local citizens preference in the selection of labor.

Do not require any worker to lodge, board or trade at a particular place, or with a particular person as a condition of employment.

Do not charge or accept a fee of any from any person who obtains work on the project. Do not require any person who obtains work on the project to pay any fee to any other person or agency obtaining employment for the person on the project.

Do not charge for tools or equipment used in connection with the duties performed, except for loss or damage of property. Do not charge for necessary camp water.

Do not charge for any transportation furnished to any person employed on the project.

The provisions apply where work is performed by piece work, station work, etc. The minimum wage paid will be exclusive of equipment rental on any shipment which the worker or subcontractor may furnish in connection with his work.

Take responsibility for carrying out the requirements of this specification and ensure that each subcontractor working on the project complies with its provisions.

Any form of subterfuge, coercion or deduction designed to evade, reduce or discount the established minimum wage scales will be considered a violation of the Contract.

The Fair Labor Standards Acts (FLSA) established one and one-half (1-1/2) pay for overtime in excess of 40 hours worked in 1 week. Do not consider time consumed by the worker in going to and returning from the place of work as part of the hours of work. Do not require or permit any worker to work in excess of 40 hours in 1 week, unless the worker receives compensation at a rate not less than 1-1/2 times the basic rate of pay for all hours worked in excess of 40 hours in the workweek.

The general rates of per diem wages prevailing in this locality for each class and type of workers whose services are considered necessary to fulfill the Contract are indicated in the special provisions, and these rates govern as minimum wage rates on this Contract. A penalty of \$60.00 per calendar day or portion of a calendar day for each worker that is paid less than the stipulated general rates of per diem wages for any work done under the Contract will be deducted. The Department, upon receipt of a complaint by a worker,

will determine within 30 days whether good cause exists to believe that the Contractor or a subcontractor has violated wage rate requirements and notify the parties involved of the findings. Make every effort to resolve the alleged violation within 14 days after notification. The next alternative is submittal to binding arbitration in accordance with the provisions of the Texas General Arbitration Act (Art. 224 et seq., Revised Statutes).

Notwithstanding any other provision of the Contract, covenant and agree that the Contractor and its subcontractors will pay each of their employees and contract labor engaged in any way in work under the Contract, a wage not less than what is generally known as the "federal minimum wage" as set out in 29 U.S.C. 206 as that Statute may be amended from time to time.

Pay any worker employed whose position is not listed in the Contract, a wage not less than the per diem wage rate established in the Contract for a worker whose duties are most nearly comparable.

---

### 3. RECORD AND INSPECTIONS

Keep copies of weekly payrolls for review. Require subcontractors to keep copies of weekly payrolls for review. Show the name, occupation, number of hours worked each day and per diem wage paid each worker together with a complete record of all deductions made from such wages. Keep records for a period of 3 years from the date of completion of the Contract.

Where the piece-work method is used, indicate on the payroll for each person involved:

- Quantity of piece work performed.
- Price paid per piece-work unit.
- Total hours employed.

The Engineer may require the Contractor to file an affidavit for each payroll certifying that payroll is a true and accurate report of the full wages due and paid to each person employed.

Post or make available to employees the prevailing wage rates from the Contract. Require subcontractors to post or make available to employees the prevailing wage rates from the Contract.

# Special Provision to Item 000

## Small Business Enterprise in State Funded Projects



### 1. DESCRIPTION

The purpose of this Special Provision is to carry out the Texas Department of Transportation's policy of ensuring that Small Business Enterprise (SBE) has an opportunity to participate in the performance of contracts. If the SBE goal is greater than zero, Article A of this Special Provision shall apply to this Contract; otherwise, Article B of this Special Provision applies. The percentage goal for SBE participation in the work to be performed under this contract will be shown in the proposal.

### 2. DEFINITIONS

Small Business Enterprise (SBE) is a firm (including affiliates) certified by the Department whose annual gross receipts do not exceed the U.S. Small Business Administration's size standards for 4 consecutive years. Firms certified as Historically Underutilized Businesses (HUBs) by the Texas Comptroller of Public Accounts and as Disadvantaged Business Enterprises (DBEs) by the Texas Uniform Certification Program automatically qualify as SBEs.

#### 2.1. Article A - SBE Goal is Greater than Zero.

2.1.1. **Policy.** The Department is committed to providing contracting opportunities for small businesses. In this regard, it is the Department's policy to develop and maintain a program in order to facilitate contracting opportunities for small businesses. Consequently, the requirements of the Department's Small Business Enterprise Program apply to this contract as follows:

2.1.1.1. The Contractor shall make a good faith effort to meet the SBE goal for this contract.

2.1.1.2. The Contractor and any Subcontractors shall not discriminate on the basis of race, color, national origin, age, disability or sex in the award and performance of this contract. These nondiscrimination requirements shall be incorporated into any subcontract and purchase order.

2.1.1.3. After a conditional award is made to the low bidder, the Department will determine the adequacy of a Contractor's efforts to meet the contract goal, as is outlined under Section 2, "Contractor's Responsibilities." If the requirements of Section 2 are met, the contract will be forwarded to the Contractor for execution.

The Contractor's performance, during the construction period of the contract in meeting the SBE goal, will be monitored by the Department.

2.1.2. **Contractor's Responsibilities.** These requirements must be satisfied by the Contractor. A SBE Contractor may satisfy the SBE requirements by performing at least 25% of the contract work with its own organization as defined elsewhere in the contract.

2.1.2.1. The Contractor shall submit a completed SBE Commitment Agreement Form for each SBE they intend to use to satisfy the SBE goal so as to arrive in the Department's Office of Civil Rights (OCR) in Austin, Texas not later than 5:00 p.m. on the 10th business day, excluding national holidays, after the conditional award of the contract. When requested, additional time, not to exceed 7 business days, excluding national holidays, may be granted based on documentation submitted by the Contractor.

2.1.2.2. A Contractor who cannot meet the contract goal, in whole or in part, shall document the good faith efforts taken to meet the SBE goal. The Department will consider as good faith efforts all documented explanations

that are submitted and that describe a Contractor's failure to meet a SBE goal or obtain SBE participation, including:

- 2.1.2.2.1. Advertising in general circulation, trade association, and/or minority/women focus media concerning subcontracting opportunities,
- 2.1.2.2.2. Dividing the contract work into reasonable portions in accordance with standard industry practices,
- 2.1.2.2.3. Documenting reasons for rejection or meeting with the rejected SBE to discuss the rejection,
- 2.1.2.2.4. Providing qualified SBEs with adequate information about bonding, insurance, plans, specifications, scope of work, and the requirements of the contract,
- 2.1.2.2.5. Negotiating in good faith with qualified SBEs, not rejecting qualified SBEs who are also the lowest responsive bidder, and;
- 2.1.2.2.6. Using the services of available minorities and women, community organizations, contractor groups, local, state and federal business assistance offices, and other organizations that provide support services to SBEs.
- 2.1.2.3. The good faith effort documentation is due at the time and place specified in Subarticle 2.(a). of this Special Provision. The Director of the DBE & SBE Programs Section will evaluate the Contractor's documentation. If it is determined that the Contractor has failed to meet the good faith effort requirements, the Contractor will be given an opportunity for reconsideration by the Department.
- 2.1.2.4. Should the bidder to whom the contract is conditionally awarded refuse, neglect or fail to meet the SBE goal and/or demonstrate to the Department's satisfaction sufficient efforts to obtain SBE participation, the proposal guaranty filed with the bid shall become the property of the State, not as a penalty, but as liquidated damages to the Department.
- 2.1.2.5. The Contractor must not terminate a SBE subcontractor submitted on a commitment agreement for a contract with an assigned goal without the prior written consent of the Department.
- 2.1.2.6. The Contractor shall designate a SBE contact person who will administer the Contractor's SBE program and who will be responsible for submitting reports, maintaining records, and documenting good faith efforts to use SBEs.
- 2.1.2.7. The Contractor must inform the Department of the representative's name, title and telephone number within 10 days of beginning work.
- 2.1.3. **Eligibility of SBEs.**
- 2.1.3.1. The Department certifies the eligibility of SBEs.
- 2.1.3.2. The Department maintains and makes available to interested parties a directory of certified SBEs.
- 2.1.3.3. Only firms certified at the time of letting or at the time the commitments are submitted are eligible to be used in the information furnished by the Contractor required under Section 2.(a) above.
- 2.1.3.4. Certified HUBs and DBEs are eligible as SBEs.
- 2.1.3.5. Small Business Size Regulations and Eligibility is referenced on e-CFR (Code of Federal Regulations), Title 13 – Business Credit and Assistance, Chapter 1 – Small Business Administration, Part 121 – Small Business Size Regulations, Subpart A – Size Eligibility Provisions and Standards.
- 2.1.4. **Determination of SBE Participation.** SBE participation shall be counted toward meeting the SBE goal in this contract in accordance with the following:

- 2.1.4.1. A Contractor will receive credit for all payments actually made to a SBE for work performed and costs incurred in accordance with the contract, including all subcontracted work.
- 2.1.4.2. A SBE Contractor or subcontractor may not subcontract more than 75% of a contract. The SBE shall perform not less than 25% of the value of the contract work with its own organization.
- 2.1.4.3. A SBE may lease equipment consistent with standard industry practice. A SBE may lease equipment from the prime contractor if a rental agreement, separate from the subcontract specifying the terms of the lease arrangement, is approved by the Department prior to the SBE starting the work in accordance with the following:
- 2.1.4.3.1. If the equipment is of a specialized nature, the lease may include the operator. If the practice is generally acceptable with the industry, the operator may remain on the lessor's payroll. The operator of the equipment shall be subject to the full control of the SBE, for a short term, and involve a specialized piece of heavy equipment readily available at the job site.
- 2.1.4.3.2. For equipment that is not specialized, the SBE shall provide the operator and be responsible for all payroll and labor compliance requirements.
- 2.1.5. **Records and Reports.**
- 2.1.5.1. The Contractor shall submit monthly reports, after work begins, on SBE payments, (including payments to HUBs and DBEs). The monthly reports are to be sent to the Area Engineer's office. These reports will be due within 15 days after the end of a calendar month.
- These reports will be required until all SBE subcontracting or supply activity is completed. The "SBE Progress Report" is to be used for monthly reporting. Upon completion of the contract and prior to receiving the final payment, the Contractor shall submit the "SBE Final Report" to the Office of Civil Rights and a copy to the Area Engineer. These forms may be obtained from the Office of Civil Rights and reproduced as necessary. The Department may verify the amounts being reported as paid to SBEs by requesting, on a random basis, copies of invoices and cancelled checks paid to SBEs. When the SBE goal requirement is not met, documentation supporting Good Faith Efforts, as outlined in Section 2.(b) of this Special Provision, must be submitted with the Final Report.
- 2.1.5.2. SBE subcontractors and/or suppliers should be identified on the monthly report by SBE certification number, name and the amount of actual payment made to each during the monthly period. **These reports are required regardless of whether or not SBE activity has occurred in the monthly reporting period.**
- 2.1.5.3. All such records must be retained for a period of 3 years following completion of the contract work and shall be available at reasonable times and places for inspection by authorized representatives of the Department.
- 2.1.6. **Compliance of Contractor.** To ensure that SBE requirements of this contract are complied with, the Department will monitor the Contractor's efforts to involve SBEs during the performance of this contract. This will be accomplished by a review of monthly reports submitted by the Contractor indicating his progress in achieving the SBE contract goal and by compliance reviews conducted by the Department.
- A Contractor's failure to comply with the requirements of this Special Provision shall constitute a material breach of this contract. In such a case, the Department reserves the right to employ remedies as the Department deems appropriate in the terms of the contract.
- 2.2. **Article B - No SBE Goal.**
- 2.2.1. **Policy.** It is the policy of the Department that SBEs shall have an opportunity to participate in the performance of contracts. Consequently, the requirements of the Department's Small Business Enterprise Program apply to this contract as specified in Section 2-5 of this Article.



- 2.2.2. **Contractor's Responsibilities.** If there is no SBE goal, the Contractor will offer SBEs an opportunity to participate in the performance of contracts and subcontracts.
- 2.2.3. **Prohibit Discrimination.** The Contractor and any subcontractor shall not discriminate on the basis of race, color, national origin, religion, age, disability or sex in the award and performance of contracts. These nondiscrimination requirements shall be incorporated into any subcontract and purchase order.
- 2.2.4. **Records and Reports.**
- 2.2.4.1. The Contractor shall submit reports on SBE (including HUB and DBE) payments. The reports are to be sent to the Area Engineer's office. These reports will be due annually by the 31<sup>st</sup> of August or at project completion, whichever comes first.
- These reports will be required until all SBE subcontracting or supply activity is completed. The "SBE Progress Report" is to be used for reporting. Upon completion of the contract and prior to receiving the final payment, the Contractor shall submit the "SBE Final Report" to the Office of Civil Rights and a copy to the Area Engineer. These forms may be obtained from the Office of Civil Rights and reproduced as necessary. The Department may verify the amounts being reported as paid to SBEs by requesting copies of invoices and cancelled checks paid to SBEs on a random basis.
- 2.2.4.2. SBE subcontractors and/or suppliers should be identified on the report by SBE Certification Number, name and the amount of actual payment made.
- 2.2.4.3. All such records must be retained for a period of 3 years following completion of the contract work and shall be available at reasonable times and places for inspection by authorized representatives of the Department.

---

## Special Provision to Item 000

### Buy America

---

Steel and iron products to be incorporated into the project must be of domestic origin. All manufacturing processes for steel and iron products to be incorporated into the project must take place domestically, including donated material.

**Reminders:**

Depending on the Steel/iron item received at the project, described below are the requirements for acceptance.

**1. Steel and Iron Items Inspected and Tested by CSTIM&P**

- The project engineer receives CST/M&P Structural Test Reports as proof of compliance with the requirements of the specification.
- CST/M&P obtains from the supplier a completed Form 1818 (D-9-USA-1), "Material Statement" with attached MTRs, certifications, galvanizing reports, etc.

**2. Steel and Iron Items Received and Sampled by the Project Engineer for Testing by CSTIM&P**

- The project engineer submits samples with the required documentation obtained from the supplier (completed Form 1818 (D-9-USA-1) with attached MTRs, certifications, galvanizing reports, etc.) to CST/M&P for testing.
- CSTM&P issues a CST/M&P General Test Report for all passing material (proof of compliance with the requirements of the specifications).

**3. Steel and Iron Items Received, Inspected, and Accepted by the Project Engineer**

- The project engineer obtains from the supplier the completed Form 1818 (D-9-USA-1) with attached MTRs, certifications, galvanizing reports, etc.
- CST/M&P assists the project engineer when requested.

**4. Steel and Iron Items Received from Regional or District Warehouse (Pretested) Stock**

- The project engineer obtains documentation verifying the material was obtained from a regional or district warehouse.
- CSTM&P, when requested to inspect and test, obtains from the supplier the completed Form 1818 (D-9-USA-1) with attached MTRs, etc.

# Special Provision to Item 000

## Schedule of Liquidated Damages



**Table 1**  
**Schedule of Liquidated Damages**

For Dollar Amount of Original Contract		Dollar Amount of Daily Contract Administration Liquidated Damages per Working Day
From More Than	To and Including	
0	100,000	570
100,000	500,000	590
500,000	1,000,000	610
1,000,000	1,500,000	685
1,500,000	3,000,000	785
3,000,000	5,000,000	970
5,000,000	10,000,000	1,125
10,000,000	20,000,000	1,285
20,000,000	Over 20,000,000	2,590

In addition to the amount shown in Table 1, the Liquidated Damages will be increased by the amount shown in Item 8 of the General Notes for Road User Cost (RUC), when applicable.

# Special Provision 000

## Notice of Contractor Performance Evaluations



### 1. GENERAL

In accordance with Texas Transportation Code §223.012, the Engineer will evaluate Contractor performance based on quality, safety, and timeliness of the project.

### 2. DEFINITIONS

- 2.1. **Project Recovery Plan (PRP)**—a formal, enforceable plan developed by the Contractor, in consultation with the District, that documents the cause of noted quality, safety, and timeliness issues and specifies how the Contractor proposes to correct project-specific performance deficiencies.

In accordance with Title 43, Texas Administrative Code (TAC), §9.23, the District will request a PRP if the Contractor's performance on a project is below the Department's acceptable standards and will monitor the Contractor's compliance with the established plan.

- 2.2. **Corrective Action Plan (CAP)**—a formal, enforceable plan developed by the Contractor, and proposed for adoption by the Construction or Maintenance Division, that documents the cause of noted quality, safety, and timeliness issues and specifies how the Contractor proposes to correct statewide performance deficiencies.

In accordance with 43 TAC §9.23, the Division will request a CAP if the average of the Contractor's statewide final evaluation scores falls below the Department's acceptable standards for the review period and will monitor the Contractor's compliance with the established plan.

### 3. CONTRACTOR EVALUATIONS

In accordance with Title 43, Texas Administrative Code (TAC) §9.23, the Engineer will schedule evaluations at the following intervals, at minimum:

- Interim evaluations—at or within 30 days after the anniversary of the notice to proceed, for Contracts extending beyond 1 yr., and
- Final evaluation—upon project closeout.

In case of a takeover agreement, neither the Surety nor its performing Contractor will be evaluated.

In addition to regularly scheduled evaluations, the Engineer may schedule an interim evaluation at any time to formally communicate issues with quality, safety, or timeliness. Upon request, work with the Engineer to develop a PRP to document expectations for correcting deficiencies.

Comply with the PRP as directed. Failure to comply with the PRP may result in additional remedial actions available to the Engineer under Item 5, "Control of the Work." Failure to meet a PRP to the Engineer's satisfaction may result in immediate referral to the Performance Review Committee for consideration of further action against the Contractor.

The Engineer will consider and document any events outside the Contractor's control that contributed to the failure to meet performance standards or comply with a PRP, including consideration of sufficient time.

Follow the escalation ladder if there is a disagreement regarding an evaluation or disposition of a PRP. The Contractor may submit additional documentation pertaining to the dispute. The District Engineer's decision

on a Contractor's evaluation score and recommendation of action required in a PRP or follow up for non-compliance is final.

---

#### 4. **DIVISION OVERSIGHT**

Upon request of the Construction or Maintenance Division, develop and submit for Division approval a proposed CAP to document expectations for correcting deficiencies in the performance of projects statewide.

Comply with the CAP as directed. The CAP may be modified at any time up to completion or resolution after written approval of the premise of change from the Division. Failure to meet an adopted or revised adopted CAP to the Division's satisfaction within 120 days will result in immediate referral to the Performance Review Committee for consideration of further action against the Contractor.

The Division will consider and document any events outside the Contractor's control that contributed to the failure to meet performance standards or comply with a CAP, including consideration of sufficient time and associated costs as appropriate.

---

#### 5. **PERFORMANCE REVIEW COMMITTEE**

The Performance Review Committee, in accordance with 43 TAC §9.24, will review at minimum all final evaluations, history of compliance with PRPs, any adopted CAPs including agreed modifications, any information about events outside a Contractor's control contributing to the Contractor's performance, and any documentation submitted by the Contractor and may recommend one or more of the following actions:

- take no action,
- reduce the Contractor's bidding capacity,
- prohibit the Contractor from bidding on one or more projects,
- immediately suspend the Contractor from bidding for a specified period of time, by reducing the Contractor's bidding capacity to zero, or
- prohibit the Contractor from being awarded a Contract on which they are the apparent low bidder.

The Deputy Executive Director will determine any further action against the Contractor.

---

#### 6. **APPEALS PROCESS**

In accordance with 43 TAC §9.25, the Contractor may appeal remedial actions determined by the Deputy Executive Director.

---

## **Special Provision 000**

### **Certificate of Interested Parties (Form 1295)**

---

Submit a Form 1295, "Certificate of Interested Parties," in the following instances:

- at contract execution for contracts awarded by the Mobility Authority;
- at any time there is an increase of \$300,000 or more to an existing contract (change orders, extensions, and renewals); or
- at any time there is a change to the information in Form 1295, when the form was filed for an existing contract.

Form 1295 and instructions on completing and filing the form are available on the Texas Ethics Commission website.

---

# Special Provision to Item 1

## Abbreviations and Responsibilities

---

Item 1, "Abbreviations and Definitions," of the Standard Specifications, is hereby amended with respect to the clauses cited below, and no other clauses or requirements of this Item are waived or changed hereby.

**Article 1.** is supplemented with the following:

### 1.0. General Statement:

For this Contract, the Standard Specifications for Construction and Maintenance of Highways, Streets and Bridges, November 1, 2014 (the "Texas Standard Specifications"), all documents referenced therein, and all manuals, bulletins, supplements, specifications, and similar materials issued by the Texas Department of Transportation ("TxDOT"), or any predecessor or successor thereto, which are applicable to this Contract, are hereby modified with respect to the terms cited below and no others are changed hereby.

The term "State", "State of Texas", "State Highway Agency", "State Highway Department Of Texas", "State Department of Highways and Public Transportation", "Texas State Department Of Highways and Public Transportation", "Texas Department of Transportation", "Department", "Texas Turnpike Authority", "State Department of Highways and Public Transportation Commission", "Texas Department of Transportation Commission", "Texas Transportation Commission", or "State Highway Commission", shall, in the use of The Texas Standard Specifications, Special Provisions and Special Specifications and General Notes and Specification Data pertaining thereto, and required contract provisions for Federal-Aid construction contracts, for all work in connection with Central Texas Regional Mobility Authority, projects and all extensions enlargements, expansions, improvements, and rehabilitations thereto, be deemed to mean Central Texas Regional Mobility Authority, unless the context clearly indicates a contrary meaning.

**Article 2, "Abbreviations,"** is supplemented with the following:

CTRMA Central Texas Regional Mobility Authority

**Article 3.28., "Commission"**, is voided and replaced by the following:

3.28. Commission. The Central Texas Regional Mobility Authority Board or authorized representative.

**Article 3.32., "Construction Contract"**, is voided and replaced by the following:

3.32. Construction Contract. The agreement between the Central Texas Regional Mobility Authority and the Contractor establishing the obligations of the parties for furnishing of materials and performance of the work prescribed in the Contract Documents.

**Article 3.45., "Debar (Debarment)"**, is voided and replaced by the following:

3.45. Debar (Debarment). Action taken by the Mobility Authority, federal government or state government pursuant to regulation that prohibits a person or company from entering into a Contract, or from participating as a subcontractor, or supplier of materials or equipment used in a highway improvement Contract as defined in Transportation Code, Chapter 223, Subchapter A.

**Article 3.47., "Department"**, is voided and replaced by the following:

3.47. Department. Central Texas Regional Mobility Authority, unless the context clearly indicates a contrary intent and meaning.

**Article 3.48., "Departmental Material Specifications"**, is voided and replaced by the following:

3.48. Departmental Material Specifications (DMS). Reference specifications for various materials published by the Texas Department of Transportation Construction Division.

**Article 3.54., "Engineer"**, is hereby deleted and replaced by the following:

3.54 Engineer. The Central Texas Regional Mobility Authority Coordinator or their duly authorized representative.

**Article 3.73., "Letting Official"**, is hereby deleted and replaced by the following:

3.73. Letting Official. An employee of the Central Texas Regional Mobility Authority empowered by the Central Texas Regional Mobility Authority to officially receive bids and close the receipt of bids at a letting.

**Article 3.79., "Manual of Testing Procedures"**, is voided and replaced by the following:

3.79. Manual of Testing Procedures. Texas Department of Transportation manual outlining test methods and procedures maintained by the Materials and Pavements Section of the Construction Division.

**Article 3.102., "Proposal Form"**, is voided and replaced by the following:

3.012. Proposal Form. The document issued by the Central Texas Regional Mobility Authority for a proposed Contract that includes:

- the specific locations (except for non-site-specific work) and description of the proposed work;
- an estimate of the various quantities and kinds of work to be performed or materials to be furnished;
- a schedule of items for which unit prices are requested;
- the number of working days within which the work is to be completed (or reference to the requirements); and
- the special provisions and special specifications applicable to the proposed Contract.

**Article 3.108., "Referee Tests"**, is voided and replaced by the following:

3.108. Referee Tests. Tests requested to resolve differences between Contractor and Engineer test results. The referee laboratory is the Texas Department of Transportation Construction Division Materials and Pavement Section, or mutually agreed to 3rd party commercial laboratory.

**Article 3.129., "State"**, is voided and replaced by the following:

3.129. State. Central Texas Regional Mobility Authority.

**3.156. Mobility Authority.** The Central Texas Regional Mobility Authority, an agency created under Texas Transportation Code Chapter 370 and approved by the Texas Transportation Commission, together with its members, partners, employees, agents officers, directors, shareholders, representatives, consultants, successors, and assigns. The Mobility Authority's principal office is presently located at 3300 N. I-35, Suite 300, Austin, Texas 78705.



**3.157. Bid Form.** The form provided by the Mobility Authority used by the bidder to submit a bid. Electronic bid forms for the project shall be submitted via the project's CivCast website.

**3.158. Full Completion of all Work (or to Fully Complete all Work).** The completion of all work specified under this Contract as evidenced by the Formal Acceptance thereof by the Mobility Authority.

**3.159. Standards.** Whenever the Plans and/or Specifications refer to "Standard Sheets" or "Design Details" such reference shall be construed to mean the set of drawings issued by the Design Divisions, Texas Department of Transportation, and entitled "Standard Sheets". Only those standards or standard drawings specifically referred to by number on the Plans or in the various Contract Documents are applicable to work on this Contract.

Whenever in the various Contract Documents term, "Department" or "State" appears, it shall be replaced by the term, "Central Texas Regional Mobility Authority." Similarly, the term, "Executive Director" shall be replaced by the term, "Central Texas Regional Mobility Authority Coordinator".

Whenever in the Texas Department of Transportation Specifications and Standard Drawings the term, "Department" or "Texas Department of Transportation" appears, it shall be replaced by the term, "Central Texas Regional Mobility Authority," except in references to said Texas Department of Transportation as being the author of certain Specifications and Standard Drawings, and in reference to said Department as the agency prequalifying prospective Bidders.

Whenever in the Texas Department of Transportation Specifications and Standard Drawing the term, "District Engineer" appears, it shall be replaced by the term, "Central Texas Regional Mobility Authority Coordinator".

---

## Special Provision to Item 2

### Instructions to Bidders

---

Item 2, "Instructions to Bidders" of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 2.3., "Issuing Proposal Forms,"** first two sentences are replaced with the following:

Mobility Authority will issue an Official Bid Form to a prequalified Bidders. The online bid form will be made available to the prequalified bidders on the CivcastUSA website: <https://www.civcastusa.com/project/605a4be50654de51f38f4e26/summary>

Prequalification requirements:

- Be registered with State of Texas,
- Be fully prequalified by Texas Department of Transportation (TxDOT),
- Have a bidding capacity per TxDOT prequalification system of \$1,000,000,
- Email a valid Non-Collusion Affidavit, Debarment Affidavit, and Child Support Statement to [Marco.Castro@atkinsglobal.com](mailto:Marco.Castro@atkinsglobal.com) and [Zane.Reid@atkinsglobal.com](mailto:Zane.Reid@atkinsglobal.com) include a phone number, email address and physical address for point of contact.

**Article 2.3., "Issuing Proposal Forms,"** is supplemented by the following:

The Department may not issue a proposal form if one or more of the following apply:

- The Contractor has been defaulted in accordance with Article 8.7., "Default of Contract" (a default for performance) on a previous Contract with the Department within the last 3 years
- The Contractor is not in compliance with Texas Government Code Sections 2155.089 and 2262.055.

## Special Provision to Item 2

### Instructions to Bidders



Item 2, "Instructions to Bidders," of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 2.3., "Issuing Proposal Forms,"** is supplemented by the following:

- the Bidder or affiliate of the Bidder that was originally determined as the apparent low Bidder on a project, but was deemed nonresponsive for failure to register or participate in the Department of Homeland Security's (DHS) E-Verify system as specified in Article 2.15., "Department of Homeland Security (DHS) E-Verify System," is prohibited from rebidding that specific project.

**Article 2.7., "Nonresponsive Bid,"** is supplemented by the following:

- the Bidder failed to participate in the Department of Homeland Security's (DHS) as specified in Article 2.15., "Department of Homeland Security (DHS) E-Verify System."

**Article 2.15., "Department of Homeland Security (DHS) E-Verify System,"** is added.

The Department will not award a Contract to a Contractor that is not registered in the DHS E-Verify system. Remain active in E-Verify throughout the life of the contract. In addition, in accordance with paragraph six of Article 8.2, "Subcontracting," include this requirement in all subcontracts and require that subcontractors remain active in E-Verify until their work is completed.

If the apparent low Bidder does not appear on the DHS E-Verify system prior to award, the Department will notify the Contractor that they must submit documentation showing that they are compliant within 5-business days after the date the notification was sent. A Contractor who fails to comply or respond within the deadline will be declared non-responsive and the Department will execute the proposal guaranty. The proposal guaranty will become the property of the State, not as a penalty, but as liquidated damages. The Bidder forfeiting the proposal guaranty will not be considered in future proposals for the same work unless there has been a substantial change in the scope of the work.

The Department may recommend that the Commission:

- reject all bids, or
- award the Contract to the new apparent low Bidder, if the Department is able to verify the Bidder's participation in the DHS E-verify system. For the Bidder who is not registered in E-Verify, the Department will allow for one business day after notification to provide proof of registration.

If the Department is unable to verify the new apparent low Bidder's participation in the DHS E-Verify system within one calendar day:

- the new apparent low Bidder will not be deemed nonresponsive,
- the new apparent low Bidder's guaranty will not be forfeited,
- the Department will reject all bids, and
- the new apparent low Bidder will remain eligible to receive future proposals for the same project.

## Special Provision to Item 3

### Award and Execution of Contract

Item 3, "Award and Execution of Contract" of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 1, "Award of Contract,"** is deleted in its entirety and replaced with the following:

The Mobility Authority will award or reject the Contract within 60 calendar days after the opening of the proposal at the sole discretion of the Mobility Authority.

**Article 4.3., "Insurance,"** is supplemented by the following:

The Contractor shall be the named insured, and the following entities shall be additional insureds on a primary and non-contributory basis: Central Texas Regional Mobility Authority, Texas Department of Transportation.

These entities shall be additional insureds to this policy with respect to liability arising out of the acts, errors, and omissions of any member of the Contractor and Subcontractors whether occurring on or off of the site, notwithstanding any other provisions of the Contract Documents, the project policy shall not be canceled, except for non-payment of premium, fraud, material misrepresentation, or noncompliance with reasonable loss control recommendations.

The Authority Board, the Authority, Texas Department of Transportation, the State of Texas, the Commission and their respective successors, assigns, officeholders, officers, directors, commissioners, consultants and employees shall be listed as "additional insureds" with respect to any insurance for which the contractor must obtain an "additional insured" rider or amendment.

**Table 2** is deleted in its entirety and replaced with the following:

Type of Insurance	Amount of Coverage
Commercial General Liability Insurance	Including products/completed operations liability and contractual liability , in the amount of \$1,000,000 per occurrence for bodily injury and property damage
Business Automobile Policy	In the amount of \$1,000,000 per occurrence for bodily injury and property damage
Workers' Compensation	Providing statutory benefits, and Employers Liability with limits of \$1,000,000
Excess Liability Insurance	In the amount of \$5,000,000 per occurrence and aggregate

---

## Special Provision to Item 3 Award and Execution Contract

---



Item 3, Award and Execution of Contract," of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Section 4.3, "Insurance."** The first sentence is voided and replaced by the following:

For construction and building Contracts, submit a certificate of insurance showing coverages in accordance with Contract requirements. For routine maintenance Contracts, refer to Article 8, "Beginning of Work."

**Article 8, "Beginning of Work."** The first sentence is supplemented by the following:

For a routine maintenance Contract, do not begin work until a certificate of insurance showing coverages in accordance with the Contract requirements is provided and accepted.

---

## Special Provision to Item 4

### Scope of Work

---

Item 4, "Scope of Work," of the Standard Specifications, is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 4.4., "Changes in the Work,"** Delete the following paragraph:

"If the changes in quantities or the alternations do not significantly change the character of the work under the Contract, the altered work will be paid for at the Contract unit price. If the changes in quantities or the alterations significantly change the character of the work, the Contract will be amended by a change order. If no unit price exists, this will be considered extra work and the Contract will be amended by a change order. Provide cost justification as requested, in an acceptable format. Payment will not be made for anticipated profits on work that is eliminated."

and replace with the following:

"The Engineer may require deviations to the Work through a written directive. Payment for the deviations and quantity overruns will be made through the Contingency Allowance. Deviations and quantity overruns will be paid for at the unit prices submitted at the bidding stage. Deviations requiring new unit prices will be negotiated and made through the Contingency Allowance. Costs exceeding the Contingency Allowance will be addressed using the change order process.

Upon completion of the Work, the total contract value will be adjusted to provide for the difference, if any, between the total amount of expenditures from the Contingency Allowance and the original amount of the Contingency Allowance. The Contractor is not entitled to all or any part of an unexpended balance of the Contingency Allowance.

When changes are made that do not fall under the Contingency Allowance, the Contract will be amended by a Change Order. Provide cost justification as requested, in an acceptable format. Payment will not be made for anticipated profits on work that is eliminated."

**Article 4.6., "Requests for Additional Compensation and Damages,"** is supplemented by the following:

"Contractor shall not be eligible for Change Order(s) for additional compensation for additional costs, including costs for developing and executing a Recovery Schedule(s), and delay and disruption damages, or additional Days incurred directly or indirectly from the virus known as severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and the disease known as COVID-19, including any disruptions to, and delays or interruptions in, construction of the Project in accordance with the Contract and any approved Baseline Schedule."

---

## Special Provision to Item 5

### Control of the Work

---



Item 5, "Control of the Work," of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 5.1, "Authority of Engineer,"** is voided and replaced by the following.

The Engineer has the authority to observe, test, inspect, approve, and accept the work. The Engineer decides all questions about the quality and acceptability of materials, work performed, work progress, Contract interpretations, and acceptable Contract fulfillment. The Engineer has the authority to enforce and make effective these decisions.

The Engineer acts as a referee in all questions arising under the terms of the Contract. The Engineer's decisions will be final and binding.

The Engineer will pursue and document actions against the Contractor as warranted to address Contract performance issues. Contract remedies include, but are not limited to, the following:

- conducting interim performance evaluations requiring a Project Recovery Plan, in accordance with Title 43, Texas Administrative Code (TAC) §9.23,
- requiring the Contractor to remove and replace defective work, or reducing payment for defective work,
- removing an individual from the project,
- suspending the work without suspending working day charges,
- assessing standard liquidated damages to recover the Department's administrative costs, including additional project-specific liquidated damages when specified in the Contract in accordance with 43 TAC §9.22,
- withholding estimates,
- declaring the Contractor to be in default of the Contract, and
- in case of a Contractor's failure to meet a Project Recovery Plan, referring the issue directly to the Performance Review Committee for consideration of further action against the Contractor in accordance with 43 TAC §9.24.

The Engineer will consider and document any events outside the Contractor's control that contributed to the failure to meet performance standards, including consideration of sufficient time.

Follow the issue escalation ladder if there is disagreement regarding the application of Contract remedies.

---

## Special Provision to Item 5

### Control of the Work

---



Item 5, "Control of the Work" of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 5.4, "Coordination of Plans, Specifications, and Special Provisions," the last sentence of the last paragraph is replaced by the following:**

Failure to promptly notify the Engineer will constitute a waiver of all contract claims against the Department for misunderstandings or ambiguities that result from the errors, omissions, or discrepancies.



---

## Special Provision to Item 6

### Control of Materials

---

For this project, Item 6, "Control of Materials," of the Standard Specifications, is hereby amended with respect to the clauses cited below, and no other clauses or requirements of this Item are waived or changed hereby.

**Article 1., "Source Control,"** is supplemented by the following:

The use of convict-produced materials is prohibited per 23 CFR 635.417.

There shall be no local preference for the purchasing of materials.

**Article 4., "Sampling, Testing, and Inspection,"** is supplemented by the following:

Quality Control testing of all materials, construction items, or products incorporated in the work shall be performed by the Contractor according to the contract specifications at the Contractor's expense.

Quality Assurance sampling and testing for acceptance will be performed by the Mobility Authority's Construction Representative/Observer in accordance with the Quality Control (QC) / Quality Assurance (QA) program outlined in the Quality Assurance Plan (QAP). The cost of such tests will be incurred by the Mobility Authority and coordinated by the Mobility Authority's Construction Representative/Observer through funds made available to the Construction Representative/Observer under his/her agreement with the Mobility Authority for the professional services related to construction engineering and inspection on the Project.

## Special Provision to Item 6

### Control of Materials



Item 6, "Control of Materials" of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 6.10., "Hazardous Materials,"** is voided and replaced by the following:

Comply with the requirements of Article 7.12., "Responsibility for Hazardous Materials."

Notify the Engineer immediately when a visual observation or odor indicates that materials on sites owned or controlled by the Department may contain hazardous materials. Except as noted herein, the Department is responsible for testing, removing, and disposing of hazardous materials not introduced by the Contractor. The Engineer may suspend work wholly or in part during the testing, removing, or disposing of hazardous materials, except in the case where hazardous materials are introduced by the Contractor.

Use materials that are free of hazardous materials. Notify the Engineer immediately if materials are suspected to contain hazardous materials. If materials delivered to the project by the Contractor are suspected to contain hazardous materials, have an approved commercial laboratory test the materials for the presence of hazardous materials as approved. Remove, remediate, and dispose of any of these materials found to contain hazardous materials. The work required to comply with this section will be at the Contractor's expense if materials are found to contain hazardous materials. Working day charges will not be suspended and extensions of working days will not be granted for activities related to handling hazardous material introduced by the Contractor. If suspected materials are not found to contain hazardous materials, the Department will reimburse the Contractor for hazardous materials testing and will adjust working day charges if the Contractor can show that this work impacted the critical path.

**10.1. Painted Steel Requirements.** Coatings on existing steel contain hazardous materials unless otherwise shown on the plans. Remove paint and dispose of steel coated with paint containing hazardous materials in accordance with the following:

**10.1.1. Removing Paint From Steel** For contracts that are specifically for painting steel, Item 446, "Field Cleaning and Painting Steel" will be included as a pay item. Perform work in accordance with that item.

For projects where paint must be removed to allow for the dismantling of steel or to perform other work, the Department will provide for a separate contractor (third party) to remove paint containing hazardous materials prior to or during the Contract. Remove paint covering existing steel shown not to contain hazardous materials in accordance with Item 446, "Field Cleaning and Painting Steel."

**10.1.2. Removal and Disposal of Painted Steel.** For steel able to be dismantled by unbolting, paint removal will not be performed by the Department. The Department will remove paint, at locations shown on the plans or as agreed, for the Contractor's cutting and dismantling purposes. Utilize Department cleaned locations for dismantling when provided or provide own means of dismantling at other locations.

Painted steel to be retained by the Department will be shown on the plans. For painted steel that contains hazardous materials, dispose of the painted steel at a steel recycling or smelting facility unless otherwise shown on the plans. Maintain and make available to the Engineer invoices and other records obtained from the facility showing the received weight of the steel and the facility name. Dispose of steel that does not contain hazardous material coatings in accordance with federal, state and local regulations.

**10.2. Asbestos Requirements.** The plans will indicate locations or elements where asbestos containing materials (ACM) are known to be present. Where ACM is known to exist or where previously unknown ACM has been found, the Department will arrange for abatement by a separate contractor prior to or during the Contract. Notify the Engineer of proposed dates of demolition or removal of structural elements with ACM at least 60 days before beginning work to allow the Department sufficient time for abatement.

The Department of State Health Services (DSHS), Asbestos Programs Branch, is responsible for administering the requirements of the National Emissions Standards for Hazardous Air Pollutants, 40 CFR Part 61, Subpart M and the Texas Asbestos Health Protection Rules (TAHPR). Based on EPA guidance and regulatory background information, bridges are considered to be a regulated "facility" under NESHAP. Therefore, federal standards for demolition and renovation apply.

The Department is required to notify the DSHS at least 10 working days (by postmarked date) before initiating demolition or renovation of each structure or load bearing member shown on the plans. If the actual demolition or renovation date is changed or delayed, notify the Engineer in writing of the revised dates in sufficient time to allow for the Department's notification to DSHS to be postmarked at least 10 days in advance of the actual work.

Failure to provide the above information may require the temporary suspension of work under Article 8.4., "Temporary Suspension of Work or Working Day Charges," due to reasons under the control of the Contractor. The Department retains the right to determine the actual advance notice needed for the change in date to address post office business days and staff availability.

**10.3. Lead Abatement.** Provide traffic control as shown on the plans, and coordinate and cooperate with the third party and the Department for managing or removing hazardous materials. Work for the traffic control shown on the plans and coordination work will not be paid for directly but will be subsidiary to pertinent Items.

---

## Special Provision to Item 7

### Legal Relations and Responsibilities

---

Item 7, "Legal Relations and Responsibilities" of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 7.3., "Laws To Be Observed", Article 7.5., "Patented Devices", Article 7.12., "Responsibility For Hazardous Materials", and Article 7.15., "Responsibility For Damage Claims",** "State" is voided and replaced by "Central Texas Regional Mobility Authority and TxDOT".

**Article 7.3., "Laws To Be Observed,"** is supplemented by the following:

By entering into Contract, the Contractor agrees to provide or make available to the Department records, including electronic records related to the Contract for a period of 3 years after the final payment. No person or entity other than TxDOT may claim third -party beneficiary status under this Contract or any of its provisions, nor may any non-party sue for personal injuries or property damage under this Contract.

**Article 7.15., "Responsibility For Damage Claims,"** the last paragraph is deleted and not replaced.

# Special Provision to Item 7

## Legal Relations and Responsibilities



Item 7, "Legal Relations and Responsibilities," of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Section 7.7.2., "Texas Pollutant Discharge Elimination System (TPDES) Permits and Storm Water Pollution Prevention Plans (SWP3)," is voided and replaced by the following:**

**7.2. Texas Pollution Discharge Elimination System (TPDES) Permits and Storm Water Pollution Prevention Plans (SWP3).**

**7.2.1. Projects with less than one acre of soil disturbance including required associated project specific locations (PSL's) per TPDES GP TXR 150000.**

No posting or filing will be required for soil disturbances within the right of way. Adhere to the requirements of the SWP3.

**7.2.2. Projects with one acre but less than five acres of soil disturbance including required associated PSL's per TPDES GP TXR 150000.**

The Department will be considered a primary operator for Operational Control Over Plans and Specifications as defined in TPDES GP TXR 150000 for construction activity in the right of way. The Department will post a small site notice along with other requirements as defined in TPDES GP TXR 150000 as the entity of having operational control over plans and specifications for work shown on the plans in the right of way.

The Contractor will be considered a Primary Operator for Day-to-Day Operational Control as defined in TPDES GP TXR 150000 for construction activity in the right of way. In addition to the Department's actions, the Contractor will post a small site notice along with other requirements as defined in TPDES GP TXR 150000 as the entity of having day-to-day operational control of the work shown on the plans in the right of way. This is in addition to the Contractor being responsible for TPDES GP TXR 150000 requirements for on- right of way and off- right of way PSL's. Adhere to all requirements of the SWP3 as shown on the plans. The Contractor will be responsible for Implement the SWP3 for the project site in accordance with the plans and specifications, TPDES General Permit TXR150000, and as directed.

**7.2.3. Projects with 5 acres or more of soil disturbance including required associated PSL's per TPDES GP TXR 150000.**

The Department will be considered a primary operator for Operational Control Over Plans and Specifications as defined in TPDES GP TXR 150000 for construction activities in the right of way. The Department will post a large site notice, file a notice of intent (NOI), notice of change (NOC), if applicable, and a notice of termination (NOT) along with other requirements per TPDES GP TXR 150000 as the entity having operational control over plans and specifications for work shown on the plans in the right of way.

The Contractor will be considered a primary operator for Day-to-Day Operational Control as defined in TPDES GP TXR 150000 for construction activities in the right of way. In addition to the Department's actions, the Contractor shall file a NOI, NOC, if applicable, and NOT and post a large site notice along with other requirements as the entity of having day-to-day operational control of the work shown on the plans in the right of way. This is in addition to the Contractor

being responsible for TPDES GP TXR 150000 requirements for on- right of way and off- right of way PSL's. Adhere to all requirements of the SWP3 as shown on the plans.

# Special Provision to Item 007

## Legal Relations and Responsibilities



Item 7, "Legal Relations and Responsibilities," of the Standard Specifications is amended with respect to the clauses cited below.

**Section 2.6., "Barricades, Signs, and Traffic Handling,"** the first paragraph is voided and replaced by the following:

- 2.6. **Barricades, Signs, and Traffic Handling.** Comply with the requirements of Item 502 "Barricades, Signs, and Traffic Handling," and as directed. Provide traffic control devices that conform to the details shown on the plans, the TMUTCD, and the Department's Compliant Work Zone Traffic Control Device List maintained by the Traffic Safety Division. When authorized or directed, provide additional signs or traffic control devices not required by the plans.

**Section 2.6.1., "Contractor Responsible Person and Alternative,"** is voided and replaced by the following:

- 2.6.1. **Contractor Responsible Person and Alternative.** Designate in writing, a Contractor's Responsible Person (CRP) and an alternate to be the representative of the Contractor who is responsible for taking or directing corrective measures regarding the traffic control. The CRP or alternate must be accessible by phone 24 hr. per day and able to respond when notified. The CRP and alternate must comply with the requirements of Section 2.6.5., "Training."

**Section 2.6.2., "Flaggers,"** the first paragraph is voided and replaced by the following:

- 2.6.2. **Flaggers.** Designate in writing, a flagger instructor who will serve as a flagging supervisor and is responsible for training and assuring that all flaggers are qualified to perform flagging duties. Certify to the Engineer that all flaggers will be trained and make available upon request a list of flaggers trained to perform flagging duties.

**Section 2.6.5., "Training,"** is voided and replaced by the following:

- 2.6.5. **Training.** Train workers involved with the traffic control using Department-approved training as shown on the "Traffic Control Training" Material Producer List.

Coordinate enrollment, pay associated fees, and successfully complete Department-approved training or Contractor-developed training. Training is valid for the period prescribed by the provider. Except for law enforcement personnel training, refresher training is required every 4 yr. from the date of completion unless otherwise specified by the course provider. The Engineer may require training at a frequency instead of the period prescribed based on the Department's needs. Training and associated fees will not be measured or paid for directly but are considered subsidiary to pertinent Items.

Certify to the Engineer that workers involved in traffic control and other work zone personnel have been trained and make available upon request a copy of the certification of completion to the Engineer. Ensure the following is included in the certification of completion:

- name of provider and course title,
- name of participant,
- date of completion, and
- date of expiration.

Where Contractor-developed training or a Department-approved training course does not produce a certification, maintain a log of attendees. Make the log available upon request. Ensure the log is legible and includes the following:

- printed name and signature of participant,
- name and title of trainer, and
- date of training.

2.6.5.1. **Contractor-developed Training.** Develop and deliver Contractor-developed training meeting the minimum requirements established by the Department. The outline for this training must be submitted to the Engineer for approval at the preconstruction meeting. The CRP or designated alternate may deliver the training instead of the Department-approved training. The work performed and materials furnished to develop and deliver the training will not be measured or paid for directly but will be considered subsidiary to pertinent items.

2.6.5.1.1. **Flagger Training Minimum Requirements.** A Contractor's certified flagging instructor is permitted to train other flaggers.

2.6.5.1.2. **Optional Contractor-developed Training for Other Work Zone Personnel.** For other work zone personnel, the Contractor may provide training meeting the curriculum shown below instead of Department-approved training.

Minimum curriculum for Contractor-provided training is as follows:

Contractor-developed training must provide information on the use of personnel protection equipment, occupational hazards and health risks, and other pertinent topics related to traffic management. The type and amount of training will depend on the job duties and responsibilities. Develop training applicable to the work being performed. Develop training to include the following topics.

- The Life You Save May Be Your Own (or other similar company safety motto).
- Purpose of the training.
  - It's the Law.
  - To make work zones safer for workers and motorists.
  - To understand what is needed for traffic control.
  - To save lives including your own.
- Personal and Co-Worker Safety.
  - **High Visibility Safety Apparel.** Discuss compliant requirements; inspect regularly for fading and reduced reflective properties; if night operations are required, discuss the additional and appropriate required apparel in addition to special night work risks; if moving operations are underway, discuss appropriate safety measures specific to the situation and traffic control plan.
  - **Blind Areas.** A blind area is the area around a vehicle or piece of construction equipment not visible to the operators, either by line of sight or indirectly by mirrors. Discuss the "Circle of Safety" around equipment and vehicles; use of spotters; maintain eye contact with equipment operators; and use of hand signals.
  - **Runovers and Backovers.** Remain alert at all times; keep a safe distance from traffic; avoid turning your back to traffic and if you must then use a spotter; and stay behind protective barriers, whenever possible. Note: It is not safe to sit on or lean against a concrete barrier, these barriers can deflect four plus feet when struck by a vehicle.
  - Look out for each other, warn co-workers.
  - Be courteous to motorists.
  - Do not run across active roadways.
  - Workers must obey traffic laws and drive courteously while operating vehicles in the work zones.
  - Workers must be made aware of company distracted driving policies.
- **Night Time Operations.** Focus should be placed on projects with a nighttime element.



- **Traffic Control Training.** Basics of Traffic Control.
  - Identify work zone traffic control supervisor and other appropriate persons to report issues to when they arise.
  - Emphasize that work zone traffic control devices must be in clean and in undamaged condition. If devices have been hit but not damaged, put back in their correct place and report to traffic control supervisor. If devices have been damaged, replace with new one and report to traffic control supervisor. If devices are dirty, faded or have missing or damaged reflective tape clean or replace and report to traffic control supervisor. Show examples of non-acceptable device conditions. Discuss various types of traffic control devices to be used and where spacing requirements can be found.
  - **Channelizing Devices and Barricades with Slanted Stripes.** Stripes are to slant in the direction you want traffic to stay or move to; demonstrate this with a device.
  - **Traffic Queuing.** Workers must be made aware of traffic queuing and the dangers created by it. Workers must be instructed to immediately notify the traffic control supervisor and other supervisory personnel if traffic is queuing beyond advance warning sign and devices or construction limits.
  - **Signs.** Signs must be straight and not leaning. Report problems to the traffic control supervisor or other as designated for immediate repair. Covered signs must be fully covered. If covers are damaged or out of place, report to traffic control supervisor or other as designated.

---

## Special Provision to Item 8

### Prosecution and Progress

---

Item 8, "Prosecution and Progress," of the Standard Specifications, is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 8.5., "Project Schedules"** is supplemented by the following

The progress schedule required for this project is the critical path method schedule (CPM schedule) as described herein. The Contractor shall prepare and submit for review and acceptance a cost loaded schedule of proposed working progress for the entire contract duration. The Engineer will provide a template with milestones from other contracts and non-construction activities for the Contractor to use in the development of their schedule. The Engineer shall also provide a Work Breakdown Structure (WBS) as well as the required report layouts for the Contractor to use to develop the progress schedule for this Contract.

Immediately after receipt of notice of award, the Division Engineer and the Contractor will establish a mutually agreeable date on which the preconstruction meeting will be held. The Contractor's project superintendent and other individuals representing the Contractor who are knowledgeable of the Contractor's proposed progress schedule or who will be in charge of major items of the work shall attend the preconstruction conference.

After work on the project has begun, construction conferences will be held periodically. The construction conferences are to be scheduled at times that are mutually agreeable to both the project superintendent and the Resident Engineer. It shall be the superintendent's responsibility to attend the conferences.

**Section 8.5.2 "Progress Schedule"** is supplemented by the following:

The Contractor shall provide a schedule that shows the various activities of Work in sufficient detail to demonstrate a reasonable and workable plan to complete the Project by the Original Contract Completion Date and any interdependent milestones identified by the Engineer or required by Contract. Show the order and interdependence of activities and the sequence for accomplishing the Work. Describe all activities in sufficient detail so that the Engineer can readily identify the Work and measure the progress of each activity.

**Section 8.5.3 "Schedule Format"** is supplemented by the following:

The Contractor shall use a compatible version of Oracle Primavera P6 or comparable scheduling software to generate the CPM schedule. It is the Contractor's responsibility to verify with the Engineer the software and version being used for this project and shall maintain the required version for the entire contract duration. The use of Microsoft Project and Primavera Project Planner (P3) and other scheduling software is prohibited.

The progress schedule shall contain the following Administrative Identifier Information:

- (1) Project Name
- (2) Contract Number
- (3) Date of Contract
- (4) Construction Completion Date
- (5) Contractor's Name
- (6) Contractor's Contact Information

The CPM schedule must reflect the scope of work and include the following:

- (1) Clear identification of tasks to be completed based on Section or Special Provisions included in the Project Manual and as listed in Pay Items, including subcontractor work activities.
- (2) Include calculations of resources required (Cost, Labor, Equipment) for constructing all facilities within the Contract duration. Specific calculations shall be provided to show quantities, manpower / crews, and equipment to support the critical path. The Contractor shall be capable of calculating the maximum crew size anticipated if any activities become critical, so the Contractor is prepared when a critical path changes or a new path occurs.
- (3) Float for each Activity.
- (4) Activities for submittals (shop drawings).
- (5) Punchlist activities with sufficient duration for the Engineer's inspection and acceptance before the final completion date
- (6) Activities for submittal review time by the Engineer, including time range showing start and end dates.
- (7) Working and shop drawing preparation, submittal, and review for acceptance.
- (8) Material and equipment procurement, fabrication and delivery; identify any long lead items as separate activities.
- (9) Owner furnished and/or installed materials and equipment shall be identified as separate activities.
- (10) NTP / Start of construction
- (11) Required phasing
- (12) Maintenance of traffic requirements as required by the contract (if any)
- (13) Intermediate completion dates (if any)
- (14) Identified interdependent milestones (if any)
- (15) Seasonal limitation/observation periods/moratoriums
- (16) Beginning and end of each traffic control work area and road openings
- (17) Other similar activities and project milestones established in the Contract Documents.
- (18) Substantial Completion Date
- (19) Final Acceptance Date
- (20) All required Reports layouts as requested by the Engineer

**Section 8.5.4 "Activity Format"** is supplemented by the following:

Activity requirements are discussed in further detail as follows:

- (1) Activity Identification (ID) - Assign each activity a unique identification number. The format for the identification number will be provided by the Engineer. All activities must begin with the same activity ID prefix as provided by the Engineer.
- (2) Activity Description - Assign each activity an unambiguous descriptive word or phrase. For example, use "Excavate Area A," not "Start Excavation."
- (3) Activity Codes – The Engineer will provide the activity code dictionary in the template. The Contractor will assign the appropriate codes to each activity.
- (4) Activity Original Duration - Assign a planned duration in working days for each activity. Do not exceed a duration of 10 working days for any activity unless accepted by the Engineer. Each activity shall have a minimum duration of 1 working day. Do not represent the maintenance of traffic, erosion control, and other similar items as single activities extending to the Completion Date. Break these Contract Items into component activities in order to meet the duration requirements of this paragraph.
- (5) Finish-to-Start Relationships - Unless allowed in writing by the Engineer, use only finish-to-start relationships with no leads or lags to link activities. All activities, except the first activity, shall have a predecessor(s). All activities, except the final activity, shall have a successor(s).
- (6) Calendars – The Engineer will provide pre-defined calendars as part of the template. The Contractor shall assign these pre-defined calendars to the appropriate activities. The Contractor may create new projectspecific

- calendars to represent their standard work schedule using the pre-defined calendars as a basis. The Contractor may not edit pre-defined calendars.
- (7) Constraints – Unless allowed in writing by the Engineer, do not use constraints in the schedule.
  - (8) Resources – Manpower and equipment shall be reflected for all activities. Incidental costs to construction shall be equally spread out across all activities. Front loaded schedules are not allowed.
  - (9) The schedule shall show the total cost of performing each activity and shall include the total labor, material, equipment and general conditions.
  - (10) The sum of cost for all activities shall equal the total Contract.
  - (11) The summed value of that portion of the activities allocated to each Contract bid item shall equal the total value of the corresponding Contract bid item.
  - (12) The Contractor shall allocate a value for unit price or lump sum contract bid items to each activity in the schedule. No Lump sum amounts should exceed \$100,000.

**Section 8.5.5.2 “Critical Path Method”** The first paragraph is voided and replaced by the following:

The Contractor shall submit the baseline CPM schedule in a bar chart format showing the critical path in red, using both hard copy and in electronic formats. Electronic formats shall be compatible with the Engineer’s computer systems. Also, submit the following information:

- (1) Written narrative – Explains the sequence of work, the controlling operations, intermediate completion dates, milestones, project phasing, anticipated work schedule and estimated resources. In addition, explain how permit requirements, submittal tracking and coordination with subcontractors, utility companies, railroads and other third party entities will be performed. The narrative shall itemize and describe the critical path (i.e. access limitations, constraints, shift work), and compare early and late date or Contract Milestone activities, and describe any critical resources.
- (2) CPM Schedule in a Bar Chart Format – Include the Administrative Identifier Information discussed above on the first page of the schedule. For each activity on the chart, indicate the Activity ID, Activity Description, Original Duration, Remaining Duration, Changes to Duration, Total Float, Early Start Date, Early Finish Date, and Calendar Name. Use arrows to show the relationships among activities.
- (3) Identify the critical path of the project on the bar chart. The critical path is defined as; 1) the sequence of activities that must be completed “on time” to ensure that the project finished on time. 2) the longest path of activities in the project that determines the project finish date.
- (4) No more than 10% of activities may be critical or near critical. Critical Activities will have a total float equal to zero. “Near critical” is defined as float in the range of 1 to 10 working days.
- (5) Six Week Look Ahead CPM Schedule in a Bar Chart Format – This schedule will have all the same requirements of the CPM schedule in bar chart format except that it shall be limited to those activities that have an early start or early finish within a six-week period of the data date.
- (6) Logic Diagram – Submit a diagram in PERT chart format showing the logic of the CPM schedule.
- (7) Activity ID Sort – Submit a listing of all activities included in the CPM schedule sorted by ascending Activity Identification Number.
- (8) Total Float Sort – Submit a listing of all activities included in the CPM schedule sorted by increasing total float and by early start date.
- (9) All float belongs to the Project and is a shared commodity between the Contractor and the Mobility Authority and is not for the exclusive use or benefit of either party. The Contractor shall notify the Engineer in writing for acceptance before using any float.
- (10) Detailed Predecessor/Successor Sort – Submit a listing of all activities included in the CPM schedule indicating the activities that immediately precede and immediately succeed that activity in the schedule logic.
- (11) Scheduling Statistics Report – Submit a report of CPM schedule statistics, including number of activities, number of activities on the longest path, number of started activities, number of completed activities, number of relationships, percent complete, and number and type of constraints.

- (12) A resource curves / Metric tracking reports (EVM) corresponding to the milestones and work activities established above.

**Section 8.5.5.2.2 “Baseline Schedule”** The second paragraph is voided and replaced by the following:

The Contractor shall submit a progress schedule for the entire duration of the Contract to the Engineer 30 calendar days following the contract award date. After review of the schedule the Engineer shall schedule a Baseline CPM Schedule meeting with the Contractor to review the schedule and identify any changes or corrections. Within 7 calendar days of the CPM Schedule meeting, the Contractor shall make any necessary adjustments to address all review comments and resubmit network diagrams and reports for the Engineer’s review. The complete baseline schedule shall be submitted and accepted no later than (45) forty-five days after contract award date. The complete progress schedule shall be accepted by the Engineer before any payments will be processed for the project.

**Section 8.5.5.2.3 “Progress Schedule”** is supplemented by the following

The Engineer may withhold pay estimates if the updated CPM schedule is not submitted as required by this section. For each updated CPM schedule, identify the actual start and finish dates for all completed activities, the actual start date and remaining duration for all activities in progress, the difference in duration of all activities since the last update and any exceptional reports associated with the update. Only accepted changes will be incorporated into the monthly progress schedule update. The schedule should represent the actual work performed and should be progressed with actuals for all the schedule activities. The final schedule will be utilized as the project actual “As Built” schedule.

Provide a written narrative that identifies any changes or shifts in the critical path and submit reasons for the changes or shifts in the critical path. Identify any changes in logic for the updated CPM schedule and submit reasons for changes to the schedule logic. In addition to the written narrative, submit the following with each updated CPM schedule:

- (1) CPM Schedule in Bar Chart Format
- (2) Four Week Look Ahead CPM Schedule in Bar Chart Format
- (3) Logic Diagram
- (4) Activity ID Sort
- (5) Total Float Sort
- (6) Detailed Predecessor/Successor Sort
- (7) Schedule Metrics and Earned Value (Schedule, Cost, Labor) Reports

The Contractor must submit a statement that there were no changes in the schedule logic, activity durations, or calendars since the previous update in lieu of submission of items (3), (5), and (6). Acceptance of schedule updates by the Engineer does not revise the Contract Documents.

A monthly schedule update meeting shall be held each month following Notice to Proceed to review monthly schedule update submittals, critical path items and recovery schedules. The Contractor shall be represented in the meeting by the Contractor’s scheduler, project manager and general superintendent. As necessary the Contractor may be also asked to attend a coordination meeting to discuss the schedule impacts to other contractors.

If the Project completion date changes or if the project schedule overrun is anticipated to exceed 5%, the Contractor shall submit a revised progress schedule to the Engineer for review and acceptance. If plan revisions are anticipated to change the sequence of construction in such a manner as will affect the progress, but not the completion date, then the Contractor may submit a revised progress schedule for review and acceptance. The Project completion date shall remain unchanged.

**Section 8.5.5.3 “Notice of Potential Time Impact”** is supplemented by the following

“Contractor shall not be eligible for Change Order(s) for additional compensation for additional costs, including costs for developing and executing a Recovery Schedule(s), and delay and disruption damages, or additional Days incurred directly or indirectly from the virus known as severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and the disease known as COVID-19, including any disruptions to, and delays or interruptions in, construction of the Project in accordance with the Contract and any approved Baseline Schedule.”

Section 8.5.5 "Schedule Types" is supplemented by the following:

#### Section 8.5.5.5 Recovery Schedule

If the progress schedule projects a finish date for the Project beyond the original Completion Date, the Contractor shall submit a revised schedule showing a plan to finish by the original Completion Date. The Mobility Authority will withhold Pay Estimates until the Engineer accepts the revised schedule. No additional compensation for developing and executing a recovery schedule(s) shall be reimbursed to the Contractor. The Engineer will use the schedule to evaluate time extensions and associated costs requested by the Contractor.

- (1) In the event Work or related construction activities shown on the Contractor's Progress Schedule fall behind schedule to the extent that dates established as contractual Completion Dates are in jeopardy, the Contractor shall prepare and submit to the Engineer, at no additional cost or time to the Mobility Authority, a Recovery Schedule showing intent to remedy delays and to regain originally scheduled time of completion of Work within a timely manner. This includes delays due to unforeseen conditions.
- (2) Recovery Schedule shall be submitted in such form and detail appropriate to the delay or delays, explaining and displaying how the Contractor intends to reschedule those activities and reestablish compliance with the accepted baseline Construction Progress Schedule during the immediate subsequent pay period or as permitted by Engineer. This shall include a schedule diagram comparing the original and the revised sequence of activities, identifying all affected activities.
- (3) Upon determining the requirement for a Recovery Schedule:
  - a. Within five (5) calendar days, the Contractor shall present to Engineer a proposed Recovery Schedule. The Recovery Schedule shall represent the Contractor's best judgment as to how to best reorganize the Work and achieve progress to comply with the accepted Construction Progress Schedule.
  - b. Changes to Contractor's means and methods, such as increased labor force, working hours, overtime, additional equipment and other means shall not constitute the basis for changes to the Contract Sum or Contract Time.
  - c. Recovery Schedule shall show remedies to bring Work back on schedule up-to-date within the immediate subsequent pay period.
  - d. The Recovery Schedule shall be prepared to a similar level of detail as the Construction Progress Schedule.
  - e. Five (5) calendar days prior to the expiration of the Recovery Schedule, Contractor shall document to the Engineer that the Work schedule has regained, or is on-track to regain, compliance with the Construction Progress Schedule.
- (4) Failure to submit Recovery Schedule in a timely manner may result in Termination of the Contract for Cause as determined by the Engineer.
- (5) Failure to achieve compliance with the accepted Construction Progress Schedule despite implementing Recovery Schedule may result in Termination of the Contract for Cause as determined by the Engineer.
- (6) Termination of Contract For Cause: In the event Contractor defaults on the terms of the Contract, including failure to maintain the Construction Progress Schedule, Engineer will assess the level of completion of the Work achieved by the Contractor and compare amount of available funds against anticipated costs required for the Mobility Authority to complete the Work, including anticipated Liquidated Damages resulting from delay, if any. Engineer will determine amount of payment due to Contractor for Work completed prior to date of Termination of Contract for Cause, if any. In the event available funds are not sufficient for the Mobility Authority to complete the Work, the Mobility Authority will withhold such funds from the amount due the Contractor.
- (7) If, in the opinion of the Engineer, the Contractor has sufficiently regained compliance with the Construction Progress Schedule, the use of the Construction Progress Schedule will be resumed. Contractor shall update and submit the Construction Progress Schedule clearly identifying Work to date and how the Contractor intends to achieve timely completion for the remainder of the Work in accordance with the Construction Documents.

---

## Special Provision to Item 8 Prosecution and Progress

---



Item 8, "Prosecution and Progress" of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 8.1., "Prosecution of Work."** The first sentence of the first paragraph is voided and replaced by the following:

Begin work 90 calendar days after the authorization date to begin work. Do not begin work before or after this period unless authorized in writing by the Engineer.

---

## Special Provision to Item 8 Prosecution and Progress

---



Item 8, "Prosecution and Progress" of the Standard Specification is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 8.2., "Subcontracting,"** is supplemented by the following paragraph, which is added as paragraph six to this article:

The Contractor certifies by signing the Contract that the Contractor will not enter into any subcontract with a subcontractor that is not registered in the Department of Homeland Security's (DHS) E-Verify system. Require that all subcontractors working on the project register and require that all subcontractors remain active in the DHS E-Verify system until their work is complete on the project.



---

## Special Provision to Item 8 Prosecution and Progress

---



Item 8, "Prosecution and Progress" of the Standard Specifications is amended with respect to the clause cited below. No other clauses or requirements of this Item are waived or changed.

**Article 8.7.2., "Wrongful Default,"** is revised and replaced by the following:

If it is determined after the Contractor is declared in default, that the Contractor was not in default, the rights and obligations of all parties will be the same as if termination had been issued for the convenience of the public as provided in Article 8.8 "Termination of Contract."

---

## Special Provision to Item 9

### Measurement and Payment

Item 9, "Measurement and Payment," of the Standard Specifications, is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 9.5., "Progress Payments,"** Delete this section of the Specifications in its entirety and substitute with the following:

Partial payments will be made once each month covering work performed and materials complete-in-place in accordance with the Contract. The invoice form to be submitted each month will be provided to the Contractor in Microsoft Excel format. The Contractor must be able to use Microsoft Excel to complete the invoice form. Partial payments will be made on the value of work performed based on approximate estimates prepared by the Engineer, provided, however, that no estimate shall be certified or payment made where the net amount receivable by the Contractor is less than Five-hundred Dollars (\$500.00).

The Engineer will review the partial payment estimate with the Contractor's representative prior to each partial payment.

Total Contract value shall be considered to mean the original amount of the Contract, except when the Contract is increased or decreased by a supplemental agreement in which case the adjusted total shall be used.

The Mobility Authority reserves the right to withhold the payment of any partial or final estimate voucher or any sum or sums thereof from such vouchers in the event of the failure of the Contractor to promptly make payment to all persons supplying equipment, tools or materials, or for any labor used by the Contractor in the prosecution of the work provided for in the Contract, and for any other cause as determined by the Mobility Authority in its sole discretion, including overpayment on previous partial payments.

**Article 9.8., "Retainage,"** is supplemented with the following:

The Mobility Authority shall not withhold funds from payments to be made to Contractor for the Work until such time as 95% of the Adjusted Contract Price has been paid to the Contractor. Following completion of and payment for 95% of the Adjusted Contract Price, the Mobility Authority shall withhold, the remaining 5% of the Adjusted Contract Price pursuant to the terms described below.

The remaining 5% for the Work, subject to reduction as specified below, shall be held by the Mobility Authority until Final Acceptance. At such time, and provided the Contractor is not in breach or default hereunder, the Mobility Authority shall release to Contractor all withheld in connection with the Work other than amounts applied to the payment of Losses or which the Mobility Authority deems advisable, in its sole discretion, to retain to cover any existing or threatened claims. The Contractor must further warrant, to the satisfaction of the Mobility Authority, that there are no outstanding claims or liens by any subcontractors or other parties with respect to the Work.

The prime contractor shall make full payment of amounts due to subcontractors within 10 calendar days following the satisfactory completion of the subcontractor's work. Satisfactory completion of the subcontractor's work shall be defined as approval, acceptance, and payment for the subcontractor's work by the Mobility Authority including the submittal and acceptance of all information, deliverables or other documents required by the contract.

Prior to the release of the remaining 5% by the Mobility Authority pursuant to the terms hereof, such amounts shall be held by the Mobility Authority. Upon the release of the remaining 5%, the Contractor shall not be entitled to any interest income that has accrued upon the amounts of the remaining 5% released to Contractor.

**Article 9.9., "Payment Provisions for Subcontractors,"** is supplemented with the following:

The Mobility Authority may pursue actions against the Contractor, including withholding of estimates and suspending the work, for noncompliance with the subcontract requirements of this Section upon receipt of written notice with sufficient details showing the subcontractor has complied with contractual obligations as described in this Article.

These requirements apply to all tiers of subcontractors. Incorporate the provisions of this Article into all subcontract or material purchase agreements.

---

## Special Provision to Item 9 Measurement and Payment

---



Item 9, "Measurement and Payment" of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Section 9.7.1.4.3., "Standby Equipment Costs,"** is voided and replaced by the following:

7.1.4.3.           **Standby Equipment Costs.** Payment for standby equipment will be made in accordance with Section 9.7.1.4., "Equipment," except that the 15% markup will not be allowed and that:

**Section 7.1.4.3.1., "Contractor-Owned Equipment,"** is voided and replaced by the following:

7.1.4.3.1.       **Contractor-Owned Equipment.** For Contractor-owned equipment:

- Standby will be paid at 50% of the monthly Equipment Watch rate after the regional and age adjustment factors have been applied. Operating costs will not be allowed. Calculate the standby rate as follows.

$$\text{Standby rate} = (\text{FHWA hourly rate} - \text{operating costs}) \times 50\%$$

- If an hourly rate is needed, divide the monthly *Equipment Watch* rate by 176.
- No more than 8 hr. of standby will be paid during a 24-hr. day period, nor more than 40 hr. per week.
- Standby costs will not be allowed during periods when the equipment would have otherwise been idle.

---

## Special Provision to Item 502

### Barricades, Signs and Traffic Handling

---



Item 502, "Barricades, Signs and Traffic Handling" of the Standard Specifications, is hereby amended with respect to the clauses cited below, and no other clauses or requirements of this Item are waived or changed hereby.

**Article 502.1., "Description,"** is supplemented by the following:

Temporary work-zone (TWZ) traffic control devices manufactured after December 31, 2019, must have been successfully tested to the crashworthiness requirements of the 2016 edition of the Manual for Assessing Safety Hardware (MASH). Such devices manufactured on or before this date and successfully tested to NCHRP Report 350 or the 2009 edition of MASH may continue to be used throughout their normal service lives. An exception to the manufacture date applies when, based on the project's date of letting, a category of MASH-2016 compliant TWZ traffic control devices are not approved, or are not self-certified after the December 31, 2019, date. In such case, devices that meet NCHRP-350 or MASH-2009 may be used regardless of the manufacture date.

Such TWZ traffic control devices include: portable sign supports, barricades, portable traffic barriers designated exclusively for use in temporary work zones, crash cushions designated exclusively for use in temporary work zones, longitudinal channelizers, truck and trailer mounted attenuators. Category I Devices (i.e., lightweight devices) such as cones, tubular markers and drums without lights or signs attached however, may be self-certified by the vendor or provider, with documentation provided to Department or as are shown on Department's Compliant Work Zone Traffic Control Device List.

**Article 502.4., "Payment,"** is supplemented by the following:

Truck mounted attenuators and trailer attenuators will be paid for under Special Specification, "Truck Mounted Attenuator (TMA) and Trailer Attenuator (TA)." Portable Changeable Message Signs will be paid for under Special Specification, "Portable Changeable Message Sign." Portable Traffic Signals will be paid for under Special Specification, "Portable Traffic Signals."

---

# Special Provision to Item 636

## Signs

---



Item 636, "Signs" of the Standard Specifications, is hereby amended with respect to the clauses cited below, and no other clauses or requirements of this Item are waived or changed hereby.

**Section 636.3.1, "Fabrication."** is deleted.

**Section 636.3.1.2, "Sheeting Application."** The last sentence of the fourth paragraph is voided and replaced by the following.

Do not splice sheeting or overlay films for signs fabricated with ink or with colored transparent films.

# Special Provision to Item 643

## Sign Identification Decals



Item 643, "Sign Identification Decals," of the Standard Specifications is amended with respect to the clauses cited below. No other clauses or requirements of this Item are waived or changed.

**Article 2. "Materials."** The sign identification decal design shown in Figure 1 and the description for each row in Table 1 are supplemented by the following.

<b>Texas Department of Transportation</b>													
<b>C</b>	<b>Fabrication Date</b>											<b>T</b>	<b>1</b>
J	F	M	A	M	J	J	A	S	O	N	D	<b>2</b>	
	201		202		203		204		205			<b>3</b>	
	0	1	2	3	4	5	6	7	8	9		<b>4</b>	
<b>Sheeting MFR - Substrate</b>													
A	B	C	D	E	F	G	H	J	K	L	M	<b>5</b>	
<b>Film MFR</b>													
A	B	C	D	E	F	G	H	J	K	L	M	<b>6</b>	
<b>Sheeting MFR - Legend</b>													
A	B	C	D	E	F	G	H	J	K	L	M	<b>7</b>	
<b>Installation Date</b>													
				0	1	2	3					<b>8</b>	
	0	1	2	3	4	5	6	7	8	9		<b>9</b>	
J	F	M	A	M	J	J	A	S	O	N	D	<b>10</b>	
	201		202		203		204		205			<b>11</b>	
	0	1	2	3	4	5	6	7	8	9		<b>12</b>	
<b>Name of Sign Fabricator</b> <b>Physical Address</b> <b>City, State, Zip Code</b>												<b>13</b>	

**Figure 1**  
**Decal Design (Row numbers explained in Table 1)**

**Table 1**  
**Decal Description**  
**Row Explanation**

<b>1</b>	Sign fabricator
<b>2</b>	Month fabricated
<b>3</b>	First 3 digits of year fabricated
<b>4</b>	Last digit of year fabricated
<b>5</b>	Manufacturer of the sheeting applied to the substrate
<b>6</b>	Film (colored transparent or non-reflective black) manufacturer
<b>7</b>	Manufacturer of the sheeting for the legend
<b>8</b>	Tens digit of date installed
<b>9</b>	Ones digit of date installed
<b>10</b>	Month installed
<b>11</b>	First 3 digits of year installed
<b>12</b>	Last digit of year installed
<b>13</b>	Name of sign fabricator and physical location of sign shop



---

# Special Provision to Special Specification 6185

## Truck Mounted Attenuator (TMA) and Trailer Attenuator (TA)

---



Item 6185, "Truck Mounted Attenuator (TMA) and Trailer Attenuator (TA)" of the Standard Specifications, is hereby amended with respect to the clauses cited below, and no other clauses or requirements of this Item are waived or changed hereby.

**Article 4. "Measurement"**, is voided and replaced by the following:

- 4.1. **Truck Mounted Attenuator/Trailer Attenuator (Stationary).** This Item will be measured by the day. TMA/TAs must be set up in a work area and operational before a calendar day can be considered measureable. A day will be measured for each TMA/TA set up and operational on the worksite.
- 4.2. **Truck Mounted Attenuator/Trailer Attenuator (Mobile Operation).** This Item will be measured by the hour or by the day. The time begins once the TMA/TA is ready for operation at the predetermined site and stops when notified by the Engineer. When measurement by the hour is specified, a minimum of 4 hr. will be paid each day for each operating TMA/TA used in a mobile operation. When measurement by the day is specified, a day will be measured for each TMA/TA set up and operational on the worksite.

# Special Specification 6001

## Portable Changeable Message Sign



### 1. DESCRIPTION

Furnish, operate, and maintain portable trailer mounted changeable message sign (PCMS) units.

### 2. MATERIALS

Furnish new or used material in accordance with the requirements of this Item and the details shown on the plans. Provide a self-contained PCMS unit with the following:

- Sign controller
- Changeable Message Sign
- Trailer
- Power source

Paint the exterior surfaces of the power supply housing, supports, trailer, and sign with Federal Orange No. 22246 or Federal Yellow No. 13538 of Federal Standard 595C, except paint the sign face assembly flat black.

2.1. **Sign Controller.** Provide a controller with permanent storage of a minimum of 75 pre-programmed messages. Provide an external input device for random programming and storage of a minimum of 75 additional messages. Provide a controller capable of displaying up to 3 messages sequentially. Provide a controller with adjustable display rates. Enclose sign controller equipment in a lockable enclosure.

2.2. **Changeable Message Sign.** Provide a sign capable of being elevated to at least 7 ft. above the roadway surface from the bottom of the sign. Provide a sign capable of being rotated 360° and secured against movement in any position.

Provide a sign with 3 separate lines of text and 8 characters per line minimum. Provide a minimum 18 in. character height. Provide a 5 × 7 character pixel matrix. Provide a message legibility distance of 600 ft. for nighttime conditions and 800 ft. for normal daylight conditions. Provide for manual and automatic dimming light sources.

The following are descriptions for 3 screen types of PCMS:

- **Character Modular Matrix.** This screen type comprises of character blocks.
- **Continuous Line Matrix.** This screen type uses proportionally spaced fonts for each line of text.
- **Full Matrix.** This screen type uses proportionally spaced fonts, varies the height of characters, and displays simple graphics on the entire sign.

2.3. **Trailer.** Provide a 2 wheel trailer with square top fenders, 4 leveling jacks, and trailer lights. Do not exceed an overall trailer width of 96 in. Shock mount the electronics and sign assembly.

2.4. **Power Source.** Provide a diesel generator, solar powered power source, or both. Provide a backup power source as necessary.

2.5. **Cellular Telephone.** When shown on the plans, provide a cellular telephone connection to communicate with the PCMS unit remotely.

---

**3. CONSTRUCTION**

Place or relocate PCMS units as shown on the plans or as directed. The plans will show the number of PCMS units needed, for how many days, and for which construction phases.

Maintain the PCMS units in good working condition. Repair damaged or malfunctioning PCMS units as soon as possible. PCMS units will remain the property of the Contractor.

---

**4. MEASUREMENT**

This Item will be measured by each PCMS or by the day used. All PCMS units must be set up on a work area and operational before a calendar day can be considered measurable. When measurement by the day is specified, a day will be measured for each PCMS set up and operational on the worksite.

---

**5. PAYMENT**

The work performed and materials furnished in accordance with this Item and measured as provided under "Measurement" will be paid for at the unit price bid for "Portable Changeable Message Sign." This price is full compensation for PCMS units; set up; relocating; removing; replacement parts; batteries (when required); fuel, oil, and oil filters (when required); cellular telephone charges (when required); software; and equipment, materials, tools, labor, and incidentals.

# Special Specification 6185

## Truck Mounted Attenuator (TMA) and Trailer Attenuator (TA)




---

### 1. DESCRIPTION

Furnish, operate, maintain and remove upon completion of work, Truck Mounted Attenuator (TMA) or Trailer Attenuator (TA).

---

### 2. MATERIALS

Furnish, operate and maintain new or used TMAs or TAs. Assure used attenuators are in good working condition and are approved for use. A list of approved TMA/TA units can be found in the Department's Compliant Work Zone Traffic Control Devices List. The host vehicle for the TMA and TA must weigh a minimum of 19,000 lbs. Host vehicles may be ballasted to achieve the required weight. Any weight added to the host vehicle must be properly attached or contained within it so that it does not present a hazard and that proper energy dissipation occurs if the attenuator is impacted from behind by a large truck. The weight of a TA will not be considered in the weight of the host vehicle but the weight of a TMA may be included in the weight of the host vehicle. Upon request, provide either a manufacturer's curb weight or a certified scales weight ticket to the Engineer.

---

### 3. CONSTRUCTION

Place or relocate TMA/TAs as shown on the plans or as directed. The plans will show the number of TMA/TAs needed, for how many days or hours, and for which construction phases.

Maintain the TMA/TAs in good working condition. Replace damaged TMA/TAs as soon as possible.

---

### 4. MEASUREMENT

4.1. **Truck Mounted Attenuator/Trailer Attenuator (Stationary).** This Item will be measured by the each or by the day. TMA/TAs must be set up in a work area and operational before a calendar day can be considered measurable. When measurement by the day is specified, a day will be measured for each TMA/TA set up and operational on the worksite.

4.2. **Truck Mounted Attenuator/Trailer Attenuator (Mobile Operation).** This Item will be measured by the hour. The time begins once the TMA/TA is ready for operation at the predetermined site and stops when notified by the Engineer. A minimum of 4 hr. will be paid each day for each operating TMA/TA used in a mobile operation.

---

### 5. PAYMENT

The work performed and materials furnished in accordance with this Item and measured as provided under "Measurement" will be paid for at the unit price bid for "Truck Mounted Attenuators/Trailer Attenuators (Stationary)," or "Truck Mounted Attenuators/Trailer Attenuators (Mobile Operation)." This price is full compensation for furnishing TMA/TA: set up; relocating; removing; operating; fuel; and equipment, materials, tools, labor, and incidentals.

---

# Special Specification 7001-RMA

## Lane Closures

---

### 1. DESCRIPTION

Install, maintain, and remove lane closures as shown on the plans, or as directed by the Engineer.

### 2. MATERIALS

Furnish material in accordance with the following:

- Section 7.2.6., "Barricades, Signs, and Traffic Handling"
- Section 502.4.2., "Law Enforcement Personnel"
- Special Specification 6185, "Truck Mounted Attenuator (TMA)"

### 3. CONSTRUCTION

Comply with the requirements of Article 7.2., "Safety," Item 502, "Barricades, Signs, and Traffic Handling", and Special Specification 6185, "Truck Mounted Attenuator (TMA)".

Implement lane closures of the types described in the plans necessary to perform the work. Submit a lane closure plan to the Authority for approval prior to implementation.

For the purposes of this Specification, a Lane Closure is defined as a single, continuous traffic control operation to close to traffic a shoulder, single traffic lane, or multiple traffic lanes.

### 4. MEASUREMENT

This Item will be measured by the Day for each working day a Lane Closure is fully operational and protecting active construction events for the work. Lane closure operations limited within one peak or off-peak period, in any consecutive 24-hours are measured as one "Day".

### 5. PAYMENT

The work performed, and materials furnished in accordance with the Item and measured as provided under "Measurement" will be paid for at the unit price bid for "Lane Closure". This price is full compensation for setup and removal of Lane Closures, maintenance of Lane Closures, and furnishing all materials, equipment, labor, tools, supplies, and incidentals.

Law enforcement personnel will be paid in accordance with Item 502.



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

## September 29, 2021 AGENDA ITEM #6

---

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

Strategic Plan Relevance:	Regional Mobility
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.

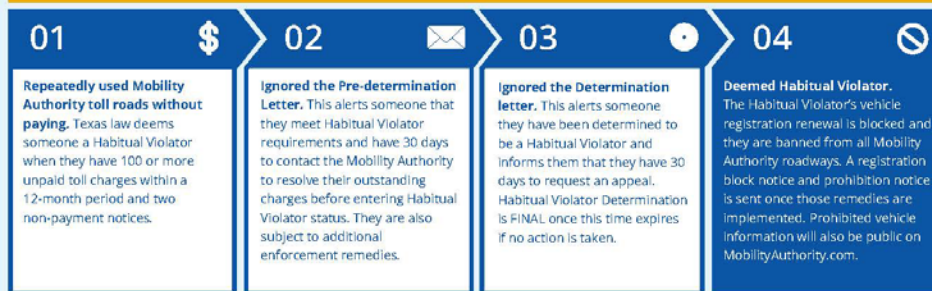
**Action requested/Staff Recommendation:** Staff affirms that all required steps have been followed and proper notice previously provided to customers determined to be habitual violators. To date, these customers have not appealed this determination or resolved their outstanding balances.

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](http://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](http://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. 21-0XX**

**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 Central Texas Regional Mobility Authority (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) 45 SW Toll; and (6) 183S 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 29, 2021; 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 29<sup>th</sup> day of September 2021.

Submitted and reviewed by:

Approved:

---

Geoffrey Petrov, General Counsel

---

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 29, 2021  
AGENDA ITEM #7

---

Accept the financial statements for  
August 2021

Strategic Plan Relevance: Regional Mobility  
Department: Finance  
Contact: Bill Chapman, 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 financial statements for August 2021.

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

**Financing:** N/A

**Action requested/Staff Recommendation:** Accept the financial statements for August 2021.

**Backup provided:** Draft Resolution  
Draft financial statements for August 2021

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

**RESOLUTION NO. 21-0XX**

**ACCEPTING THE FINANCIAL STATEMENTS FOR AUGUST 2021**

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;

WHEREAS, the Executive Director, working with the Chief Financial Officer, has reviewed and authorized the disbursements necessary for the month of August 2021 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 financial statements for August 2021 attached hereto as Exhibit A.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 29<sup>th</sup> day of September 2021.

Submitted and reviewed by:

Approved:

\_\_\_\_\_  
Geoffrey Petrov, General Counsel

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

**Exhibit A**

**Financial Statements for August 2021**

**Central Texas Regional Mobility Authority**  
**Income Statement**  
**For the Period Ending August 31, 2021**

	Budget			
	Amount FY	Actual Year	Percent of	Actual Prior
	2021	to Date	Budget	Year to Date
<b>REVENUE</b>				
<b>Operating Revenue</b>				
Toll Revenue - Tags	105,220,500	19,071,327	18.13%	11,321,157
Video Tolls	31,433,500	7,133,258	22.69%	3,456,280
Fee Revenue	13,921,000	2,382,412	17.11%	1,920,075
<b>Total Operating Revenue</b>	<b>150,575,000</b>	<b>28,586,997</b>	<b>18.99%</b>	<b>16,697,512</b>
<b>Other Revenue</b>				
Interest Income	1,230,764	36,338	2.95%	179,364
Grant Revenue	2,180,000	20,995	0.96%	380,990
Misc Revenue	320,000	38,248	11.95%	-
Gain/Loss on Sale of Asset	-	6,568	-	-
<b>Total Other Revenue</b>	<b>3,730,764</b>	<b>102,149</b>	<b>2.74%</b>	<b>560,354</b>
<b>TOTAL REVENUE</b>	<b>\$154,305,764</b>	<b>\$28,689,146</b>	<b>18.59%</b>	<b>17,257,866</b>
<b>EXPENSES</b>				
<b>Salaries and Benefits</b>				
Salary Expense-Regular	4,940,743	661,747	13.39%	665,078
Salary Reserve	80,000	-	-	-
TCDRS	1,016,106	98,832	9.73%	96,731
FICA	238,665	30,981	12.98%	30,191
FICA MED	74,643	10,169	13.62%	10,170
Health Insurance Expense	584,978	64,078	10.95%	79,504
Life Insurance Expense	6,714	1,193	17.77%	829
Auto Allowance Expense	10,200	1,275	12.50%	1,275
Other Benefits	209,200	18,211	8.71%	23,560
Unemployment Taxes	5,184	166	3.20%	144
<b>Total Salaries and Benefits</b>	<b>7,166,434</b>	<b>886,652</b>	<b>12.37%</b>	<b>907,482</b>



**Central Texas Regional Mobility Authority**  
**Income Statement**  
**For the Period Ending August 31, 2021**

	Budget			
	Amount FY	Actual Year	Percent of	Actual Prior
	2021	to Date	Budget	Year to Date
<b>Administrative</b>				
<b>Administrative and Office Expenses</b>				
Accounting	9,000	1,277	14.19%	1,455
Auditing	144,550	-	-	11,000
Human Resources	30,000	84	0.28%	643
IT Services	285,000	21,482	7.54%	10,634
Internet	450	-	-	-
Software Licenses	514,500	15,638	3.04%	12,318
Cell Phones	24,800	2,935	11.83%	2,251
Local Telephone Service	105,000	14,625	13.93%	14,754
Overnight Delivery Services	200	44	21.91%	-
Local Delivery Services	50	-	-	-
Copy Machine	16,000	1,272	7.95%	2,544
Repair & Maintenance-General	10,000	-	-	175
Meeting Expense	13,250	83	0.63%	434
Toll Tag Expense	3,000	300	10.00%	600
Parking / Local Ride Share	2,750	-	-	-
Mileage Reimbursement	4,800	11	0.23%	35
Insurance Expense	651,000	102,598	15.76%	68,866
Rent Expense	575,000	96,373	16.76%	93,792
Building Parking	11,000	22	0.20%	-
Legal Services	312,500	10,389	3.32%	36,481
<b>Total Administrative and Office Expenses</b>	<b>2,712,850</b>	<b>267,134</b>	<b>9.85%</b>	<b>255,982</b>
<b>Office Supplies</b>				
Books & Publications	4,250	292	6.86%	839
Office Supplies	11,000	475	4.32%	1,789
Misc Office Equipment	4,500	630	13.99%	-
Computer Supplies	186,950	6,030	3.23%	2,971
Copy Supplies	1,500	-	-	-
Other Reports-Printing	5,000	-	-	-
Office Supplies-Printed	5,000	-	-	-
Postage Expense	650	112	17.21%	8
<b>Total Office Supplies</b>	<b>218,850</b>	<b>7,538</b>	<b>3.44%</b>	<b>5,606</b>

**Central Texas Regional Mobility Authority**  
**Income Statement**  
**For the Period Ending August 31, 2021**

	Budget Amount FY 2021	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
<b>Communications and Public Relations</b>				
Graphic Design Services	75,000	-	-	-
Website Maintenance	100,000	5,477	5.48%	3,412
Research Services	275,000	-	-	30,671
Communications and Marketing	500,000	12,827	2.57%	17,556
Advertising Expense	800,000	48,832	6.10%	81,036
Direct Mail	85,000	-	-	-
Video Production	179,000	8,820	4.93%	8,820
Photography	10,000	199	1.99%	-
Radio	75,000	-	-	-
Promotional Items	10,000	-	-	945
Annual Report printing	5,600	780	13.92%	553
Direct Mail Printing	40,000	-	-	-
Other Communication Expenses	15,000	10,760	71.73%	450
<b>Total Communications and Public Relations</b>	<b>2,169,600</b>	<b>87,695</b>	<b>4.04%</b>	<b>143,443</b>
<b>Employee Development</b>				
Subscriptions	50,560	123	0.24%	119
Agency Memberships	57,942	150	0.26%	950
Continuing Education	11,000	-	-	275
Professional Development	14,000	-	-	-
Other Licenses	1,850	375	20.27%	-
Seminars and Conferences	45,500	-	-	399
Travel	89,500	-	-	(154)
<b>Total Employee Development</b>	<b>270,352</b>	<b>648</b>	<b>0.24%</b>	<b>1,589</b>
<b>Financing and Banking Fees</b>				
Trustee Fees	60,000	11,463	19.10%	3,763
Bank Fee Expense	2,000	638	31.89%	19
Continuing Disclosure	4,000	-	-	-
Arbitrage Rebate Calculation	10,000	-	-	-
Rating Agency Expense	50,000	-	-	17,000
<b>Total Financing and Banking Fees</b>	<b>126,000</b>	<b>12,100</b>	<b>9.60%</b>	<b>20,781</b>
<b>Total Administrative</b>	<b>5,497,652</b>	<b>375,115</b>	<b>6.82%</b>	<b>427,401</b>

**Central Texas Regional Mobility Authority**  
**Income Statement**  
**For the Period Ending August 31, 2021**

	Budget Amount FY 2021	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
<b>Operations and Maintenance</b>				
<b>Operations and Maintenance Consulting</b>				
GEC-Trust Indenture Support	521,829	226,485	43.40%	215,201
GEC-Financial Planning Support	243,804	19,713	8.09%	31,828
GEC-Toll Ops Support	1,314,155	144,037	10.96%	59,148
GEC-Roadway Ops Support	1,186,339	61,672	5.20%	128,627
GEC-Technology Support	1,438,856	221,342	15.38%	432,982
GEC-Public Information Support	-	32,253	-	2,215
GEC-General Support	1,473,429	174,490	11.84%	94,568
General System Consultant	1,653,940	152,849	9.24%	39,109
Traffic Modeling	67,000	1,784	2.66%	28,627
Traffic and Revenue Consultant	175,000	-	-	-
<b>Total Operations and Maintenance Consulting</b>	<b>8,074,352</b>	<b>1,034,624</b>	<b>12.81%</b>	<b>1,032,304</b>
<b>Roadway Operations and Maintenance</b>				
Roadway Maintenance	4,487,800	9,056	0.20%	455,934
Landscape Maintenance	2,302,400	199,715	8.67%	-
Signal & Illumination Maint	50,000	-	-	-
Maintenance Supplies-Roadway	350,000	26,100	7.46%	-
Tools & Equipment Expense	25,000	-	-	2,090
Gasoline	30,000	2,423	8.08%	1,774
Repair & Maintenance - Vehicles	10,000	234	2.34%	1,342
Natural Gas	2,500	656	26.24%	528
Electricity - Roadways	250,000	23,345	9.34%	17,001
<b>Total Roadway Operations and Maintenance</b>	<b>7,507,700</b>	<b>261,530</b>	<b>3.48%</b>	<b>478,670</b>
<b>Toll Processing and Collection Expense</b>				
Image Processing	3,000,000	160,000	5.33%	283,382
Tag Collection Fees	6,041,000	1,485,254	24.59%	899,025
Court Enforcement Costs	75,000	-	-	-
DMV Lookup Fees	250	-	-	-
<b>Total Processing and Collection Expense</b>	<b>9,116,250</b>	<b>1,645,254</b>	<b>18.05%</b>	<b>1,182,407</b>

**Central Texas Regional Mobility Authority**  
**Income Statement**  
**For the Period Ending August 31, 2021**

	Budget Amount FY 2021	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
<b>Toll Operations Expense</b>				
Generator Fuel	3,000	-	-	-
Fire and Burglar Alarm	500	-	-	-
Refuse	2,200	262	11.91%	229
Water - Irrigation	7,500	423	5.64%	306
Electricity	500	123	24.68%	106
ETC spare parts expense	50,000	-	-	-
Repair & Maintenance Toll Equip	75,000	-	-	-
Law Enforcement	450,000	26,200	5.82%	39,468
ETC Maintenance Contract	5,390,000	54,000	1.00%	704,980
ETC Toll Management Center System Operation	642,852	37,500	5.83%	88,187
ETC Development	1,140,000	192,580	16.89%	98,030
ETC Testing	200,000	-	-	700
<b>Total Toll Operations Expense</b>	<b>7,961,552</b>	<b>311,088</b>	<b>3.91%</b>	<b>932,006</b>
<b>Total Operations and Maintenance</b>	<b>32,659,854</b>	<b>3,252,497</b>	<b>9.96%</b>	<b>3,625,387</b>
<b>Other Expenses</b>				
<b>Special Projects and Contingencies</b>				
HERO	148,000	12,319	8.32%	12,319
Special Projects	150,000	-	-	4,447
71 Express Net Revenue Payment	4,000,000	-	-	-
Technology Initiatives	185,000	7,058	3.82%	21,145
Other Contractual Svcs	370,000	17,000	4.59%	122,202
Contingency	300,000	-	-	-
<b>Total Special Projects and Contingencies</b>	<b>5,153,000</b>	<b>36,377</b>	<b>0.71%</b>	<b>160,114</b>

**Central Texas Regional Mobility Authority**  
**Income Statement**  
**For the Period Ending August 31, 2021**

	Budget Amount FY 2021	Actual Year to Date	Percent of Budget	Actual Prior Year to Date
<b>Non Cash Expenses</b>				
Amortization Expense	1,125,000	233,186	20.73%	150,833
Amort Expense - Refund Savings	2,715,425	452,571	16.67%	176,302
Dep Exp - Furniture & Fixtures	2,614	436	16.67%	436
Dep Expense - Equipment	2,500	417	16.67%	417
Dep Expense - Autos & Trucks	43,085	3,823	8.87%	7,195
Dep Expense - Buildng & Toll Fac	176,748	29,458	16.67%	29,458
Dep Expense - Highways & Bridges	49,342,469	8,436,924	17.10%	5,797,390
Dep Expense - Toll Equipment	4,060,300	679,072	16.72%	609,638
Dep Expense - Signs	1,202,171	169,428	14.09%	169,428
Dep Expense - Land Improvements	1,163,209	147,489	12.68%	147,489
Depreciation Expense - Computers	192,000	31,514	16.41%	32,699
Undevelopable Projects	-	-	-	4,468,748
<b>Total Non Cash Expenses</b>	<b>60,025,522</b>	<b>10,184,317</b>	<b>16.97%</b>	<b>11,590,033</b>
<b>Total Other Expenses</b>				
	<b>65,178,522</b>	<b>10,220,695</b>	<b>15.68%</b>	<b>11,750,147</b>
<b>Non Operating Expenses</b>				
Bond Issuance Expense	1,227,474	140,570	11.45%	171,619
Loan Fee Expense	50,000	-	-	-
Interest Expense	83,789,516	13,707,378	16.36%	6,734,866
Community Initiatives	57,500	2,550	4.43%	5,050
<b>Total Non Operating Expenses</b>	<b>85,124,490</b>	<b>13,850,498</b>	<b>16.27%</b>	<b>6,911,535</b>
<b>TOTAL EXPENSES</b>	<b>\$195,626,952</b>	<b>\$28,585,457</b>	<b>14.61%</b>	<b>\$23,621,952</b>
<b>Net Income</b>	<b>(\$41,321,188)</b>	<b>\$103,689</b>		<b>(6,364,086)</b>

**Central Texas Regional Mobility Authority**  
**Balance Sheet**  
**as of August 31, 2021**

	as of 08/31/2021		as of 08/31/2020	
<b>ASSETS</b>				
<b>Current Assets</b>				
<b>Cash</b>				
Regions Operating Account	\$	899,883	\$	246,210
Cash in TexStar		440,210		240,071
Regions Payroll Account		166,851		108,071
<b>Restricted Cash</b>				
Goldman Sachs FSGF 465		806,475,366		122,065,948
Restricted Cash - TexSTAR		154,480,846		276,636,565
Overpayments account		688,742		719,478
<b>Total Cash and Cash Equivalents</b>		963,151,899		400,016,342
<b>Accounts Receivable</b>				
Accounts Receivable		2,770,089		2,770,089
Due From Other Agencies		76,268		45,611
Due From TTA		2,134,668		777,862
Due From NTTA		1,247,828		725,839
Due From HCTRA		1,715,017		970,521
Due From TxDOT		361,003		740,574
Interest Receivable		1,964,162		314,596
<b>Total Receivables</b>		10,269,034		6,345,093
<b>Short Term Investments</b>				
Treasuries		268,632,640		9,855,135
Agencies		-		10,144,865
<b>Total Short Term Investments</b>		268,632,640		20,000,000
<b>Total Current Assets</b>		1,242,053,574		426,361,435
<b>Total Construction in Progress</b>		204,486,315		645,909,465
<b>Fixed Assets (Net of Depreciation and Amortization)</b>				
Computers		256,074		446,254
Computer Software		2,424,280		3,229,707
Furniture and Fixtures		4,356		6,970
Equipment		120,047		4,207
Autos and Trucks		35,709		66,224
Buildings and Toll Facilities		4,564,308		4,741,056
Highways and Bridges		1,754,264,393		1,187,689,075
Toll Equipment		21,796,971		22,263,609
Signs		13,554,909		12,875,729
Land Improvements		6,936,714		7,821,648
Right of way		88,149,606		88,149,606
Leasehold Improvements		83,164		129,307
<b>Total Fixed Assets</b>		1,892,190,532		1,327,423,391
<b>Other Assets</b>				
Intangible Assets-Net		123,933,985		100,912,279
2005 Bond Insurance Costs		3,611,848		3,825,356
Prepaid Insurance		51,299		188,809
Deferred Outflows (pension related)		641,074		198,767
Pension Asset		591,247		896,834
<b>Total Other Assets</b>		128,829,452		106,022,046
<b>Total Assets</b>		\$ 3,467,559,872		\$ 2,505,716,337

**Central Texas Regional Mobility Authority**  
**Balance Sheet**  
**as of August 31, 2021**

	as of 08/31/2021	as of 08/31/2020
<b>LIABILITIES</b>		
<b>Current Liabilities</b>		
Accounts Payable	\$ 66,637,480	\$ 7,029,091
Construction Payable	11,552,071	20,988,259
Overpayments	692,058	722,663
Salaries Payable	-	-
Interest Payable	18,288,130	9,957,006
Due to other Funds	-	1,687,633
Deferred Compensation Payable	-	-
TCDRS Payable	79,882	71,733
Health Insurance Payable	-	-
Medical Reimbursement Payable	-	-
Due to other Agencies	8,018	4,784
Due to TTA	636,027	404,307
Due to NTTA	91,905	53,095
Due to HCTRA	128,705	72,730
Due to TIFIA	-	-
Due to State of Texas	-	-
Due to Other Entities	1,302,613	800,954
71E TxDOT Obligation - ST	1,523,691	1,268,601
FICA Payable	-	-
FICA MED PAYABLE	-	-
Federal Withholding Payable	-	-
Other	-	-
<b>Total Current Liabilities</b>	<b>100,940,580</b>	<b>43,060,855</b>
<b>Long Term Liabilities</b>		
Compensated Absences	329,791	543,329
Retainage Payable	-	-
Arbitrage Payable	-	-
Deferred Inflows (pension related)	109,052	164,402
<b>Long Term Payables</b>	<b>438,844</b>	<b>707,731</b>
<b>Bonds Payable</b>		
<b>Senior Lien Revenue Bonds:</b>		
Sr Lien Rev Bonds Paybl	-	-
Senior Lien Revenue Bonds 2005	-	-
Senior Lien Revenue Bonds 2010	82,336,073	76,419,103
Senior Lien Revenue Bonds 2011	18,760,451	17,634,871
Senior Refunding Bonds 2013	7,080,000	133,195,000
Senior Lien Revenue Bonds 2015	298,790,000	298,790,000
Senior Lien Put Bnd 2015	-	68,785,000
Senior Lien Refunding Revenue Bonds 2016	348,295,000	356,785,000
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	56,205,000	-
Senior Lien Refunding Bonds 2020C	138,435,000	-
Senior Lien Revenue Bonds 2020E	167,160,000	-
Senior Lien Revenue Bonds 2021B	255,075,000	-
Sn Lien Rev Bnd Prem/Disc 2005	-	-
Sn Lien Rev Bnd Prem/Disc 2010	-	-
Sn Lien Rev Bnd Prem/Disc 2011	-	-
Sn Lien Rev Bnd Prem/Disc 2013	2,385,490	4,174,607
Sn Lien Revenue Bnd Prem 2015	16,988,417	18,184,921
Sn Lien Put Bond Prem 2015	-	-
Senior Lien Premium 2016 Revenue Bonds	38,299,760	42,368,485
Sn Lien Revenue Bond Premium 2018	3,371,935	3,638,508

**Central Texas Regional Mobility Authority**  
**Balance Sheet**  
**as of August 31, 2021**

	as of 08/31/2021	as of 08/31/2020
Senior Lien Revenue Bond Premium 2020A	11,450,447	11,656,830
Senior Lien Refunding Bond Premium 2020B	12,217,552	-
Senior Lien Revenue Bonds Premium 2020E	27,285,411	-
Senior Lien Revenue Bonds Premium 2021B	53,721,177	-
<b>Total Senior Lien Revenue Bonds</b>	1,632,466,712	1,126,242,326
<b>Sub Lien Revenue Bonds:</b>		
Jr Lien Rev Bonds Pay Prem/Dis	-	-
Subordinated Lien Bond 2010	-	-
Subordinated Lien Bond 2011	-	-
Sub Lien Refunding Bonds 2013	5,320,000	95,945,000
Sub Lien Refunding Bonds 2016	73,055,000	73,490,000
Subordinated Lien BANs 2018	46,020,000	46,020,000
Sub Lien Refunding Bonds 2020D	99,705,000	-
Subordinated Lien BANs 2020F	110,875,000	-
Subordinate Lien Refunding Bonds 2020G	61,570,000	-
Subordinated Lien BANs 2021C	244,185,000	-
Sub Lien Bond 2011 Prem/Disc	-	-
Sub Refunding 2013 Prem/Disc	508,997	890,744
Sub Refunding 2016 Prem/Disc	6,476,588	7,313,146
Sub Lien BANS 2018 Premium	88,189	705,511
Subordinated Lien BANs 2020F Premium	13,342,882	-
Subordinated Lien Refunding Bonds Premium 2020G	7,504,863	-
Sub Lien BANS 2021C Premium	40,595,613	-
<b>Total Sub Lien Revenue Bonds</b>	709,247,131	224,364,401
<b>Other Obligations</b>		
TIFIA Note 2015	-	298,561,393
TIFIA Note 2019	-	51,917
TIFIA Note 2021	305,282,074	-
SIB Loan 2015	-	33,695,520
State Highway Fund Loan 2015	-	33,695,550
71E TxDOT Obligation - LT	57,263,411	60,728,211
Regions 2017 MoPAC Note	24,990,900	24,990,900
<b>Total Other Obligations</b>	387,536,385	451,723,490
<b>Total Long Term Liabilities</b>	2,729,689,072	1,803,037,948
<b>Total Liabilities</b>	2,830,629,652	1,846,098,804
<b>NET ASSETS</b>		
Contributed Capital	121,462,104	121,462,104
Net Assets Beginning	515,363,818	544,518,906
Current Year Operations	104,299	(6,363,476)
<b>Total Net Assets</b>	636,930,220	659,617,534
<b>Total Liabilities and Net Assets</b>	\$ 3,467,559,872	\$ 2,505,716,337



**Central Texas Regional Mobility Authority**  
**Statement of Cash Flow**  
**as of August 2021**

**Cash flows from operating activities:**

Receipts from toll revenues	\$	28,587,355
Receipts from interest income		38,153
Payments to vendors		(5,076,764)
Payments to employees		(953,835)
Net cash flows provided by (used in) operating activities		22,594,908

**Cash flows from capital and related financing activities:**

Proceeds from notes payable		-
Payments on bonds		-
Interest payments		(38,898,411)
Acquisitions of construction in progress		(39,466,361)
Net cash flows provided by (used in) capital and related financing activities		(78,364,772)

**Cash flows from investing activities:**

Interest income		(11,301,064)
Purchase of investments		(10,554,355)
Proceeds from sale or maturity of investments		21,108,917
Net cash flows provided by (used in) investing activities		(746,501)
Net increase (decrease) in cash and cash equivalents		(56,516,365)
Cash and cash equivalents at beginning of period		1,019,668,263
Cash and cash equivalents at end of period	\$	963,151,899

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

Operating income		\$ 13,802,946
Adjustments to reconcile change in net assets to net cash provided by operating activities:		
Depreciation and amortization		9,964,932
Changes in assets and liabilities:		
(Increase) decrease in accounts receivable		30,963
(Increase) decrease in prepaid expenses and other assets		118,080
(Decrease) increase in accounts payable		(1,270,311)
Increase (decrease) in accrued expenses		(51,701)
(Decrease) increase in Pension Asset		-
(Increase) in deferred outflows of resources		-
(Increase) in deferred inflows of resources		-
Total adjustments		8,791,963
Net cash flows provided by (used in) operating activities	\$	22,594,908

**Reconciliation of cash and cash equivalents:**

Unrestricted cash and cash equivalents		\$ 105,603,799
Restricted cash and cash equivalents		857,548,100
Total	\$	963,151,899

**INVESTMENTS by FUND**

		Balance August 31, 2021		
Renewal & Replacement Fund				
TexSTAR	1,794.27		TexSTAR	154,920,056.14
Goldman Sachs	183,336.09		Goldman Sachs	794,122,478.61
Agencies/ Treasuries		185,130.36	Agencies & Treasury Notes	268,632,640.43
Grant Fund				\$ 1,217,675,175.18
TexSTAR	4,454,566.50			
Goldman Sachs	5,637,211.15			
Agencies/ Treasuries	-	10,091,777.65		
<b>Senior Debt Service Reserve Fund</b>				
TexSTAR	17,728,072.19			
Goldman Sachs	15,791,128.99			
Agencies/ Treasuries	73,901,133.91	107,420,335.09		
2010 Senior Lien Debt Service Account				
Goldman Sachs	60,643.91	60,643.91		
2011 Sr Debt Service Accountt				
Goldman Sachs	853,206.89	853,206.89		
2013 Sr Debt Service Accountt				
Goldman Sachs	2,462,502.82	2,462,502.82		
2013 Sub Debt Service Account				
Goldman Sachs	1,774,504.65	1,774,504.65		
2013 Sub Debt Service Reserve Fund				
Goldman Sachs	59.70	780,793.52		
TexSTAR	780,733.82			
2015 Sr Debt Service Account				
Goldman Sachs	2,489,592.37	2,489,592.37		
2015 Sr Capitalized Interest				
Goldman Sachs	-	1,224.29		
TexSTAR	1,224.29			
2016 Sr Lien Rev Refunding Debt Service Account				
Goldman Sachs	10,226,264.13	10,226,264.13		
2016 Sub Lien Rev Refunding Debt Service Account				
Goldman Sachs	851,564.71	851,564.71		
2016 Sub Lien Rev Refunding DSR				
Goldman Sachs	3,523,617.50			
Agencies/ Treasuries	3,448,268.36	6,971,885.86		
Operating Fund				
TexSTAR	440,209.85			
TexSTAR-Trustee	6,302,630.51			
Goldman Sachs	1,135,028.13	7,877,868.49		
Revenue Fund				
Goldman Sachs	6,445,304.75	6,445,304.75		
General Fund				
TexSTAR	29,878,842.32			
Goldman Sachs	25,986,458.05			
Agencies/ Treasuries	49,267,254.21	105,132,554.58		
71E Revenue Fund				
Goldman Sachs	17,584,524.04	17,584,524.04		
MoPac Revenue Fund				
Goldman Sachs	50,338.58	50,338.58		
MoPac General Fund				
Goldman Sachs	10,381,875.40	10,381,875.40		
MoPac Operating Fund				
Goldman Sachs	2,735,718.22	2,735,718.22		
MoPac Loan Repayment Fund				
Goldman Sachs	35,718.53	35,718.53		
2015B Project Account				
Goldman Sachs	15,976,656.65			
TexSTAR	26,349,683.59	42,326,340.24		
2015 TIFIA Project Account				
Goldman Sachs	30,415.43			
TexSTAR	47,968,273.14			
Agencies/ Treasuries	-	47,998,688.57		
2011 Sr Financial Assistance Fund				
Goldman Sachs	-	8,082,328.88		
TexSTAR	8,082,328.88			
2018 Sr Lien Project Cap I				
Goldman Sachs	2,414,794.65	2,414,794.65		
2018 Sr Lien Project Account				
Goldman Sachs	209,189.43			
TexSTAR	12,931,696.78	13,140,886.21		
2018 Sub Debt Service Account				
Goldman Sachs	5,193,597.48	5,193,597.48		
2019 TIFIA Sub Lien Project Account				
Goldman Sachs	0.00	0.00		
2020A Senior Lien Debt Service Account				
Goldman Sachs	418,941.15	418,941.15		
2020 SH 45SW Project Account				
Goldman Sachs	771,973.54	771,973.54		
2020B Senior Lien Debt Service Account				
Goldman Sachs	857,102.34	857,102.34		
2020C Senior Lien Debt Service Account				
Goldman Sachs	629,954.26	629,954.26		
2020D Sub Lien Debt Service Account				
Goldman Sachs	1,247,291.53	1,247,291.53		
2020D Sub Debt Service Reserve Fund				
Goldman Sachs	4,152,099.41			
Agencies/ Treasuries	3,941,238.91	8,093,338.32		
2020E Senior Lien Project Account				
Goldman Sachs	71,169,488.14			
Agencies/ Treasuries	79,800,617.51	150,970,105.65		
2020E Senior Lien Project Cap Interest				
Goldman Sachs	29,136,096.92	29,136,096.92		
2020F Sub Lien Project Account				
Goldman Sachs	24,822,203.17			
Agencies/ Treasuries	58,274,127.53	83,096,330.70		
2020F Sub Lien Deb Service Account				
Goldman Sachs	924,101.20	924,101.20		
2020G Sub Lien Debt Service Account				
Goldman Sachs	425,503.61	425,503.61		
2020G Sub Lien Debt Service Reserve Account				
Goldman Sachs	1,497,351.08	1,497,351.08		
2021A Sub Lien Debt Service Reserve Account				
Goldman Sachs	5,879,124.33	5,879,124.33	23,222,493.11	
2021B Senior Lien Cap I Project Fund				
Goldman Sachs	57,696,083.51	57,696,083.51		
2021B Senior Lien Project Account				
Goldman Sachs	231,094,871.55	231,094,871.55		
2021C Sub Lien Cap I Project Fund				
Goldman Sachs	6,105,284.63	6,105,284.63		
2021C Sub Lien Project Account				
Goldman Sachs	225,261,755.99	225,261,755.99		
		\$ 1,217,675,175.18		

**CTRMA INVESTMENT REPORT**

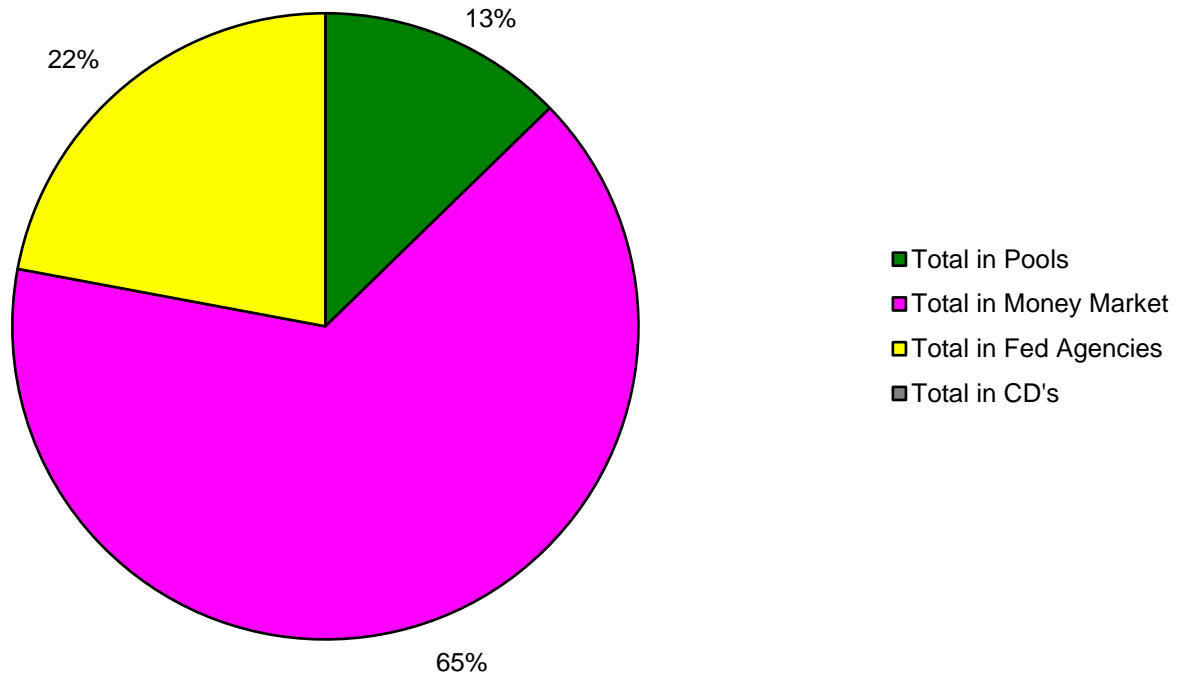
	Month Ending 8/31/2021					Rate August	
	Balance 8/1/2021	Additions	Discount Amortization	Accrued Interest	Withdrawals		Balance 8/31/2021
<b>Amount in Trustee TexStar</b>							
2011 Sr Lien Financial Assist Fund	8,966,006.62			72.26	883,750.00	8,082,328.88	0.0100%
2013 Sub Lien Debt Service Reserve General Fund	780,727.27			6.55		780,733.82	0.0100%
Trustee Operating Fund	29,878,588.47	3,000,000.00		253.85		29,878,842.32	0.0100%
Renewal and Replacement	5,502,584.99			45.52	2,200,000.00	6,302,630.51	0.0100%
Grant Fund	1,794.27			0.00		1,794.27	0.0100%
Senior Lien Debt Service Reserve Fund	4,454,528.68			37.82		4,454,566.50	0.0100%
2015A Sr Ln Project Cap Interest	17,727,921.57			150.62		17,728,072.19	0.0100%
2015B Sr Ln Project	1,224.29			0.00		1,224.29	0.0100%
2015C TIFIA Project	26,349,459.77			223.82		26,349,683.59	0.0100%
2018 Sr Lien Project Account	48,703,142.98			412.58	735,282.42	47,968,273.14	0.0100%
	12,931,587.00			109.78		12,931,696.78	0.0100%
	155,297,565.91	3,000,000.00		1,312.80	3,819,032.42	154,479,846.29	
<b>Amount in TexStar Operating Fund</b>	440,205.80	2,200,000.00		4.05	2,200,000.00	440,209.85	0.0100%
<b>Goldman Sachs</b>							
Operating Fund	1,081,581.00	3,060,332.60		22.75	3,006,908.22	1,135,028.13	0.0300%
2020 SH 45SW Project Account	771,947.66	7.90		17.98		771,973.54	0.0300%
2020A Senior Lien Debt Service Account	209,517.00	209,421.60		2.55		418,941.15	0.0300%
2020B Senior Lien Debt Service Account	579,859.07	277,233.19		10.08		857,102.34	0.0300%
2020C Senior Lien Debt Service Account	315,046.01	314,904.42		3.83		629,954.26	0.0300%
2020D Sub Lien Debt Service Account	904,983.96	342,290.94		16.63		1,247,291.53	0.0300%
2020D Sub Debt Service Reserve Fund	4,152,007.38			92.03		4,152,099.41	0.0300%
2020E Sr Lien Project Account	71,167,910.71			1,577.43		71,169,488.14	0.0300%
2020E Sr Ln Project Cap Interest	29,135,451.14			645.78		29,136,096.92	0.0300%
2020E Sr Lien Debt Service Account	0.00			0.00		0.00	0.0300%
2020F Sub Lien Project Account	25,017,979.35			644.23	196,420.41	24,822,203.17	0.0300%
2020F Sub Lien Debt Service Account	462,150.72	461,944.86		5.62		924,101.20	0.0300%
2020G Sub Lien Debt Service Account	212,801.28	212,699.74		2.59		425,503.61	0.0300%
2020G Sub Debt Service Reserve Fund	1,401,457.45	95,863.53		30.10		1,497,351.08	0.0300%
2021A Sub Debt Service Reserve Fund	5,688,782.36	190,217.78		124.19		5,879,124.33	0.0300%
2021B Senior Lien Cap I Project Fund	57,694,804.71			1,278.80		57,696,083.51	0.0300%
2021B Senior Lien Project Account	231,136,194.01			5,123.29	46,445.75	231,094,871.55	0.0300%
2021B Senior Lien Debt Service Account	0.00			0.00		0.00	0.0300%
2021C Sub Lien Cap I Project Fund	6,105,149.31			135.32		6,105,284.63	0.0300%
2021C Sub Lien Project Account	234,905,841.63	1,404,512.47		5,317.45	11,053,915.56	225,261,755.99	0.0300%
2021C Sub Lien Debt Service Account	0.00			0.00		0.00	0.0300%
2011 Sr Financial Assistance Fund	0.00			0.00		0.00	0.0300%
2010 Senior DSF	60,642.57			1.34		60,643.91	0.0300%
2011 Senior Lien Debt Service Account	845,205.36	7,982.88		18.65		853,206.89	0.0300%
2013 Senior Lien Debt Service Account	2,132,573.55	329,885.30		43.97		2,462,502.82	0.0300%
2013 Sub Debt Service Reserve Fund	59.70			0.00		59.70	0.0300%
2013 Subordinate Debt Service Account	1,536,056.32	238,416.67		31.66		1,774,504.65	0.0300%
2015A Sr Lien Debt Service Account	1,244,834.26	1,244,742.98		15.13		2,489,592.37	0.0300%
2015A Sr Ln Project Cap Interest	0.00			0.00		0.00	0.0300%
2015B Project Account	15,976,302.54			354.11		15,976,656.65	0.0300%
2015C TIFIA Project Account	30,793.13	735,282.42		0.62	735,660.74	30,415.43	0.0300%
2016 Sr Lien Rev Refunding Debt Service Account	8,011,598.72	2,214,510.00		155.41		10,226,264.13	0.0300%
2016 Sub Lien Rev Refunding Debt Service Account	538,349.53	313,206.38		8.80		851,564.71	0.0300%
2016 Sub Lien Rev Refunding DSR	3,523,539.40			78.10		3,523,617.50	0.0300%
2018 Sr Lien Project Cap I	2,414,741.13			53.52		2,414,794.65	0.0300%
2019 Sr Lien Project Cap I Debt Service Account	0.00			0.00		0.00	0.0300%
2018 Sr Lien Project Account	274,114.29			39.95	64,964.81	209,189.43	0.0300%
2018 Sub Debt Service Account	4,429,352.06	764,154.89		90.53		5,193,597.48	0.0300%
2019 TIFIA Sub Lien Project Account	0.00			0.00		0.00	0.0300%
Grant Fund	5,637,086.43			124.72		5,637,211.15	0.0300%
Renewal and Replacement	183,332.05			4.04		183,336.09	0.0300%
Revenue Fund	9,362,751.87	15,525,774.52		131.68	18,443,353.32	6,445,304.75	0.0300%
General Fund	19,198,473.11	6,930,606.52		434.35	143,055.93	25,986,458.05	0.0300%
Senior Lien Debt Service Reserve Fund	15,790,778.99			350.00		15,791,128.99	0.0300%
71E Revenue Fund	16,766,638.60	906,308.57		361.88	88,785.01	17,584,524.04	0.0300%
MoPac Revenue Fund	56,429.04	690,335.63		2.93	696,429.02	50,338.58	0.0300%
MoPac General Fund	10,191,709.37	496,429.02		219.65	306,482.64	10,381,875.40	0.0300%
MoPac Operating Fund	2,647,731.29	250,410.62		56.46	162,480.15	2,735,718.22	0.0300%
MoPac Loan Repayment Fund	0.00	35,718.43		0.10		35,718.53	0.0300%
	791,796,558.06	37,253,193.86		17,628.25	34,944,901.56	794,122,478.61	
<b>Amount in Fed Agencies and Treasuries</b>							
Amortized Principal	269,006,794.45		(374,154.02)	0.00		268,632,640.43	
	269,006,794.45	0.00	(374,154.02)	0.00		268,632,640.43	
<b>Certificates of Deposit</b>							
<b>Total in Pools</b>	155,737,771.71	5,200,000.00		1,316.85	6,019,032.42	154,920,056.14	
<b>Total in GS FSGF</b>	791,796,558.06	37,253,193.86		17,628.25	34,944,901.56	794,122,478.61	
<b>Total in Fed Agencies and Treasuries</b>	269,006,794.45	0.00	(374,154.02)	0.00		268,632,640.43	
<b>Total Invested</b>	1,216,541,124.22	42,453,193.86		18,945.10	40,963,933.98	1,217,675,175.18	

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

Mary Temple, Controller

8/31/2021

## Allocation of Funds



Amount of Investments As of August 31, 2021

Agency	CUSIP #	COST	Book Value	Market Value	Yield to Maturity	Purchased	Matures	FUND
Treasury	912828J76B	3,969,623.85	3,941,238.91	3,939,448.33	0.9787%	3/9/2021	3/31/2022	2020D Sub DSR
Treasury	912828J76	3,473,102.91	3,448,268.36	3,446,701.75	0.9787%	3/9/2021	3/31/2022	2016 Sub DSR
Treasury	912828J76E	80,375,344.30	79,800,617.51	79,764,362.49	0.9787%	3/9/2021	3/31/2022	2020E Sr Project
Treasury	912828J76D	74,433,372.42	73,901,133.91	73,867,559.15	0.9787%	3/9/2021	3/31/2022	Sr Lien DSR
Treasury	912828J76A	29,773,450.70	29,560,554.58	29,547,124.63	0.9787%	3/9/2021	3/31/2022	2020F Sub Project
Treasury	912828T34	28,856,437.70	28,713,572.95	28,701,806.54	0.0530%	3/9/2021	9/30/2021	2020F Sub Project
Treasury	912828J76C	49,622,078.65	49,267,254.21	49,244,871.15	0.9787%	3/9/2021	3/31/2022	General Fund
		<u>270,503,410.53</u>	<u>268,632,640.43</u>	<u>268,511,874.04</u>				

Agency	CUSIP #	COST	Cummulative Amortization	Book Value	Maturity Value	Interest Income		
						Accrued Interest	Amortization	Interest Earned
Treasury	912828J76B	3,969,623.85	(28,384.94)	3,941,238.91	3,413,500.00	5,689.69	(5,676.99)	12.70
Treasury	912828J76	3,473,102.91	(24,834.55)	3,448,268.36	3,413,500.00	4,978.02	(4,966.91)	11.11
Treasury	912828J76E	80,375,344.30	(574,726.79)	79,800,617.51	3,413,500.00	115,202.50	(114,945.36)	257.14
Treasury	912828J76D	74,433,372.42	(532,238.51)	73,901,133.91	3,413,500.00	106,685.83	(106,447.70)	238.13
Treasury	912828J76A	29,773,450.70	(212,896.12)	29,560,554.58	3,413,500.00	42,674.48	(42,579.22)	95.26
Treasury	912828T34	28,856,437.70	(142,864.75)	28,713,572.95	3,413,500.00	26,892.19	(28,572.95)	(1,680.76)
Treasury	912828J76C	49,622,078.65	(354,824.44)	49,267,254.21	3,413,500.00	71,123.65	(70,964.89)	158.76
		<u>270,503,410.53</u>	<u>(1,870,770.10)</u>	<u>268,632,640.43</u>	<u>23,894,500.00</u>	<u>373,246.36</u>	<u>(374,154.02)</u>	<u>(907.66)</u>

## ESCROW FUNDS

### Travis County Escrow Fund - Elroy Road

	<u>Balance</u>		<u>Accrued</u>		<u>Balance</u>
	<u>8/1/2021</u>	<u>Additions</u>	<u>Interest</u>	<u>Withdrawals</u>	<u>8/31/2021</u>
Goldman Sachs	10,943,133.89		253.46	429,635.46	10,513,751.89

### Travis County Escrow Fund - Ross Road

	<u>Balance</u>		<u>Accrued</u>		<u>Balance</u>
	<u>8/1/2021</u>	<u>Additions</u>	<u>Interest</u>	<u>Withdrawals</u>	<u>8/31/2021</u>
Goldman Sachs	105,894.26		3.87		105,898.13

### Travis County Escrow Fund - Old San Antonio Road

	<u>Balance</u>		<u>Accrued</u>		<u>Balance</u>
	<u>8/1/2021</u>	<u>Additions</u>	<u>Interest</u>	<u>Withdrawals</u>	<u>8/31/2021</u>
Goldman Sachs	89,104.94		4.91		89,109.85

### Travis County Escrow Fund - Old Lockhart Road

	<u>Balance</u>		<u>Accrued</u>		<u>Balance</u>
	<u>8/1/2021</u>	<u>Additions</u>	<u>Interest</u>	<u>Withdrawals</u>	<u>8/31/2021</u>
Goldman Sachs	267,712.21		8.58		267,720.79

### Travis County Escrow Fund - County Line Road

	<u>Balance</u>		<u>Accrued</u>		<u>Balance</u>
	<u>8/1/2021</u>	<u>Additions</u>	<u>Interest</u>	<u>Withdrawals</u>	<u>8/31/2021</u>
Goldman Sachs	507,596.33		13.05	9,018.58	498,590.80

### Travis County Escrow Fund - South Pleasant Valley Road

	<u>Balance</u>		<u>Accrued</u>		<u>Balance</u>
	<u>8/1/2021</u>	<u>Additions</u>	<u>Interest</u>	<u>Withdrawals</u>	<u>8/31/2021</u>
Goldman Sachs	366,229.08		8.26		366,237.34

### Travis County Escrow Fund - Thaxton Road

	<u>Balance</u>		<u>Accrued</u>		<u>Balance</u>
	<u>8/1/2021</u>	<u>Additions</u>	<u>Interest</u>	<u>Withdrawals</u>	<u>8/31/2021</u>
Goldman Sachs	163,651.31		3.68		163,654.99

### Travis County Escrow Fund - Pearce Lane Road

	<u>Balance</u>		<u>Accrued</u>		<u>Balance</u>
	<u>8/1/2021</u>	<u>Additions</u>	<u>Interest</u>	<u>Withdrawals</u>	<u>8/31/2021</u>
Goldman Sachs	357,915.66		8.02		357,923.68



**183 South Design-Build Project**  
**Contingency Status**  
 August 31, 2021



**Original Construction Contract Value: \$581,545,700**

<b>Total Project Contingency</b>	<b>\$47,860,000</b>
----------------------------------	---------------------

<b>Obligations</b>	CO#1 City of Austin ILA Adjustment	(\$2,779,934)
	CO#2 Addition of Coping to Soil Nail Walls	\$742,385
	CO#4 Greenroads Implementation	\$362,280
	CO#6 51st Street Parking Trailhead	\$477,583
	CO#9 Patton Interchange Revisions	\$3,488,230
	CO#10 City of Austin Utility (\$1,010,000 - no cost to RMA)	\$0
	CO#17 Boggy Creek Turnaround	\$2,365,876
	CO#21 Wall 125 Differing Site Condition - Part A	\$1,263,577
	CO#26 Roadway Paving Additions	\$1,302,696
	CO#28 Cable Barrier System	\$316,501
	CO#21b Wall 125 Differing Site Condition - Part B	\$1,292,264
	CO-31 City of Austin Waterline 133 (Bolm Rd)	\$632,557
	CO-37 Montopolis Truss Bridge Rail Revision and Overlay	\$597,572
	Others Less than \$300,000 (29)	\$3,749,592
Executed Change Orders		\$13,811,000
Change Orders Under Negotiation		\$620,000
Potential Contractual Obligations		\$12,292,000

<b>(-) Total Obligations</b>	<b>\$26,723,000</b>
------------------------------	---------------------

<b>Remaining Project Contingency</b>	<b>\$21,137,000</b>
--------------------------------------	---------------------



**290E Ph. III**  
**Contingency Status**  
 August 31, 2021



**Original Construction Contract Value: \$71,236,424**

<b>Total Mobility Authority Contingency</b>	<b>\$10,633,758</b>
<b>Total TxDOT Project Contingency</b>	<b>\$15,292,524</b>

<b>Obligations</b>	Others Less than \$300,000 (11)	\$311,351
	Executed Change Orders	\$311,351
	Change Orders Under Negotiation	\$277,709
	Potential Contractual Obligations	\$1,860,000

<b>(-) Total Obligations</b>	<b>\$2,449,060</b>
------------------------------	--------------------

<b>Remaining Mobility Authority Contingency</b>	<b>\$8,404,909</b>
<b>Remaining TxDOT Contingency</b>	<b>\$15,072,313</b>





# 183A Phase III Project

## Contingency Status

August 31, 2021



**Original Construction Contract Value: \$175,695,656**

<b>Total Project Contingency</b>	<b>\$9,640,442</b>
----------------------------------	--------------------

<b>Obligations</b>	Others Less than \$300,000 (2)	\$0
	Executed Change Orders	\$0
	Change Orders Under Negotiation	\$45,000
	Potential Contractual Obligations	\$0

<b>(-) Total Obligations</b>	<b>\$45,000</b>
------------------------------	-----------------

<b>Remaining Project Contingency</b>	<b>\$9,595,442</b>
--------------------------------------	--------------------



**183 North Mobility Project**  
**Contingency Status**  
 August 31, 2021



**Original Construction Contract Value: \$477,149,654**

<b>Total Project Contingency</b>	<b>\$39,541,000</b>
----------------------------------	---------------------

<b>Obligations</b>		
	Executed Change Orders	\$0
	Change Orders Under Negotiation	\$15,510,000
	Potential Contractual Obligations	\$0

<b>(-) Total Obligations</b>	<b>\$15,510,000</b>
------------------------------	---------------------

<b>Remaining Project Contingency</b>	<b>\$24,031,000</b>
--------------------------------------	---------------------



## PERFORMANCE

### As of August 31, 2021

Current Invested Balance	\$8,945,411,473.29
Weighted Average Maturity (1)	50 Days
Weighted Average Life (2)	71 Days
Net Asset Value	1.000063
Total Number of Participants	955
Management Fee on Invested Balance	0.06%*
Interest Distributed	\$484,103.67
Management Fee Collected	\$407,093.35
% of Portfolio Invested Beyond 1 Year	0.88%
Standard & Poor's Current Rating	AAAm

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

### August Averages

Average Invested Balance	\$9,067,340,125.32
Average Monthly Yield, on a simple basis	0.0100%
Average Weighted Maturity (1)	52 Days
Average Weighted Life (2)	74 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 waved in full or in part in the discretion of the TexSTAR co-administrators at any time as provided for in the TexSTAR Information Statement.

## NEW PARTICIPANTS

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

- |  |   |
|--|---|
| * Fort Bend County Levee Improvement District No. 6  | * Fort Bend County Municipal Utility District No. 39  |
| * Fort Bend County Municipal Utility District No. 49 | * Fort Bend County Municipal Utility District No. 207 |
| * City of Gatesville                                 | * Harris County Municipal Utility District No. 152    |

## HOLIDAY REMINDER

In observance of **Columbus Day**, **TexSTAR will be closed on Monday, October 11, 2021**. All ACH transactions initiated on Friday, October 8th will settle on Tuesday, October 12th. Please plan accordingly for your liquidity needs.

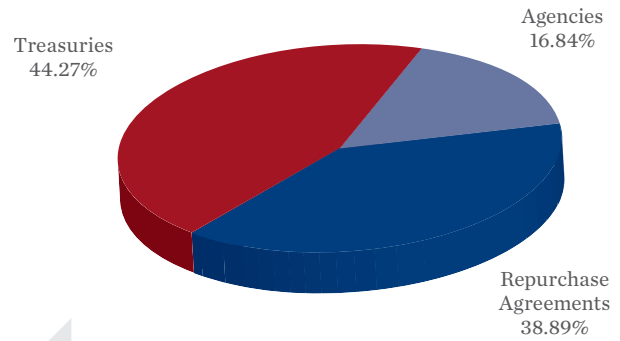
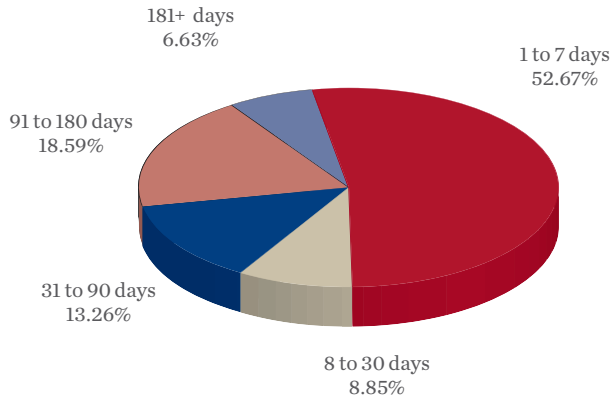
## ECONOMIC COMMENTARY

### Market review

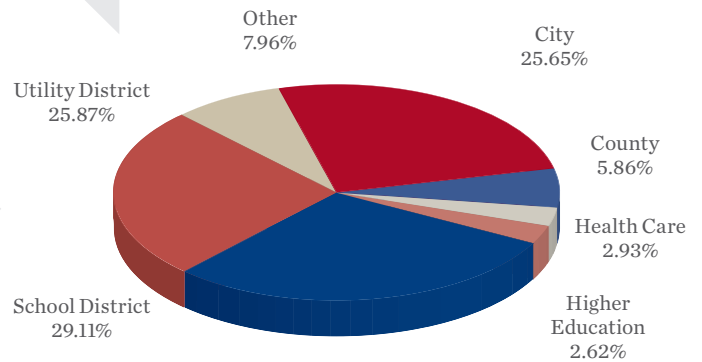
Recent economic data prints suggested a constructive macro outlook despite Delta variant concerns. Fed policy continued to remain accommodative, and risk markets marched higher as investors focused on news of the FDA's full approval of the Pfizer vaccine. Within fixed income markets, longer term U.S. Treasury note yields rose at the end of the month as Fed tapering expectations continued to be priced in, while Treasury bill yields were relatively unchanged. Strong data prints and easy monetary policy continued to provide a tailwind for economic growth, despite growth momentum having already peaked. August's flash purchasing managers' indices (PMIs) printed at 61.2 and 55.4 for manufacturing and services, respectively. Inflation has now well surpassed the FOMC's 2% target, as the headline PCE price index rose +0.4% month-over-month (m/m) and +4.2% year-over-year (y/y) in July. The core PCE deflator also rose to +0.3% m/m and +3.6% y/y, with the latter slightly above market expectations. The July CPI report showed consumer prices rising at their fastest 12-month rate in more than a decade, but the moderation in the month-over-month pace signaled that some of the drivers of much higher inflation are beginning to subside. Headline CPI for July rose +0.5% m/m, from 0.9% in June, and +5.4% y/y, while consumer prices excluding food and energy rose +0.3% m/m and +4.3% y/y.

## INFORMATION AT A GLANCE

### PORTFOLIO BY TYPE OF INVESTMENT AS OF AUGUST 31, 2021



### PORTFOLIO BY MATURITY AS OF AUGUST 31, 2021 (1)



### DISTRIBUTION OF PARTICIPANTS BY TYPE AS OF AUGUST 31, 2021

## HISTORICAL PROGRAM INFORMATION

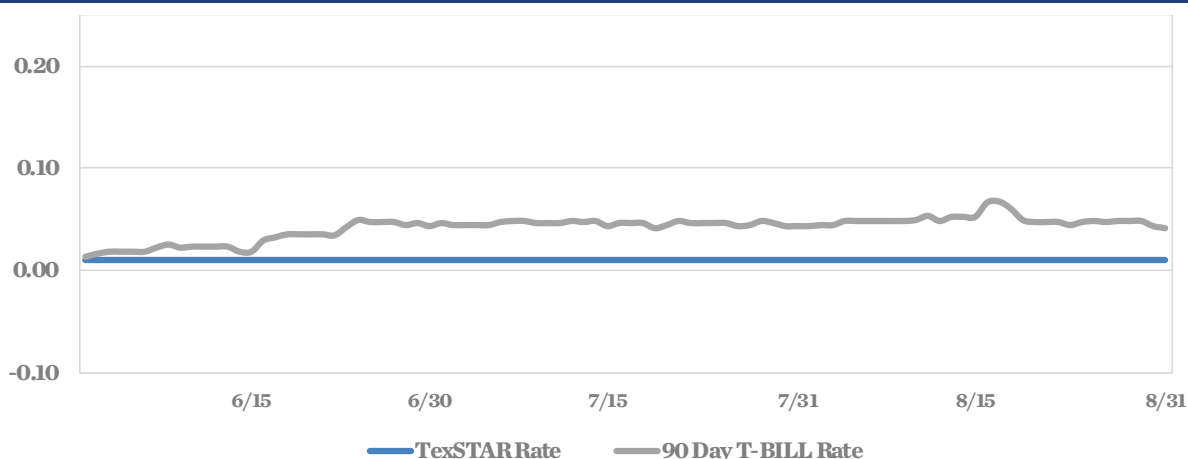
MONTH	AVERAGE RATE	BOOK VALUE	MARKET VALUE	NET ASSET VALUE	WAM (1)	WAL (2)	NUMBER OF PARTICIPANTS
Aug 21	0.0100%	\$8,945,411,473.29	\$8,945,978,474.21	1.000063	52	74	955
Jul 21	0.0100%	9,139,785,043.86	9,140,404,119.19	1.000071	41	68	949
Jun 21	0.0100%	9,172,985,137.74	9,173,600,615.43	1.000084	40	71	943
May 21	0.0100%	9,216,832,522.03	9,217,901,991.74	1.000116	46	82	938
Apr 21	0.0113%	8,986,711,365.42	8,987,836,525.94	1.000131	40	78	936
Mar 21	0.0216%	9,103,231,627.43	9,104,638,524.44	1.000154	47	86	935
Feb 21	0.0334%	9,576,230,496.50	9,577,678,764.35	1.000151	46	87	934
Jan 21	0.0583%	9,443,485,770.86	9,445,046,065.21	1.000165	38	84	934
Dec 20	0.0676%	8,682,050,804.34	8,683,648,113.09	1.000183	42	96	933
Nov 20	0.0944%	8,910,228,194.78	8,911,909,859.79	1.000188	46	104	933
Oct 20	0.1150%	9,083,922,054.96	9,085,783,748.92	1.000203	42	100	933
Sep 20	0.1339%	9,297,135,540.13	9,299,528,645.66	1.000257	39	101	932

## PORTFOLIO ASSET SUMMARY AS OF AUGUST 31, 2021

	BOOK VALUE	MARKET VALUE
Uninvested Balance	\$ (2,743.43)	\$ (2,743.43)
Accrual of Interest Income	1,266,047.56	1,266,047.56
Interest and Management Fees Payable	(508,165.43)	(508,165.43)
Payable for Investment Purchased	(149,982,937.50)	(149,982,937.50)
Repurchase Agreement	3,536,889,999.74	3,536,889,999.74
Government Securities	5,557,749,272.35	5,558,316,273.27
<b>TOTAL</b>	<b>\$ 8,945,411,473.29</b>	<b>\$ 8,945,978,474.21</b>

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 2021

DATE	MNY MKT FUND EQUIV. [SEC Std.]	DAILY ALLOCATION FACTOR	INVESTED BALANCE	MARKET VALUE PER SHARE	WAM DAYS (1)	WAL DAYS (2)
8/1/2021	0.0100%	0.000000274	\$9,139,785,043.86	1.000071	53	76
8/2/2021	0.0100%	0.000000274	\$9,151,162,913.67	1.000075	52	76
8/3/2021	0.0100%	0.000000274	\$9,185,379,328.13	1.000072	52	76
8/4/2021	0.0100%	0.000000274	\$9,186,464,956.26	1.000072	52	75
8/5/2021	0.0100%	0.000000274	\$9,216,656,732.26	1.000068	52	76
8/6/2021	0.0100%	0.000000274	\$9,318,049,214.46	1.000075	50	73
8/7/2021	0.0100%	0.000000274	\$9,318,049,214.46	1.000075	50	73
8/8/2021	0.0100%	0.000000274	\$9,318,049,214.46	1.000075	50	73
8/9/2021	0.0100%	0.000000274	\$9,246,210,452.22	1.000075	51	74
8/10/2021	0.0100%	0.000000274	\$9,245,761,350.97	1.000071	51	73
8/11/2021	0.0100%	0.000000274	\$9,266,389,770.51	1.000068	53	75
8/12/2021	0.0100%	0.000000274	\$9,146,796,007.22	1.000068	54	77
8/13/2021	0.0100%	0.000000274	\$9,058,732,498.74	1.000071	53	76
8/14/2021	0.0100%	0.000000274	\$9,058,732,498.74	1.000071	53	76
8/15/2021	0.0100%	0.000000274	\$9,058,732,498.74	1.000071	53	76
8/16/2021	0.0100%	0.000000274	\$9,093,189,217.50	1.000073	53	75
8/17/2021	0.0100%	0.000000274	\$9,097,924,038.68	1.000078	53	75
8/18/2021	0.0100%	0.000000274	\$9,149,047,036.58	1.000074	52	74
8/19/2021	0.0100%	0.000000274	\$9,079,467,542.63	1.000081	52	74
8/20/2021	0.0100%	0.000000274	\$8,949,895,457.46	1.000076	51	74
8/21/2021	0.0100%	0.000000274	\$8,949,895,457.46	1.000076	51	74
8/22/2021	0.0100%	0.000000274	\$8,949,895,457.46	1.000076	51	74
8/23/2021	0.0100%	0.000000274	\$9,000,805,560.38	1.000069	51	73
8/24/2021	0.0100%	0.000000274	\$8,880,419,613.23	1.000080	53	75
8/25/2021	0.0100%	0.000000274	\$8,909,070,093.24	1.000078	52	74
8/26/2021	0.0100%	0.000000274	\$8,896,171,040.23	1.000080	52	74
8/27/2021	0.0100%	0.000000274	\$8,814,718,340.57	1.000074	51	73
8/28/2021	0.0100%	0.000000274	\$8,814,718,340.57	1.000074	51	73
8/29/2021	0.0100%	0.000000274	\$8,814,718,340.57	1.000074	51	73
8/30/2021	0.0100%	0.000000274	\$8,827,245,180.44	1.000079	51	73
8/31/2021	0.0100%	0.000000274	\$8,945,411,473.29	1.000063	50	71
22						
<b>Average</b>	<b>0.0100%</b>	<b>0.000000274</b>	<b>\$9,067,340,125.32</b>		<b>52</b>	<b>74</b>



## *ECONOMIC COMMENTARY (cont.)*

While inflation remained at elevated levels, July's figures signaled that some of the "transitory" components of much higher inflation are finally beginning to moderate. While this should give the Fed some confidence in their transitory argument, the rise in prices has certainly been stronger and more sustained than they predicted earlier this year. At the highly anticipated Federal Reserve's annual Jackson Hole summit, Chairman Powell's speech depicted a clearer outlook for tapering asset purchases. In his view, the inflation criteria for tapering asset purchases has now been met and while there is still "much ground to cover" before the economy reaches full employment, he broadly hinted tapering could begin before the end of the year. In line with this, we believe the Fed will announce a timetable for tapering later this fall, and begin to taper the pace of its purchases in December. He reaffirmed his view that current inflation levels are transitory and stressed that interest rate hikes are not imminent. After showing strong improvement in July, hiring momentum in August slowed sharply as the Delta variant curbed in-person consumer activity and businesses continued to grapple with chronic labor shortages. However, despite the slowdown in hiring, robust wage growth suggested the weakness is primarily supply-side driven. Total nonfarm payrolls increased by a meager +235,000 in August, falling well short of consensus expectations, but saw meaningful upward revisions to the June and July readings. The leisure and hospitality sector, which had been the powerhouse for job gains this year, significantly disappointed with zero net job creation. The leisure and hospitality sector is the most vulnerable to a demand slowdown from renewed pandemic worries, but they also have the lowest-paid workers and as such, are most impacted by acute labor shortages.

In contrast, the unemployment rate fell to 5.2% from 5.4% in July, while the labor force participation rate remained at 61.7%. Additionally, wages spiked higher as average hourly earnings, albeit a noisy series, continued to demonstrate robust improvement, rising 0.6% m/m and 4.3% y/y. It is clear the Delta variant and ongoing supply shortages have taken some steam out of the recovery. Still, the large jump in wages suggests the economy's issues are primarily supply-side driven. While August's job gain figure represents a significant drop in momentum in the labor market recovery, we do not believe this will derail the Fed's plans to taper by the end of the year. In terms of the U.S. federal budget, more questions remain as House Democrats passed the \$3.5 trillion budget resolution. Now, it remains within the Senate where there is strong sentiment for a smaller bill. House Speaker Nancy Pelosi committed to holding a vote on the infrastructure bill by September 27th. This should allow for both wings of the Democratic Party to agree on the contents of the reconciliation bill, which will likely be smaller than the \$3.5 trillion proposed. Once this is complete, then the end of September could, surprisingly, see the passage of the infrastructure bill, the reconciliation bill and an increase in the debt ceiling. With this backdrop, Treasury bill yields were relatively unchanged. The three-month Treasury bill yield ended the month at 0.04%, and the 12-month Treasury bill yield ended at 0.06%.

## **Outlook**

The Delta variant continues to pose a risk to the recovery. While uncertainty has increased, it is unlikely to derail the recovery. In his Jackson Hole speech, Fed Chairman Jerome Powell gave some fairly clear signals on how and when the Fed expects to taper bond purchases and begin to raise short-term interest rates. When the Fed begins to taper purchases, it is beginning to look more likely that they will reduce them by \$15 billion per month, \$10 billion from Treasuries and \$5 billion from mortgage backed securities, reducing the total monthly pace of accumulation from \$120 billion in November 2021 to zero by July 2022. This would allow the Fed to take some time following the end of asset purchases before considering raising the federal funds rate, which they may want to do by the end of 2022, but will likely do in the beginning of 2023. Finally, it is now looking more likely that the Fed will make their tapering announcement in November rather than September. The stated reasons for this seem reasonable: The Fed wants to see how the Delta variant is impacting the economy and whether it will wane in the weeks ahead. They also want to see further signs of progress in the labor market after federal enhanced unemployment benefits come to an end next week.

This information is an excerpt from an economic report dated August 2021 provided to TexSTAR by JP Morgan Asset Management, Inc., the investment manager of the TexSTAR pool.



## TEXSTAR BOARD MEMBERS

Monte Mercer	North Central TX Council of Government	Governing Board President
David Pate	Richardson ISD	Governing Board Vice President
Anita Cothran	City of Frisco	Governing Board Treasurer
David Medanich	Hilltop Securities	Governing Board Secretary
Jennifer Novak	J.P. Morgan Asset Management	Governing Board Asst. Sec./Treas
Brett Starr	City of Irving	Advisory Board
James Mauldin	DFW Airport/Non-Participant	Advisory Board
Sandra Newby	Tarrant Regional Water Dist/Non-Participant	Advisory Board
Eric Cannon	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 may change at any time based on market or other conditions and may not come to pass. While we believe the information presented is reliable, we cannot guarantee its accuracy. HilltopSecurities is a wholly owned subsidiary of Hilltop Holdings, Inc. (NYSE: HTH) located at 717 N. Hardwood Street, Suite 3400, Dallas, TX 75201, (214) 859-1800. Member NYSE/FINRA/SIPC. Past performance is no guarantee of future results. Investment Management Services are offered through J.P. Morgan Asset Management Inc. and/or its affiliates. Marketing and Enrollment duties are offered through HilltopSecurities and/or its affiliates. HilltopSecurities and J.P. Morgan Asset Management Inc. are separate entities.







CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
**AGENDA ITEM #8**

---

Discuss and consider authorizing the Issuance, Sale, and Delivery of Central Texas Regional Mobility Authority Senior Lien Revenue Refunding Bonds in accordance with Specified Parameters

Strategic Plan Relevance: Regional Mobility  
Department: Finance  
Contact: Bill Chapman, Chief Financial Officer  
Associated Costs: N/A  
Action Requested: Consider and act on the draft resolution

**Background:** The Mobility Authority is authorized to issue revenue bonds, notes, certificates or other obligations for the purposes of (i) financing and refinancing all or a portion of the cost of the acquisition, construction, improvement, extension or expansion of one or more turnpike projects (as defined in the Act), (ii) refunding, defeasing and redeeming any such obligations previously issued by the Authority and (iii) paying the expenses of issuing such revenue bonds, notes, certificates or other obligations.

Low current interest rates give the Mobility Authority an opportunity to refund certain existing Bonds to reduce financing costs.

**2021 Senior Lien Refunding Bonds:** Senior Lien Revenue Refunding Bonds, Series 2021D and Senior Lien Revenue Refunding Bonds, Taxable Series 2021E (collectively the “2021 Senior Lien Bonds”) will be issued to (i) refund all or a portion of the Senior Lien Revenue Refunding Bonds, Series 2016 (the “Series 2016 Refunded Bonds”) and Senior Lien Revenue Bonds, Series 2015A (the “Series 2015A Refunded Bonds”), (ii) make required deposits, if any, to the senior lien reserve fund, and (iii) pay the costs of issuance for the 2021 Senior Lien Bonds.

**Parameters Resolution:** The parameters resolution authorizes the issuance of the 2021 Obligations and authorizes the Board’s designated Authorized Officer (Chairman, Executive Director, or Chief Financial Officer) to act on behalf of the Board to determine the final terms and conditions of the 2021 Obligations, to authorize and approve the forms of a preliminary official statement and a final official statement, and authorize and





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

RESOLUTION NO. 21-0XX

RESOLUTION AUTHORIZING THE ISSUANCE, SALE AND DELIVERY OF CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY SENIOR LIEN REVENUE REFUNDING BONDS (THE “2021 OBLIGATIONS”), IN ACCORDANCE WITH SPECIFIED PARAMETERS; APPROVING THE FORM OF, AND AUTHORIZING THE EXECUTION AND DELIVERY OF, ONE OR MORE SENIOR LIEN SUPPLEMENTAL TRUST INDENTURES; APPOINTING AN AUTHORIZED OFFICER TO AUTHORIZE, APPROVE AND DETERMINE CERTAIN TERMS AND PROVISIONS OF THE 2021 OBLIGATIONS AND THE FORM OF EACH OF THE 2021 OBLIGATIONS; APPROVING AND AUTHORIZING THE TERMS AND CONDITIONS OF ONE OR MORE PURCHASE CONTRACTS PERTAINING TO THE 2021 OBLIGATIONS AND THE EXECUTION AND DELIVERY OF SUCH PURCHASE CONTRACTS; APPROVING THE PREPARATION OF ONE OR MORE PRELIMINARY OFFICIAL STATEMENTS AND OFFICIAL STATEMENTS IN CONNECTION WITH THE OFFERING AND SALE OF THE 2021 OBLIGATIONS; AUTHORIZING THE EXECUTION AND DELIVERY OF ANY AND ALL DOCUMENTS, CERTIFICATES, AGREEMENTS, CLOSING INSTRUCTIONS, AND INSTRUMENTS NECESSARY OR DESIRABLE TO BE EXECUTED AND DELIVERED IN CONNECTION WITH THE FOREGOING AND ENACTING OTHER PROVISIONS RELATING TO THE SUBJECT;

WHEREAS, the Central Texas Regional Mobility Authority (the “Authority”) has been created and organized pursuant to and in accordance with the provisions of Chapter 361, Texas Transportation Code, and operates pursuant to the Constitution and laws of the State, including, particularly, Chapter 370, Texas Transportation Code (the “Act”), for the purposes of constructing, maintaining and operating transportation projects, including turnpike projects, in Travis and Williamson Counties, Texas; and

WHEREAS, pursuant to the Act, the Authority is authorized to: (i) study, evaluate, design, finance, acquire, construct, maintain, repair and operate transportation projects (as defined in the Act), individually or as a system (as defined in the Act); (ii) issue bonds, certificates, notes or other obligations payable from the revenues of a transportation project or system, including tolls, fees, fares or other charges, to pay all or part of the cost of a transportation project and to refund any bonds previously issued for a transportation project; and (iii) impose tolls, fees, fares or other charges for the use of each of its transportation projects and the different parts or sections of each of its transportation projects; and

WHEREAS, pursuant to the Act and other applicable laws, the Authority is authorized to issue revenue bonds, notes, certificates or other obligations for the purposes of (i) financing and refinancing all or a portion of the cost of the acquisition, construction, improvement, extension or expansion of one or more turnpike projects (as defined in the Act), (ii) refunding, defeasing and

redeeming any such obligations previously issued by the Authority and (iii) paying the expenses of issuing such revenue bonds, notes, certificates or other obligations; and

WHEREAS, the Authority has previously executed and delivered that certain Master Trust Indenture (the “Master Indenture”), between the Authority and Regions Bank, as successor in trust to JPMorgan Chase Bank, National Association, as trustee (the “Trustee”), providing for the issuance from time to time by the Authority of one or more series of its revenue obligations (collectively, the “Obligations”) (the Master Indenture, as previously supplemented and amended is referred to herein as the “Indenture”); and

WHEREAS, Sections 301, 302, 706 and 1002 of the Master Indenture authorize the Authority and the Trustee to execute and deliver supplemental indentures authorizing the issuance of Obligations, including Additional Senior Lien Obligations, and to include in such supplemental indentures the terms of such Additional Senior Lien Obligations and any other matters and things relative to the issuance of such Obligations that are not inconsistent with or in conflict with the Indenture, to add to the covenants of the Authority, and to pledge other moneys, securities or funds as part of the Trust Estate; and

WHEREAS, pursuant to the Act, Chapter 1371, Texas Government Code, as amended, and Chapter 1207, Texas Government Code, as amended, the Board of Directors (the “Board”) of the Authority has determined to issue one or more series of Additional Senior Lien Obligations (collectively, the “2021 Obligations”) for the purposes specified herein pursuant to the Master Indenture and one or more Senior Lien Supplemental Trust Indentures (each, a “Senior Lien Supplement” and, collectively, the “Senior Lien Supplements”) between the Authority and the Trustee, each Senior Lien Supplement being dated as of the date specified in one or more Award Certificates (as hereinafter defined), all under and in accordance with the Constitution and the laws of the State; and

WHEREAS, the Board has determined to refund and redeem, with a portion of the proceeds of the 2021 Obligations, all or a portion of the Authority’s Outstanding Senior Lien Revenue Bonds, Series 2015A (the “2015A Refunded Bonds”), and all or a portion of the Authority’s Outstanding Senior Lien Revenue Refunding Bonds, Series 2016 (the “2016 Refunded Bonds”); and

WHEREAS, the Board has been presented with and examined proposed forms of a Senior Lien Supplement and an escrow agreement and the Board finds that the form and substance of such documents are satisfactory and the recitals and findings contained therein are true, correct and complete, and hereby adopts and incorporates by reference such recitals and findings as if set forth in full in this Resolution, and finds that it is in the best interest of the public and the Authority to issue the 2021 Obligations and to authorize the execution and delivery of one or more of each such documents as provided herein; and

WHEREAS, the Board now desires to appoint one or more officers of the Authority to act on behalf of the Authority to determine the final terms and conditions of the 2021 Obligations, as provided herein, and to make such determinations and findings as may be required by the Senior Lien Supplements, and to carry out the purposes of this Resolution and execute one or more Award

Certificates setting forth such determinations and authorizing and approving all other matters relating to the issuance, sale and delivery of the 2021 Obligations; and

WHEREAS, the Board desires to authorize the execution and delivery of one or more Senior Lien Supplements providing for the issuance of and setting forth the terms and provisions relating to the 2021 Obligations and the pledge and security therefor; and

WHEREAS, the 2021 Obligations shall be issued as Additional Senior Obligations and Long-Term Obligations pursuant to and in accordance with the provisions of the Master Indenture and one or more Senior Lien Supplements; and

WHEREAS, the Board desires to approve, ratify and confirm the preparation and distribution of one or more preliminary official statements and one or more official statements relating to the offering and sale of the 2021 Obligations; and

WHEREAS, the Board desires to provide for the issuance of the 2021 Obligations in accordance with the requirements of the Master Indenture and the Senior Lien Supplements and to authorize the execution and delivery of the 2021 Obligations and such certificates, agreements, instruction letters and other instruments as may be necessary or desirable in connection therewith; and

WHEREAS, the Board desires to authorize the execution and delivery of one or more Purchase Contracts (the "Purchase Contracts" or "Purchase Contract" as applicable), between the Authority and the underwriters named therein relating to the 2021 Obligations, as determined by the Authorized Officer (as hereinafter defined) in an Award Certificate relating thereto;

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF DIRECTORS OF THE CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY THAT:

## ARTICLE I

### FINDINGS AND DETERMINATIONS

Section 1.1. Findings and Determinations. (a) The findings and determinations set forth in the preamble hereof are hereby incorporated herein for all purposes as though such findings and determinations were set forth in full herein. Capitalized terms used herein and not otherwise defined herein shall have the meanings assigned thereto in the Master Indenture and the Senior Lien Supplements.

(b) The Board has found and determined that the 2021 Obligations may be issued as one or more series of Additional Senior Lien Obligations, as designated by the Authorized Officer in one or more Award Certificates (the "Award Certificates" or "Award Certificate," as applicable), and as Long-Term Obligations.

(c) It is officially found, determined and declared that the meeting at which this Resolution has been adopted was open to the public and public notice of the time, place and subject matter of the public business to be considered and acted upon at said meeting, including this

Resolution was given, all as required by the applicable provisions of Chapter 551, Texas Government Code, as amended.

(d) The Board hereby finds and determines that the issuance of the 2021 Obligations is in the best interest of the Authority.

## ARTICLE II

### ISSUANCE OF 2021 OBLIGATIONS; APPROVAL OF DOCUMENTS

Section 2.1. Issuance, Execution and Delivery of 2021 Obligations; Approval of Senior Lien Supplement. The Authority hereby authorizes, approves and directs the issuance of the 2021 Obligations in accordance with the terms of this Resolution, the Master Indenture and one or more Senior Lien Supplements, a draft of which was presented to the Authority and its counsel, the form, terms and provisions of such Senior Lien Supplement being hereby authorized and approved with such changes as may be approved by the Authorized Officer, such approval to be evidenced by the execution thereof. The Authorized Officer is hereby authorized to execute each such Senior Lien Supplement and the Secretary of the Board is hereby authorized to attest the signature of the Authorized Officer. Each Senior Lien Supplement shall have such supplement number as shall be deemed appropriate by the Authorized Officer and may include such terms and provisions as are necessary or desirable to reflect the final terms and conditions of the 2021 Obligations.

Section 2.2. The Issuance of the 2021 Obligations. The issuance, execution and delivery of the 2021 Obligations, which shall be issued in the aggregate principal amounts, in one or more series of Additional Senior Lien Obligations and bearing interest in accordance with the terms of the applicable Senior Lien Supplement, all as determined by the Authorized Officer and set forth in one or more Award Certificates, to provide funds to (i) refund all or a portion of the 2015A Refunded Bonds, (ii) refund all or a portion of the 2016 Refunded Bonds, (iii) make any necessary deposits to a reserve fund, and (iv) pay the costs of issuance for the 2021 Obligations, all pursuant to and in accordance with the Master Indenture and the applicable Senior Lien Supplement, are hereby authorized and approved.

## ARTICLE III

### APPOINTMENT OF AUTHORIZED OFFICER; DELEGATION OF AUTHORITY

Section 3.1. Appointment of Authorized Officer. The Board hereby appoints the Chairman of the Board, the Executive Director and the Chief Financial Officer, and any person serving in an interim capacity for any such position, severally and each of them, to act as an authorized officer (the "Authorized Officer") on behalf of the Board and to perform all acts authorized and required of an Authorized Officer set forth in this Resolution and each Senior Lien Supplement. The Authorized Officer is hereby authorized and directed to execute one or more Award Certificates setting forth the information authorized to be stated therein pursuant to this Resolution and required to be stated therein pursuant to each Senior Lien Supplement.

Section 3.2. Delegation of Authority. (a) The Board hereby authorizes and directs that the Authorized Officer act on behalf of the Authority to determine the final terms and conditions of the 2021 Obligations, the supplement number and dated date for each Senior Lien Supplement, the dated dates for the 2021 Obligations, the method of sale for the 2021 Obligations, the prices at which the 2021 Obligations will be sold, any different or additional designation or title of each series of the 2021 Obligations, the principal amounts and maturity dates therefor, the per annum interest rates for the 2021 Obligations (including whether such interest rates will be variable or fixed rates), the aggregate principal amount of 2021 Obligations to be issued, the respective aggregate principal amounts of each series of 2021 Obligations, the redemption provisions, dates and prices for the 2021 Obligations, the final forms of the 2021 Obligations, to determine whether each respective series of 2021 Obligations will be issued as taxable bonds or tax-exempt bonds and such other terms and provisions that shall be applicable to the 2021 Obligations, to select the 2015A Refunded Bonds and 2016 Refunded Bonds to be refunded, to make such determinations as may be necessary or desirable to calculate the redemption prices of the 2015A Refunded Bonds and the 2016 Refunded Bonds in accordance with the supplemental indentures and award certificates relating thereto, to designate one or more escrow agents in connection therewith, to approve the form and substance of an escrow agreement in connection therewith, to designate the underwriters of the 2021 Obligations, to approve the form and substance of one or more Purchase Contracts providing for the sale of the 2021 Obligations, to authorize and approve the form of one or more preliminary official statements and one or more final official statements and to make such findings and determinations as are otherwise authorized herein or as may be required by each Senior Lien Supplement to carry out the purposes of this Resolution and to execute one or more Award Certificates setting forth such determinations, such other matters as authorized herein, and authorizing and approving all other matters relating to the issuance, sale and delivery of the 2021 Obligations; provided, that the following conditions can be satisfied:

- (i) the aggregate principal amount of the 2021 Obligations to be issued shall not exceed \$720,000,000; and
- (ii) each series of 2021 Obligations shall not bear interest at a true interest rate greater than 5.00%; and
- (iii) each series of 2021 Obligations shall mature not later than January 1, 2046; and
- (iv) the refunding of the 2015A Refunded Bonds shall result in a net present value savings of not less than 7.00% of the principal amount of the 2015A Refunded Bonds being refunded; and
- (v) the refunding of the 2016 Refunded Bonds shall result in a net present value savings of not less than 7.00% of the principal amount of the 2016 Refunded Bonds being refunded.

all based on bond market conditions and available rates for the 2021 Obligations on the date of sale of the 2021 Obligations and on the terms, conditions and provisions negotiated by the Authority for the issuance, sale and delivery of 2021 Obligations.

(b) The 2021 Obligations may be issued as one or more series of Senior Lien Obligations, all as specified in the Award Certificates.

Section 3.3. Limitation on Delegation of Authority. The authority granted to the Authorized Officer under Article III of this Resolution shall expire at 5:00 p.m. Central Time on September 28, 2022, unless otherwise extended by the Board by separate Resolution. Any 2021 Obligations, with respect to which an Award Certificate is executed prior to 5:00 p.m. Central Time on September 28, 2022, may be delivered to the initial purchaser(s) thereof after such date.

## ARTICLE IV

### APPROVAL OF SALE OF 2020 OBLIGATIONS

Section 4.1. Approval of Sale of 2021 Obligations. The sale of the 2021 Obligations in one or more series, in the aggregate principal amounts, bearing interest at the rates and at the prices set forth in one or more Purchase Contracts between the Authority and the underwriters named therein, all as determined by the Authorized Officer on the date of sale of the 2021 Obligations, is hereby authorized and approved. The Authorized Officer is hereby authorized and directed to execute and deliver such Purchase Contracts on behalf of the Authority providing for the sale of the 2021 Obligations in such form as determined by the Authorized Officer, to be dated as of the date of its execution and delivery by the Authority and the underwriters named therein. The Authorized Officer is hereby authorized and directed to approve the final terms and provisions of such Purchase Contracts and to approve and to execute and deliver such Purchase Contracts on behalf of the Authority, such approval to be conclusively evidenced by the execution thereof.

Section 4.2. Sale on Best Terms Available. The 2021 Obligations shall be sold at the prices, bearing interest at the rates and having such other terms and provisions, that, based on then current market conditions, result in the best terms reasonably available and advantageous to the Authority, as is determined by the Authorized Officer on the date of sale of each series of the 2021 Obligations. The Authorized Officer is hereby authorized and directed to make such findings and determinations in the Award Certificates regarding the terms of the sale of the 2021 Obligations and the benefit of such sale to the Authority.

## ARTICLE V

### APPROVAL OF ESCROW AGREEMENT; NOTICE OF REDEMPTION

Section 5.1. Approval of Escrow Agreement. To provide for the security and investment of a portion of the proceeds of the 2021 Obligations until such time as such proceeds are to be paid to the registered owners of the 2015A Refunded Bonds and 2016 Refunded Bonds, respectively, the Authority hereby approves the form and substance of an escrow deposit agreement, substantially in the form of the Escrow Agreement (the "Escrow Agreement"), between the Authority and Regions Bank, as escrow agent (the "Escrow Agent"), dated as of the date set forth in an Award Certificate, a draft of which was presented to the Board and its counsel, the form, terms and provisions of such Escrow Agreement being hereby authorized and approved. The Authorized Officer is hereby authorized and directed to execute and deliver one or more Escrow Agreements, as determined by the Authorized Officer, in the name and on behalf of the Authority,

with such changes therein as the Authorized Officer may approve, such approval to be conclusively evidenced by such Authorized Officer's execution thereof.

Section 5.2. Notice of Redemption to Owners of Refunded Bonds. The Board hereby authorizes and calls for the redemption of the 2015A Refunded Bonds and 2016 Refunded Bonds, respectively, to be refunded on the dates and at the prices determined by the Authorized Officer and set forth in an Award Certificate. The Authorized Officer shall cause notice of redemption to be given to the registered owners of such 2015A Refunded Bonds and 2016 Refunded Bonds, respectively, in accordance with the Master Indenture and the supplemental trust indenture to which such 2015A Refunded Bonds and 2016 Refunded Bonds, respectively, were issued.

## ARTICLE VI

### APPROVAL OF OFFICIAL STATEMENT

Section 6.1. Approval of Official Statement. The Authorized Officer is hereby authorized and directed to authorize and approve the form and substance of one or more Preliminary Official Statements prepared in connection with the public offering of the 2021 Obligations, together with any addenda, supplement or amendment thereto (the "Preliminary Official Statement"), and the preparation, use and distribution of such Preliminary Official Statements in the marketing of the 2021 Obligations. The Authorized Officer is authorized to "deem final" each Preliminary Official Statement as of its date (except for the omission of pricing and related information) within the meaning and for the purposes of paragraph (b)(1) of Rule 15c2-12 under the Securities Exchange Act of 1934, as amended. The Authorized Officer is hereby further authorized and directed to use and distribute or authorize the use and distribution of, one or more final official statements and any addenda, supplement or amendment thereto (the "Official Statement"). The use thereof in the public offering and sale of the 2021 Obligations is hereby authorized and approved. The Chairman of the Board is hereby authorized and directed to execute and the Authorized Officer to deliver each Official Statement in accordance with the terms of the Purchase Contracts. The Secretary of the Board is hereby authorized and directed to include and maintain copies of each Preliminary Official Statement and each Official Statement in the permanent records of the Authority.

## ARTICLE VII

### USE AND APPLICATION OF PROCEEDS; LETTERS OF INSTRUCTION; POWER TO REVISE DOCUMENTS

Section 7.1. Use and Application of Proceeds; Letters of Instruction. The proceeds from the sale of the 2021 Obligations shall be used for the respective purposes set forth in and in accordance with the terms and provisions of the related Senior Lien Supplement and the related Award Certificate. The deposit and application of the proceeds from the sale of the 2021 Obligations shall be set forth in Letters of Instruction of the Authority executed by the Authorized Officer.



Section 7.2. Execution and Delivery of Other Documents. The Authorized Officer is hereby authorized and directed to execute and deliver from time to time and on an ongoing basis such other documents and agreements, including amendments, modifications, supplements or consents to existing agreements (including any agreements with the Texas Department of Transportation and the United States Department of Transportation), assignments, certificates, instruments, releases, financing statements, written requests, filings with the Internal Revenue Service and letters of instruction, whether or not mentioned herein, as may be necessary or convenient to carry out or assist in carrying out the purposes of this Resolution and to comply with the requirements of the Indenture, any Senior Lien Supplement, the Award Certificates and the Purchase Contracts.

Section 7.3. Power to Revise Form of Documents. Notwithstanding any other provision of this Resolution, the Authorized Officer is hereby authorized to make or approve such revisions in the form of the documents presented at this meeting and any other document, certificate or agreement pertaining to the issuance and delivery of the 2021 Obligations in accordance with the terms of the Master Indenture and any Senior Lien Supplement as, in the judgment of such person, may be necessary or convenient to carry out or assist in carrying out the purposes of this Resolution, such approval to be evidenced by the execution thereof.

## ARTICLE VIII

### APPROVAL AND RATIFICATION OF CERTAIN ACTIONS

Section 8.1. Approval of Submission to the Attorney General of Texas. The Authority's Bond Counsel is hereby authorized and directed to submit to the Attorney General, for his approval, transcripts of the legal proceedings relating to the issuance, sale and delivery of the 2021 Obligations as required by law, and to the Comptroller of Public Accounts of the State of Texas for registration. In connection with the submission of the records of proceedings for the 2021 Obligations to the Attorney General of the State of Texas for examination and approval of such 2021 Obligations, the Authorized Officer is hereby authorized and directed to issue one or more checks of the Authority payable to, or make one or more wire transfers to, the Attorney General of the State of Texas as a nonrefundable examination fee in the amount required by Chapter 1202, Texas Government Code. The initial 2021 Obligations shall be delivered to the Trustee for delivery to the underwriters thereof against payment therefor and upon satisfaction of the requirements of the Indenture, the related Senior Lien Supplement, as applicable, and the Purchase Contracts relating thereto.

Section 8.2. Certification of the Minutes and Records. The Secretary and any Assistant Secretary of the Board are each hereby severally authorized to certify and authenticate minutes and other records on behalf of the Authority for the issuance of the 2021 Obligations and for all other Authority activities.

Section 8.3. Ratifying Other Actions. All other actions taken or to be taken by the Executive Director, the Chief Financial Officer, the Authorized Officer, the Controller (and any person serving in an interim capacity for any such positions) and the Authority's staff in connection with the issuance of the 2021 Obligations are hereby approved, ratified and confirmed.

Section 8.4. Authority to Invest Funds. The Executive Director, the Chief Financial Officer and the Controller (and any person serving in an interim capacity for any such positions) are each hereby severally authorized on an ongoing basis to undertake all appropriate actions and to execute such documents, agreements or instruments as they deem necessary or desirable under the Indenture and the related Senior Lien Supplement, as applicable, with respect to the investment of proceeds of the 2021 Obligations and other funds of the Authority.

Section 8.5. Federal Tax Considerations. In addition to any other authority provided under this Resolution, each Authorized Officer is hereby further expressly authorized, acting for and on behalf of the Authority, to determine and designate in the Award Certificate for each series of 2021 Obligations whether such bonds will be issued as taxable bonds or tax-exempt bonds for federal income tax purposes and to make all appropriate elections under the Internal Revenue Code of 1986, as amended. Each Authorized Officer is hereby further expressly authorized and empowered from time to time and at any time to perform all such acts and things deemed necessary or desirable and to execute and deliver any agreements, certificates, documents or other instruments, whether or not herein mentioned, to carry out the terms and provisions of this section, including but not limited to, the preparation and making of any filings with the Internal Revenue Service.

## ARTICLE IX

### GENERAL PROVISIONS

Section 9.1. Changes to Resolution. The Executive Director, the Chief Financial Officer and the Authorized Officer, and any of them, singly and individually, are hereby authorized to make such changes to the text of this Resolution as may be necessary or desirable to carry out the purposes hereof or to comply with the requirements of the Attorney General of Texas in connection with the issuance of the 2021 Obligations herein authorized.

Section 9.2. Effective Date. This Resolution shall be in full force and effect from and upon its adoption.

Adopted, passed and approved by the Board of Directors of the Central Texas Regional Mobility Authority on the 29th day of September, 2021.

Submitted and reviewed by:

Approved:

---

Geoffrey Petrov, General Counsel

---

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

---

[\_\_\_\_\_]¹ SUPPLEMENTAL TRUST INDENTURE

BETWEEN

CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY

AND

REGIONS BANK, TRUSTEE

AUTHORIZING

SENIOR LIEN REVENUE REFUNDING BONDS, SERIES 2021D

AND

SENIOR LIEN REVENUE REFUNDING BONDS, TAXABLE SERIES 2021E

Dated as of October 1, 2021

---

¹ Supplement number to be determined by Authorized Officer

**TABLE OF CONTENTS**

Page

**ARTICLE I.  
DEFINITIONS AND STATUTORY AUTHORITY**

Section 1.1.	Supplemental Indenture .....	3
Section 1.2.	Definitions.....	3
Section 1.3.	Authority for This Supplemental Indenture .....	7
Section 1.4.	Rules of Construction.....	7
Section 1.5.	Interpretation .....	7
Section 1.6.	Indenture to Remain in Force.....	7
Section 1.7.	Successors and Assigns.....	7
Section 1.8.	Separability Clause.....	7
Section 1.9.	Benefits of Supplemental Indenture.....	7
Section 1.10.	Governing Law.....	8
Section 1.11.	Miscellaneous.....	8

**ARTICLE II.  
AUTHORIZATION AND TERMS OF 2021 SENIOR LIEN BONDS**

Section 2.1.	Authorization, Principal Amounts, Designation of Series, Terms and Provisions to Apply.....	8
Section 2.2.	Purposes .....	9
Section 2.3.	Pledge; Limited Obligations .....	9
Section 2.4.	Date, Denomination, Numbers, and Letters.....	10
Section 2.5.	Interest Payment Dates, Interest Rates and Maturity Dates of the 2021 Senior Lien Bonds.....	10
Section 2.6.	Paying Agent; Method and Place of Payment.....	10
Section 2.7.	Securities Depository; Book-Entry System .....	11
Section 2.8.	Redemption Prices and Terms .....	12
Section 2.9.	Selection of Bonds to be Redeemed; Notice of Redemption.....	12

**ARTICLE III.  
ACCOUNTS; APPLICATION OF PROCEEDS**

Section 3.1.	Debt Service Account 2021D Senior Lien.....	13
Section 3.2.	Debt Service Account 2021E Senior Lien .....	13
Section 3.3.	Bond Proceeds Clearance Fund; Costs of Issuance Fund; Initial Deposits.....	13
Section 3.4.	Senior Lien Debt Service Reserve Requirement.....	14
Section 3.5.	2005 TxDOT Grant Fund.....	14

**ARTICLE IV.  
FORMS OF BONDS**

Section 4.1.	Forms of 2021 Senior Lien Bonds .....	15
Section 4.2.	Initial 2021 Senior Lien Bonds .....	15
Section 4.3.	Additional Provisions Regarding Bonds.....	15

**ARTICLE V.  
TAX MATTERS; REBATE**

Section 5.1.	Federal Income Tax Matters Relating to Series 2021D Bonds.....	15
Section 5.2.	2021D Senior Lien Rebate Account .....	17

**ARTICLE VI.  
CONTINUING DISCLOSURE**

Section 6.1.	Definitions.....	18
Section 6.2.	Annual Reports .....	19
Section 6.3.	Event Notices .....	19
Section 6.4.	Limitations, Disclaimers and Amendments .....	21

**ARTICLE VII.  
OTHER MATTERS**

Section 7.1.	Execution in Several Counterparts.....	22
Section 7.2.	Confirmation of Funds and Accounts .....	22
Section 7.3.	Compliance with Texas Government Code .....	22

Exhibit A	-	Continuing Disclosure
-----------	---	-----------------------

[ \_\_\_\_\_ ] **SUPPLEMENTAL TRUST INDENTURE**

THIS [ \_\_\_\_\_ ] SUPPLEMENTAL TRUST INDENTURE, dated as of October 1, 2021 (this “Supplemental Indenture” or “[ \_\_\_\_\_ ] Supplemental Indenture”), is made by and between the CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY (together with any successor to its rights, duties, and obligations hereunder, the “Authority”), a body politic and corporate and a political subdivision of the State of Texas (the “State”) duly created, organized and existing under the laws of the State, and REGIONS BANK, an Alabama state banking corporation, as successor in trust to JPMorgan Chase Bank, National Association, as trustee (together with any successor trustee hereunder, the “Trustee”). Capitalized terms used herein and not otherwise defined shall have the meanings provided in Section 1.2 of this Supplemental Indenture.

RECITALS

WHEREAS, the Authority has been created and organized pursuant to and in accordance with the provisions of Chapter 361, Texas Transportation Code, and operates pursuant to the Constitution and laws of the State, including, particularly, Chapter 370, Texas Transportation Code, as amended (the “Act”), for the purposes of constructing, maintaining and operating transportation projects in Travis and Williamson Counties, Texas; and

WHEREAS, pursuant to the Act, the Authority is authorized to: (i) study, evaluate, design, finance, acquire, construct, maintain, repair and operate transportation projects (as defined in the Act), individually or as a system (as defined in the Act); and (ii) issue bonds, certificates, notes or other obligations payable from the revenues of a transportation project or system, including tolls, fees, fares or other charges, to pay all or part of the cost of a transportation project and to refund any bonds previously issued for a transportation project; and (iii) impose tolls, fees, fares or other charges for the use of each of its transportation projects and the different parts or sections of each of its transportation projects; and

WHEREAS, pursuant to the Act and other applicable laws, the Authority is authorized to issue revenue bonds, notes, certificates or other obligations as hereinafter provided, and to enter into this Supplemental Indenture; and

WHEREAS, the Authority and the Trustee have executed and delivered the Master Indenture, providing for the issuance from time to time by the Authority of one or more series of its revenue obligations (collectively, the “Obligations”); and

WHEREAS, Section 1002 of the Master Indenture authorizes the Authority and the Trustee to execute and deliver a supplemental indenture, authorizing Obligations of a Series, to include any other matters and things relative to such Obligations which are not inconsistent with or contrary to the Master Indenture, to add to the covenants of the Authority, and to pledge other moneys, securities or funds as part of the Trust Estate; and

WHEREAS, pursuant to the authority granted in the Act, Chapter 1371, Texas Government Code, and Chapter 1207, Texas Government Code, the Authority has determined to authorize the issuance of its Senior Lien Revenue Refunding Bonds, Series 2021D (the “Series 2021D Bonds”), pursuant to the Master Indenture and this Supplemental Indenture for the purpose of providing funds (i) to refund all or a portion of the Authority’s Senior Lien Revenue Refunding Bonds, Series

2016, identified as being refunded in the Award Certificate relating to the Series 2021D Bonds (the “2016 Refunded Bonds”), and (ii) for the other purposes specified herein; and

WHEREAS, pursuant to the authority granted in the Act, Chapter 1371, Texas Government Code, and Chapter 1207, Texas Government Code, the Authority has determined to authorize the issuance of its Senior Lien Revenue Refunding Bonds, Taxable Series 2021E (the “Taxable Series 2021E Bonds” and, together with the Series 2021D Bonds, the “2021 Senior Lien Bonds”), pursuant to the Master Indenture and this Supplemental Indenture for the purpose of providing funds (i) to refund all or a portion of the Authority’s Senior Lien Revenue Bonds, Series 2015A, identified as being refunded in the Award Certificate relating to the Taxable Series 2021E Bonds (the “2015A Refunded Bonds” and, together with the 2016 Refunded Bonds, the “Refunded Obligations”), and (ii) for the other purposes specified herein; and

WHEREAS, the Authority is authorizing the refunding of the Refunded Obligations for the purpose of realizing a debt service savings through such refunding; and

WHEREAS, the Board hereby finds and determines that the issuance of the 2021 Senior Lien Bonds is in the best interests of the Authority; and

WHEREAS, pursuant to the Bond Resolution, the Authority has authorized the Authorized Officer to make such findings and determinations as may be required in connection with the issuance of the 2021 Senior Lien Bonds and the refunding of the Refunded Obligations and to set forth such findings and determinations in one or more Award Certificates; and

WHEREAS, the execution and delivery of this Supplemental Indenture and the issuance of the 2021 Senior Lien Bonds have been in all respects duly and validly authorized by the Bond Resolution; and

WHEREAS, the Trustee has accepted the trusts created by the Master Indenture and this Supplemental Indenture and in evidence thereof has joined in the execution and delivery hereof; and

WHEREAS, except as provided herein, all acts and conditions and things required by the laws of the State to happen, exist and be performed precedent to execution and delivery of this Supplemental Indenture have happened, exist and have been performed as so required in order to make the Indenture, as supplemented by this Supplemental Indenture, a valid, binding and legal instrument for the security of the 2021 Senior Lien Bonds and a valid and binding agreement in accordance with its terms;

NOW, THEREFORE, in consideration of the premises, the acceptance by the Trustee of the trusts hereby created, the purchase and acceptance of the 2021 Senior Lien Bonds by the holders thereof, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and for the further purpose of fixing and declaring the terms and conditions upon which the 2021 Senior Lien Bonds are to be issued, authenticated, delivered and accepted by the holders thereof, the Authority and the Trustee do hereby mutually covenant and agree, for the equal and proportionate benefit of the respective Holders from time to time of the Obligations, including the 2021 Senior Lien Bonds, as follows:



## ARTICLE I.

### DEFINITIONS AND STATUTORY AUTHORITY

Section 1.1. Supplemental Indenture. This Supplemental Indenture is supplemental to the Master Indenture and is adopted in accordance with Article III and Article X thereof.

Section 1.2. Definitions. Unless the context shall require otherwise, all defined terms contained in the Master Indenture shall have the same meanings in this Supplemental Indenture as such defined terms are given in Section 101 of the Master Indenture.

As used in this Supplemental Indenture, unless the context shall otherwise require, the following terms shall have the following respective meanings:

“Arbitrage Analyst” shall mean any nationally recognized firm of certified public accountants or any other nationally recognized firm or Person approved by the Authority and expert in the area of verification of arbitrage calculations related to tax-exempt bonds.

“Authorized Denomination” shall mean, with respect to 2021 Senior Lien Bonds, \$5,000 principal amount or any integral multiple thereof.

“Authorized Officer” shall mean the Chairman of the Board of Directors of the Authority, the Executive Director of the Authority and the Chief Financial Officer of the Authority, and any person serving in an interim capacity for any such positions, severally and each of them, as provided in the Bond Resolution.

“Award Certificate” means the Award Certificate executed and delivered by an Authorized Officer pursuant to Section 2.1 hereof in connection with initial issuance and delivery of the 2021 Senior Lien Bonds authorized to be issued hereunder.

“Bond Forms” shall mean, collectively, the substantially final forms of the Series 2021D Bond Form and the Taxable Series 2021E Bond Form, as applicable, attached to the Award Certificate, with such changes and modifications as shall be appropriate to conform to the terms of the Award Certificate.

“Bond Proceeds Clearance Fund SR LIEN 2021D” shall mean the “Bond Proceeds Clearance Fund Senior Lien 2021D” established pursuant to Section 3.3(a) hereof, and any Accounts established therein pursuant to a Letter of Instructions signed by an Authorized Officer.

“Bond Proceeds Clearance Fund SR LIEN 2021E” shall mean the “Bond Proceeds Clearance Fund Senior Lien 2021E” established pursuant to Section 3.3(b) hereof, and any Accounts established therein pursuant to a Letter of Instructions signed by an Authorized Officer.

“Bond Proceeds Funded Account” shall mean the Account by that name established pursuant to the Twelfth Supplemental Indenture as part of the Senior Lien Debt Service Reserve Fund.

“Bond Resolution” shall mean Resolution No. 21-\_\_\_\_, adopted by the Board of Directors of the Authority on September 29, 2021.

“Bond Year” shall mean each one-year period that ends at the close of business on the day that is each anniversary of the Issuance Date and on the date of final maturity of the Series 2021D Bonds. The last Bond Year may be a short period.

“Code” shall mean the Internal Revenue Code of 1986, as amended, and, with respect to a specific section thereof, such reference shall be deemed to include (a) the Regulations promulgated under such section, (b) any successor provision of similar import hereafter enacted, (c) any corresponding provision of any subsequent Internal Revenue Code and (d) the regulations promulgated under the provisions described in (b) and (c).

“COI 2021D Fund SR LIEN” shall mean the “2021D Costs of Issuance Fund Senior Lien” established pursuant to Section 3.3(c) hereof.

“COI 2021E Fund SR LIEN” shall mean the “2021E Costs of Issuance Fund Senior Lien” established pursuant to Section 3.3(d) hereof.

“Computation Date” shall mean each Installment Computation Date and the Final Computation Date.

“Debt Service Account 2021D SR LIEN” shall mean the “Debt Service Account 2021D Senior Lien” established in Section 3.1(a) hereof as part of the Senior Lien Debt Service Fund and any subaccounts established therein pursuant to this Supplemental Indenture or a Letter of Instructions signed by an Authorized Officer.

“Debt Service Account 2021E SR LIEN” shall mean the “Debt Service Account 2021E Senior Lien” established in Section 3.2(a) hereof as part of the Senior Lien Debt Service Fund and any subaccounts established therein pursuant to this Supplemental Indenture or a Letter of Instructions signed by an Authorized Officer.

“Depository Participant” shall mean a broker, dealer, bank, other financial institution or any other Person for whom from time to time a Securities Depository effects book-entry transfers and pledges of securities deposited with such Securities Depository.

“Designated Payment/Transfer Office” shall mean, initially, the office of the Trustee located in Houston, Texas, or such other office designated by the Trustee from time to time as the place of payment and transfer of registration of ownership of the 2021 Senior Lien Bonds.

“DTC” shall mean The Depository Trust Company, its successors and assigns.

“Final Computation Date” shall mean the date on which the last bond of the Series 2021D Bonds is discharged.

“First Supplemental Indenture” shall mean the First Supplemental Trust Indenture, dated as of February 1, 2005, between the Authority and the Trustee.

“Indenture” shall mean the Master Indenture, as amended or supplemented (i) by each Supplemental Indenture (as defined in the Master Indenture) heretofore executed and delivered by the Authority and the Trustee in accordance with the terms of the Master Indenture, prior to the date of this [\_\_\_\_\_] Supplemental Indenture; (ii) by this [\_\_\_\_\_] Supplemental

Indenture; and (iii) hereafter from time to time in accordance with the terms of the Master Indenture.

“Initial 2021 Senior Lien Bonds” shall mean, collectively, the Initial Series 2021D Bonds and Initial Taxable Series 2021E Bonds, if any, as described in Section 2.4 hereof.

“Installment Computation Date” shall mean the last day of the fifth Bond Year and each succeeding fifth Bond Year.

“Interest Payment Date” shall mean, with respect to each Series of the 2021 Senior Lien Bonds, each July 1 and January 1, commencing on the date or dates specified in the Award Certificate.

“Issuance Date” shall mean the date of initial issuance and delivery of the 2021 Senior Lien Bonds to the Underwriters, or the representative thereof, against payment therefor.

“Letter of Representations” shall mean that certain Blanket Issuer Letter of Representations between the Authority and DTC, as the Securities Depository.

“Master Indenture” shall mean the Master Trust Indenture, dated as of February 1, 2005, between the Authority and the Trustee, without regard to supplements and amendments thereto.

“Official Statement” shall mean the Authority’s final official statement prepared in connection with the public offering and sale of the 2021 Senior Lien Bonds, together with any addenda, supplements and amendments thereto.

“Purchase Agreement” shall mean the Bond Purchase Agreement between the Authority and the respective Underwriters providing for the purchase of the 2021 Senior Lien Bonds by the Underwriters.

“Rebate Amount” shall mean that amount, as of each respective Computation Date, described in section 1.148-3(b) of the Regulations and generally means the excess as of any date of the future value of all receipts on nonpurpose investments over the future value of all payments on nonpurpose investments all as determined in accordance with section 1.148-3 of the Regulations.

“Record Date” shall mean with respect to the 2021 Senior Lien Bonds, the fifteenth (15th) calendar day of the month preceding each Interest Payment Date.

“Refunded Obligations” shall have the meaning given to such term in the recitals of this [\_\_\_\_\_] Supplemental Indenture.

“Regulations” shall mean the applicable proposed, temporary or final Treasury Regulations promulgated under the Code or, to the extent applicable to the Code, under the Internal Revenue Code of 1954, as such regulations may be amended or supplemented from time to time.

“Revenue Funded Account” shall mean the Account by that name established pursuant to the Twelfth Supplemental Indenture as part of the Senior Lien Debt Service Reserve Fund.

“Securities Depository” shall mean The Depository Trust Company, a limited purpose trust company organized under the laws of the State of New York, and any successor Securities Depository appointed pursuant to Section 913 of the Master Indenture and Section 2.6 of this Supplemental Indenture.

“Senior Lien Debt Service Reserve Requirement” shall mean an amount equal to the least of (i) the maximum Annual Debt Service on all Outstanding Senior Lien Obligations, (ii) 1.25 times the Average Annual Debt Service on all Outstanding Senior Lien Obligations, or (iii) ten percent (10%) of the aggregate amount of the Outstanding Senior Lien Obligations, as determined on the date each Series of Senior Lien Obligations is issued.

“Series 2021D Bonds” shall mean the Authority’s Senior Lien Revenue Refunding Bonds, Series 2021D authorized pursuant to this Supplemental Indenture and designated as such in the Award Certificate.

“Special Payment Date” shall mean the date that is fifteen (15) days after the Special Record Date.

“Special Record Date” shall mean the new record date for interest payment established in the event of a nonpayment of interest on a scheduled payment date, and for thirty (30) days thereafter.

“Springing Lien Account” shall have the meaning given to such term in the Twelfth Supplemental Indenture.

“Springing Lien Obligation” shall have the meaning given to such term in the Twelfth Supplemental Indenture.

“Stated Maturity” shall mean the date on which a 2021 Senior Lien Bond is scheduled to mature, as set forth in the Award Certificate.

“Supplemental Indenture” or “[\_\_\_\_\_] Supplemental Indenture” shall mean this [\_\_\_\_\_] Supplemental Trust Indenture by and between the Authority and the Trustee, dated as of the date first above written, together with any amendments hereto.

“Taxable Series 2021E Bonds” shall mean the Authority’s Senior Lien Revenue Refunding Bonds, Taxable Series 2021E authorized pursuant to this Supplemental Indenture and designated as such in the Award Certificate.

“Treasury” shall mean the United States Department of the Treasury, or any successor department or agency to the obligations thereof.

“Twelfth Supplemental Indenture” shall mean the Twelfth Supplemental Trust Indenture, dated as of November 1, 2015, between the Authority and the Trustee.

“2021 Senior Lien Bonds” shall mean, collectively, the Series 2021D Bonds and the Taxable Series 2021E Bonds.

“2021D Senior Lien Rebate Account” shall mean the account by that name established pursuant to Section 5.2 hereof and such subaccounts as may be established therein pursuant to a Letter of Instructions signed by an Authorized Officer.

“Underwriters” shall mean the underwriters named in the Purchase Agreement.

Section 1.3. Authority for This Supplemental Indenture. This Supplemental Indenture is adopted pursuant to the provisions of the Act and the Master Indenture, particularly Section 1002(a) of the Master Indenture.

Section 1.4. Rules of Construction.

(a) For all purposes of this Supplemental Indenture unless the context requires otherwise, all references to designated Articles, Sections and other subdivisions are to the articles, sections and other subdivisions of this Supplemental Indenture.

(b) Except where the context otherwise requires, terms defined in this Supplemental Indenture to impart the singular number shall be considered to include the plural number and vice versa.

(c) Unless the context requires otherwise, words of the masculine gender shall be construed to include correlative words of the feminine and neuter genders and vice versa.

(d) This Supplemental Indenture and all the terms and provisions hereof shall be liberally construed to effectuate the purposes set forth herein and to sustain the validity of this Supplemental Indenture and the Master Indenture which it supplements.

Section 1.5. Interpretation. The Table of Contents, titles and headings of the Articles and Sections of this Supplemental Indenture have been inserted for convenience of reference only and are not to be considered a part hereof and shall not in any way modify or restrict the terms or provisions hereof.

Section 1.6. Indenture to Remain in Force. Except as amended by this Supplemental Indenture, the Indenture shall remain in full force and effect as to the matters covered therein.

Section 1.7. Successors and Assigns. All covenants and agreements in this Supplemental Indenture by the Authority and the Trustee shall bind their respective successors and assigns, whether so expressed or not.

Section 1.8. Separability Clause. In case any provision in this Supplemental Indenture shall be determined to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.

Section 1.9. Benefits of Supplemental Indenture. Subject to the terms of the Master Indenture and the terms hereof, nothing in this Supplemental Indenture or in the 2021 Senior Lien Bonds, express or implied, shall give to any Person, other than the parties hereto, their successors hereunder, and the Holders of 2021 Senior Lien Bonds, any benefit or any legal or equitable right, remedy or claim under this Supplemental Indenture.

Section 1.10. Governing Law. This Supplemental Indenture shall be construed in accordance with and governed by the laws of the State.

Section 1.11. Miscellaneous. Every “request,” “order,” “demand,” “application,” “notice,” “statement,” “certificate,” “consent,” “instruction,” or similar action hereunder shall, unless the form thereof is specifically provided herein, be in writing, and in the case of the Authority signed by an Authorized Representative or Authorized Officer of the Authority or in the case of any other Person signed by its President or Vice President, or other officer serving in similar capacities specifically authorized to execute such writing on behalf of any other Person, as the case may be.

## ARTICLE II.

### AUTHORIZATION AND TERMS OF 2021 SENIOR LIEN BONDS

Section 2.1. Authorization, Principal Amounts, Designation of Series, Terms and Provisions to Apply.

(a) General. In accordance with and subject to the terms, conditions and limitations established in the Indenture and this Supplemental Indenture, (i) the Series 2021D Bonds are hereby authorized to be issued pursuant to and in accordance with the provisions of the Bond Resolution, the Master Indenture, Chapter 1207, Texas Government Code, as amended, Chapter 1371, Texas Government Code, as amended, and the Act, and (ii) the Taxable Series 2021E Bonds are hereby authorized to be issued pursuant to and in accordance with the provisions of the Bond Resolution, the Master Indenture, Chapter 1207, Texas Government Code, as amended, Chapter 1371, Texas Government Code, as amended, and the Act. The Authorized Officer shall determine the aggregate principal amount of the 2021 Senior Lien Bonds to be issued and the amount of each Series of the 2021 Senior Lien Bonds to be issued for each of the purposes identified in Section 2.2 of this Supplemental Indenture and shall make such findings as required by law, as authorized by the Bond Resolution or as otherwise deemed appropriate by the Authorized Officer, all of which shall be set forth in the Award Certificate. The terms of the 2021 Senior Lien Bonds shall be as set forth in the Master Indenture, this Supplemental Indenture and the Award Certificate. All terms and provisions of the Award Certificate relating to the 2021 Senior Lien Bonds shall be deemed to be incorporated into and shall become a part of this Supplemental Indenture.

(b) Series 2021D Bonds. The Authorized Officer shall determine and shall set forth in the Award Certificate the aggregate principal amount of Series 2021D Bonds to be issued, the Series designation thereof, the maturity dates, the per annum interest rates, the redemption provisions and any other terms and provisions determined by the Authorized Officer as necessary or desirable with respect to the terms of such Series 2021D Bonds.

(c) Taxable Series 2021E Bonds. The Authorized Officer shall determine and shall set forth in the Award Certificate the aggregate principal amount of Taxable Series 2021E Bonds to be issued, the Series designation thereof, the maturity dates, the per annum interest rates, the redemption provisions and any other terms and provisions determined by the Authorized Officer as necessary or desirable with respect to the terms of such Taxable Series 2021E Bonds.

Section 2.2. Purposes.

(a) The Series 2021D Bonds are issued in accordance with Section 302(b) of the Master Indenture for the purpose of providing funds to: (i) refund the 2016 Refunded Bonds; (ii) make required deposits, if any, to the Senior Lien Debt Service Reserve Fund; and (iii) pay certain costs of issuance for the Series 2021D Bonds, all under and in accordance with the Constitution and the laws of the State.

(b) The Taxable Series 2021E Bonds are issued in accordance with Section 302(b) of the Master Indenture for the purpose of providing funds to: (i) refund the 2015A Refunded Bonds; (ii) make required deposits, if any, to the Senior Lien Debt Service Reserve Fund; and (iii) pay certain costs of issuance for the Taxable Series 2021E Bonds, all under and in accordance with the Constitution and the laws of the State.

Section 2.3. Pledge; Limited Obligations.

(a) The 2021 Senior Lien Bonds are designated as Senior Lien Obligations, Long-Term Obligations and Refunding Obligations under the Master Indenture.

(b) The 2021 Senior Lien Bonds shall be limited obligations of the Authority constituting Senior Lien Obligations payable from and secured solely by a first lien on, pledge of and security interest in the Trust Estate. The 2021 Senior Lien Bonds, as Senior Lien Obligations, shall constitute a valid claim of the Holder thereof against the Trust Estate, which is pledged to secure the payment of the principal of, redemption premium, if any, and interest on the 2021 Senior Lien Bonds. The 2021 Senior Lien Bonds shall not constitute a general obligation of the Authority and under no circumstances shall the 2021 Senior Lien Bonds be payable from, nor shall the Holder thereof have any rightful claim to, any income, revenues, funds or assets of the Authority other than those pledged hereunder and under the Master Indenture as security for the payment of the Senior Lien Obligations.

NONE OF THE STATE OF TEXAS OR ANY OTHER AGENCY OR POLITICAL SUBDIVISION OF THE STATE OF TEXAS OTHER THAN THE AUTHORITY IS OBLIGATED TO PAY THE PRINCIPAL OF, PREMIUM, IF ANY, OR INTEREST ON THE 2021 SENIOR LIEN BONDS. THE 2021 SENIOR LIEN BONDS ARE PAYABLE SOLELY FROM THE TRUST ESTATE AND CERTAIN FUNDS CREATED UNDER THE INDENTURE. NEITHER THE FAITH AND CREDIT NOR THE TAXING POWER OF THE STATE OF TEXAS OR ANY POLITICAL SUBDIVISION THEREOF IS PLEDGED TO THE PAYMENT OF THE PRINCIPAL OF, PREMIUM, IF ANY, OR INTEREST ON THE 2021 SENIOR LIEN BONDS. THE AUTHORITY HAS NO TAXING POWER.

NO RECOURSE UNDER THE 2021 SENIOR LIEN BONDS SHALL BE HAD AGAINST ANY PAST, PRESENT OR FUTURE OFFICER OF THE AUTHORITY. THE 2021 SENIOR LIEN BONDS SHALL NEVER BE PAID IN WHOLE OR IN PART OUT OF ANY FUNDS RAISED OR TO BE RAISED BY TAXATION OR OUT OF ANY OTHER REVENUES OF THE AUTHORITY, EXCEPT THOSE REVENUES ASSIGNED BY THE INDENTURE.

By its purchase and acceptance of the 2021 Senior Lien Bonds, each holder thereof acknowledges that, the Authority has previously issued and there is currently outstanding, and the Authority has reserved the right pursuant to the Master Indenture to issue or incur in the future

Subordinate Lien Obligations that, upon the occurrence of an Event of Default described in Section 801(d) of the Master Indenture, will be deemed to be and will automatically become a Senior Lien Obligation in accordance with the provisions of the Supplemental Indenture (as defined in the Master Indenture) authorizing such Subordinate Lien Obligations.

Section 2.4. Date, Denomination, Numbers, and Letters.

(a) The 2021 Senior Lien Bonds shall be dated as provided in the Award Certificate and shall be issued in Authorized Denominations.

(b) Unless the Authority shall direct otherwise, each Series 2021D Bond shall be lettered and numbered separately from D-1 upward. The Series 2021D Bonds registered by the Comptroller of Public Accounts of the State of Texas (the “Initial Series 2021D Bonds”), if any, shall be lettered and numbered separately from DT-1 upward.

(c) Unless the Authority shall direct otherwise, each Taxable Series 2021E Bond shall be lettered and numbered separately from E-1 upward. The Taxable Series 2021E Bonds registered by the Comptroller of Public Accounts of the State of Texas (the “Initial Taxable Series 2021E Bonds”), if any, shall be numbered separately from ET-1 upward.

Section 2.5. Interest Payment Dates, Interest Rates and Maturity Dates of the 2021 Senior Lien Bonds.

(a) The 2021 Senior Lien Bonds shall bear interest from the later of their respective Issuance Date or the most recent Interest Payment Date to which interest has been paid or provided for until the principal of such 2021 Senior Lien Bonds has been paid or provided for either at Stated Maturity or the prior redemption thereof. Interest on the 2021 Senior Lien Bonds shall be calculated on the basis of a 360-day year composed of twelve 30-day months and shall be payable on each Interest Payment Date.

(b) The 2021 Senior Lien Bonds shall mature on January 1 in the years, in the respective principal amounts and shall bear interest at the per annum rates set forth in the Award Certificate.

Section 2.6. Paying Agent; Method and Place of Payment.

(a) The Trustee is hereby appointed as Paying Agent for the 2021 Senior Lien Bonds.

(b) The principal of the 2021 Senior Lien Bonds shall be payable on the due date thereof (whether at Stated Maturity or, if applicable, prior redemption date) upon the presentation and surrender thereof at the Designated Payment/Transfer Office.

(c) Interest payable on each 2021 Senior Lien Bonds shall be paid by check dated as of the Interest Payment Date and mailed by the Trustee to the Holder in whose name such 2021 Senior Lien Bonds is registered at the close of business on the Record Date, by mail, first class postage prepaid, to the address of the Holder as it appears in the registration books kept by the Trustee, or such other customary banking arrangements acceptable to the Trustee and the Person to whom interest is to be paid; provided, however, that such Person shall bear all risk and expenses of such other customary banking arrangements. In the event of nonpayment of interest on a



scheduled Interest Payment Date, and for 30 days thereafter, a new record date for such interest payment (defined in Section 1.2 hereof as a “Special Record Date”) will be established by the Trustee, if and when funds for the payment of such interest have been received from the Authority. Notice of the Special Record Date and of the scheduled payment date of the past due interest (defined in Section 1.2 hereof as the “Special Payment Date,” which shall be 15 days after the Special Record Date) shall be sent at least five Business Days prior to the Special Record Date by United States mail, first class postage prepaid, to the address of each Holder of a 2021 Senior Lien Bond appearing on the books of the Trustee at the close business on the last Business Day preceding the date of mailing of such notice.

Section 2.7. Securities Depository; Book-Entry System.

(a) Pursuant to Section 913 of the Master Indenture, the Authority hereby appoints The Depository Trust Company (“DTC”) as Securities Depository for the 2021 Senior Lien Bonds. In accordance with the Letter of Representations, the Authority shall cause the 2021 Senior Lien Bonds to be registered in the name of Cede & Co., as nominee for DTC, and to be delivered by the Underwriters to DTC on the Issuance Date.

(b) With respect to 2021 Senior Lien Bonds registered in the registration books maintained by the Trustee in the name of Cede & Co., or a nominee of any successor Securities Depository, pursuant to Section 913 of the Master Indenture, the Authority and the Trustee shall have no responsibility or obligation to any Depository Participant or to any Person on behalf of whom such Depository Participant holds an interest in 2021 Senior Lien Bonds. The Authority and the Trustee may treat and consider the Holder of any 2021 Senior Lien Bonds as the absolute owner of such 2021 Senior Lien Bonds for the purpose of payment of the principal of, premium, if any, and interest on such 2021 Senior Lien Bonds, for the purpose of giving notices of redemption and other matters with respect to such 2021 Senior Lien Bonds, for the purpose of registering transfers and exchanges with respect to such 2021 Senior Lien Bonds, and for all other purposes whatsoever. The Trustee shall pay the principal of, premium, if any, and interest on the 2021 Senior Lien Bonds only to or upon the order of the respective Holders of the 2021 Senior Lien Bonds and all such payments shall be valid and effective with respect to such payments to the extent of the sum or sums so paid. The Authority and the Trustee shall have no responsibility or obligation with respect to (i) the accuracy of the records of DTC, any successor Securities Depository or any Depository Participant with respect to any ownership interest in 2021 Senior Lien Bonds, (ii) the delivery to any Depository Participant or any other Person, other than a Holder of a 2021 Senior Lien Bonds as shown in the registration books for Obligations required to be kept and maintained pursuant to the Master Indenture, of any notice with respect to the 2021 Senior Lien Bonds, including any notice of redemption, or (iii) the payment to any Depository Participant or any other Person, other than a Holder of a 2021 Senior Lien Bonds, of any amount with respect to any 2021 Senior Lien Bonds. The rights of Depository Participants and Persons on behalf of whom any Depository Participant holds a beneficial interest in 2021 Senior Lien Bonds shall be limited to those established by law and agreements between such Depository Participants and other Persons and the applicable Securities Depository.

(c) In the event that either (i) the Securities Depository that is, directly or through a nominee, the Holder of all of the Outstanding 2021 Senior Lien Bonds of any Series notifies the Trustee and the Authority that it is no longer willing or able to discharge its responsibilities as a Securities Depository or (ii) the Authority determines that continuance of the existing book-entry

system for ownership of interests in the 2021 Senior Lien Bonds is not in the best interest of such owners of beneficial interests in the 2021 Senior Lien Bonds, then the Authority shall direct the Securities Depository to terminate the existing book-entry system for ownership of interests in the 2021 Senior Lien Bonds. Upon such termination, the Authority shall promptly select a substitute Securities Depository (and shall notify the Trustee in writing of such selection) to provide a system of book-entry ownership of beneficial interests in the 2021 Senior Lien Bonds, if one is available satisfactory to the Authority, and the ownership of all 2021 Senior Lien Bonds shall be transferred on the registration books for the 2021 Senior Lien Bonds to such successor Securities Depository, or its nominee. In the alternative, the Authority may direct the Trustee to, and if the Authority fails to promptly designate a successor Securities Depository the Trustee, without further direction, shall, notify the Depository Participants, through the Securities Depository for the 2021 Senior Lien Bonds, of the availability of 2021 Senior Lien Bonds registered in the names of such Persons as are owners of beneficial interests in the 2021 Senior Lien Bonds and, upon surrender to the Trustee of the Outstanding 2021 Senior Lien Bonds held by the Securities Depository, accompanied by registration instructions from the Securities Depository, the Trustee shall, at the expense of the transferees, cause to be printed and authenticated 2021 Senior Lien Bonds, in Authorized Denominations, to the owners of beneficial interests in the 2021 Senior Lien Bonds as of the date of the termination of the existing book-entry ownership system for the 2021 Senior Lien Bonds. Neither the Authority nor the Trustee shall be liable for any delay in delivery of such instructions and may conclusively rely on, and shall be protected in relying upon, such instructions. So long as the Authority has designated a Securities Depository to provide a system of book-entry ownership of the 2021 Senior Lien Bonds, all of the 2021 Senior Lien Bonds must be held under such book-entry system.

(d) Notwithstanding any other provisions in Article II hereof, the Authority and the Trustee may, but shall not be required to, enter into separate agreements with one or more Securities Depositories which may provide for alternative or additional provisions with respect to the delivery of notices, payment of interest and/or principal, or any other matters.

Section 2.8. Redemption Prices and Terms. The 2021 Senior Lien Bonds shall be subject to redemption prior to Stated Maturity only as provided in the Award Certificate for each Series of 2021 Senior Lien Bonds and in this Supplemental Indenture.

Section 2.9. Selection of Bonds to be Redeemed; Notice of Redemption.

(a) Unless otherwise specified herein, or in the Award Certificate, the terms and provisions of Article IV of the Master Indenture relating to the selection of Obligations for redemption and the giving of notice therefor shall apply to the 2021 Senior Lien Bonds. In addition, if the 2021 Senior Lien Bonds are registered in the name of the nominee of the Securities Depository, the Trustee shall deliver notice of such redemption to the Securities Depository at the times and in the manner required by the operational procedures of such Securities Depository in order to timely effect the redemption of such 2021 Senior Lien Bonds.

(b) Any notice mailed or transmitted as provided in this Section shall be conclusively presumed to have been duly given, whether or not the registered owner of such 2021 Senior Lien Bonds receives the notice.

## **ARTICLE III.**

### **ACCOUNTS; APPLICATION OF PROCEEDS**

#### **Section 3.1. Debt Service Account 2021D Senior Lien.**

(a) There is hereby established within the Senior Lien Debt Service Fund an account designated “Debt Service Account 2021D Senior Lien” (“Debt Service Account 2021D SR LIEN”). Moneys on deposit in the Debt Service Account 2021D SR LIEN shall be used to pay debt service on the Series 2021D Bonds when due.

(b) On or prior to each Interest Payment Date with respect to the Series 2021D Bonds, the Trustee shall deposit to the Debt Service Account 2021D SR LIEN from Revenues an amount sufficient to pay debt service then due on the Series 2021D Bonds.

#### **Section 3.2. Debt Service Account 2021E Senior Lien.**

(a) There is hereby established within the Senior Lien Debt Service Fund an account designated “Debt Service Account 2021E Senior Lien” (“Debt Service Account 2021E SR LIEN”). Moneys on deposit in the Debt Service Account 2021E SR LIEN shall be used to pay debt service on the Taxable Series 2021E Bonds when due.

(b) On or prior to each Interest Payment Date with respect to the Taxable Series 2021E Bonds, the Trustee shall deposit to the Debt Service Account 2021E SR LIEN from Revenues an amount sufficient to pay debt service then due on the Taxable Series 2021E Bonds.

#### **Section 3.3. Bond Proceeds Clearance Fund; Costs of Issuance Fund; Initial Deposits.**

(a) The Trustee is hereby authorized and directed to establish a special temporary Fund designated “Bonds Proceeds Clearance Fund Senior Lien 2021D” (the “Bond Proceeds Clearance Fund SR LIEN 2021D”). On the Issuance Date, the proceeds from the sale of the Series 2021D Bonds shall be deposited to the Bond Proceeds Clearance Fund SR LIEN 2021D and shall be applied and disbursed as set forth in a Letter of Instructions signed by an Authorized Officer. The Trustee shall create within the Bond Proceeds Clearance Fund SR LIEN 2021D such accounts as shall be authorized in a Letter of Instructions signed by an Authorized Officer and deposit the proceeds of the Series 2021D Bonds as shall be directed in such Letter of Instructions. The Bond Proceeds Clearance Fund SR LIEN 2021D shall be closed upon disbursement of all amounts deposited thereto.

(b) The Trustee is hereby authorized and directed to establish a special temporary Fund designated “Bonds Proceeds Clearance Fund Senior Lien 2021E” (the “Bond Proceeds Clearance Fund SR LIEN 2021E”). On the Issuance Date, the proceeds from the sale of the Taxable Series 2021E Bonds shall be deposited to the Bond Proceeds Clearance Fund SR LIEN 2021E and shall be applied and disbursed as set forth in a Letter of Instructions signed by an Authorized Officer. The Trustee shall create within the Bond Proceeds Clearance Fund SR LIEN 2021E such accounts as shall be authorized in a Letter of Instructions signed by an Authorized Officer and deposit the proceeds of the Taxable Series 2021E Bonds as shall be directed in such Letter of Instructions. The Bond Proceeds Clearance Fund SR LIEN 2021E shall be closed upon disbursement of all amounts deposited thereto.

(c) There is hereby established with the Trustee the “2021D Costs of Issuance Fund Senior Lien” (“COI 2021D Fund SR LIEN”), relating to the Series 2021D Bonds. There shall be deposited to the COI 2021D Fund SR LIEN from the proceeds of the Series 2021D Bonds deposited to the Bond Proceeds Clearance Fund SR LIEN 2021D, together with other lawfully available funds of the Authority, if any, the amounts set forth in a Letter of Instructions from the Authority. Such amounts shall be disbursed as set forth in a Letter of Instructions from the Authority. Amounts remaining in the COI 2021D Fund SR LIEN on the date which is 90 days after the Issuance Date of the Series 2021D Bonds shall be transferred to the Debt Service Account 2021D SR LIEN. Following such transfer, the COI 2021D Fund SR LIEN shall be closed.

(d) There is hereby established with the Trustee the “2021E Costs of Issuance Fund Senior Lien” (“COI 2021E Fund SR LIEN”), relating to the Taxable Series 2021E Bonds. There shall be deposited to the COI 2021E Fund SR LIEN from the proceeds of the Taxable Series 2021E Bonds deposited to the Bond Proceeds Clearance Fund SR LIEN 2021E, together with other lawfully available funds of the Authority, if any, the amounts set forth in a Letter of Instructions from the Authority. Such amounts shall be disbursed as set forth in a Letter of Instructions from the Authority. Amounts remaining in the COI 2021E Fund SR LIEN on the date which is 90 days after the Issuance Date of the Taxable Series 2021E Bonds shall be transferred to the Debt Service Account 2021E SR LIEN. Following such transfer, the COI 2021E Fund SR LIEN shall be closed.

Section 3.4. Senior Lien Debt Service Reserve Requirement. The Senior Lien Debt Service Reserve Requirement established in the First Supplemental Indenture is hereby confirmed and reestablished with respect to the 2021 Senior Lien Bonds as if set forth in full in this Supplemental Indenture. The provisions of Sections 3.9 and 3.10 of the Twelfth Supplemental Indenture relating to the establishment and operation of certain Accounts within the Senior Lien Debt Service Reserve Fund (including, but not limited to, the Bond Proceeds Funded Account, the Revenue Funded Account and the Springing Lien Account) are hereby ratified and affirmed, shall apply to and benefit the 2021 Senior Lien Bonds and Springing Lien Obligations generally, and shall survive the payment or defeasance of any Senior Lien Obligations issued pursuant to the Twelfth Supplemental Indenture.

Section 3.5. 2005 TxDOT Grant Fund. The 2005 TxDOT Grant Fund, established and created pursuant to the First Supplemental Indenture, is hereby reestablished, recreated and affirmed. The 2005 TxDOT Grant Fund shall be established with, and held and maintained by, the Trustee in accordance with the provisions of the Indenture and this Section 3.5. Until transferred in accordance with this Section 3.5, amounts on deposit in the 2005 TxDOT Grant Fund shall be invested by the Trustee in accordance with the provisions of the Indenture. Interest earned from the investment of any amounts in the 2005 TxDOT Grant Fund or any profits realized from any Permitted Investment of amounts in the 2005 TxDOT Grant Fund shall remain in such Fund. Amounts on deposit in the 2005 TxDOT Grant Fund shall be transferred by the Trustee from time to time in accordance with a Letter of Instruction from the Authority to the Operating Fund or the Senior Lien Debt Service Fund.

## **ARTICLE IV.**

### **FORMS OF BONDS**

Section 4.1. Forms of 2021 Senior Lien Bonds. The form of the 2021 Senior Lien Bonds, including any 2021 Senior Lien Bonds issued in exchange or replacement for any other 2021 Senior Lien Bonds or portion thereof, including the form of the Trustee's Authentication Certificate, the Registration Certificate of the Comptroller of Public Accounts of the State of Texas with respect to Initial 2021 Senior Lien Bonds and the Form of Assignment, shall be substantially as set forth in or attached to the Award Certificate, with such omissions, insertions, and variations as permitted or required by the Master Indenture, this Supplemental Indenture and the Award Certificate.

Section 4.2. Initial 2021 Senior Lien Bonds. The Award Certificate may provide for the use of Initial 2021 Senior Lien Bonds, as described in Section 2.4, representing the entire principal amount of the Series 2021D Bonds and Taxable Series 2021E Bonds, respectively, payable in stated installments to the order of the representative of the Underwriters or its designee, executed by the manual or facsimile signature of the Chairman of the Board of Directors of the Authority and attested by manual or facsimile signature of the Secretary of the Board of Directors of the Authority, approved by the Attorney General of Texas, and registered and manually signed by the Comptroller of Public Accounts of the State of Texas.

#### Section 4.3. Additional Provisions Regarding Bonds.

(a) The 2021 Senior Lien Bonds may have such letters, numbers, or other marks of identification (including identifying numbers and letters of the Committee on Uniform Securities Identification Procedures of the American Bankers Association) and such legends and endorsements (including any reproduction of an opinion of bond counsel) thereon as, consistent herewith, may be determined by the officers executing the 2021 Senior Lien Bonds, as evidenced by their execution thereof.

(b) The definitive 2021 Senior Lien Bonds shall be typewritten, printed, lithographed, or engraved and may be produced by any combination of such methods or produced in any other similar manner, all as determined by the officers executing such 2021 Senior Lien Bonds, as evidenced by their execution thereof.

(c) The Initial 2021 Senior Lien Bonds submitted to the Attorney General of the State of Texas may be typewritten or photocopied or otherwise produced or reproduced.

## **ARTICLE V.**

### **TAX MATTERS; REBATE**

#### Section 5.1. Federal Income Tax Matters Relating to Series 2021D Bonds.

(a) General. The Authority covenants not to take any action or omit to take any action that, if taken or omitted would cause the interest on the Series 2021D Bonds to be includable in gross income for federal income tax purposes. In furtherance thereof, the Authority covenants to

comply with sections 103 and 141 through 150 of the Code and the provisions set forth in the Federal Tax Certificate executed by the Authority in connection with the Series 2021D Bonds.

(b) No Private Activity Bonds. The Authority covenants that it will use the proceeds of the Series 2021D Bonds (including investment income) and the property financed, directly or indirectly, with such proceeds so that the Series 2021D Bonds will not be “private activity bonds” within the meaning of section 141 of the Code. Furthermore, the Authority will not take a deliberate action (as defined in section 1.141-2(d)(3) of the Regulations) that causes the Series 2021D Bonds to be a “private activity bond” unless it takes a remedial action permitted by section 1.141-12 of the Regulations.

(c) No Federal Guarantee. The Authority covenants not to take any action or omit to take any action that, if taken or omitted, would cause the Series 2021D Bonds to be “federally guaranteed” within the meaning of section 149(b) of the Code, except as permitted by section 149(b)(3) of the Code.

(d) No Hedge Bonds. The Authority covenants not to take any action or omit to take action that, if taken or omitted, would cause the Series 2021D Bonds to be “hedge bonds” within the meaning of section 149(g) of the Code.

(e) No Arbitrage Bonds. The Authority covenants that it will make such use of the proceeds of the Series 2021D Bonds (including investment income) and regulate the investment of such proceeds of the Series 2021D Bonds so that the Series 2021D Bonds will not be “arbitrage bonds” within the meaning of section 148(a) of the Code.

(f) Required Rebate. The Authority covenants that, if the Authority does not qualify for an exception to the requirements of section 148(f) of the Code, the Authority will comply with the requirement that certain amounts earned by the Authority on the investment of the gross proceeds of the Series 2021D Bonds, be rebated to the United States.

(g) Information Reporting. The Authority covenants to file or cause to be filed with the Secretary of the Treasury an information statement concerning the Series 2021D Bonds in accordance with section 149(e) of the Code.

(h) Record Retention. The Authority covenants to retain all material records relating to the expenditure of the proceeds (including investment income) of the 2016 Refunded Bonds and the Series 2021D Bonds and the use of the property financed, directly or indirectly, thereby until three years after the last Series 2021D Bond is redeemed or paid at maturity (or such other period as provided by subsequent guidance issued by the Department of the Treasury) in a manner that ensures their complete access throughout such retention period.

(i) Registration. The Series 2021D Bonds will be issued in registered form.

(j) Favorable Opinion of Bond Counsel. Notwithstanding the foregoing, the Authority will not be required to comply with any of the federal tax covenants set forth above if the Authority has received an opinion of nationally recognized bond counsel that such noncompliance will not adversely affect the excludability of interest on the Series 2021D Bonds from gross income for federal income tax purposes.

(k) Continuing Compliance. Notwithstanding any other provision of this Supplemental Indenture, the Authority's obligations under the federal tax covenants set forth above will survive the defeasance and discharge of the Series 2021D Bonds for as long as such matters are relevant to the excludability of interest on the Series 2021D Bonds from gross income for federal income tax purposes.

Section 5.2. 2021D Senior Lien Rebate Account.

(a) There is hereby established within the Rebate Fund, but not as part of the Trust Estate, a special account designated "2021D Senior Lien Rebate Account." Amounts deposited to the 2021D Senior Lien Rebate Account shall be applied to the payment of the Rebate Amount pursuant to a Letter of Instructions from the Authority. The 2021D Senior Lien Rebate Account and amounts on deposit therein are not security for the Series 2021D Bonds and are not part of the Trust Estate.

(b) The Authority will deliver to the Trustee, within 55 days after each Computation Date:

(i) a statement, signed by an officer of the Authority, stating the Rebate Amount as of such Computation Date; and

(ii) (1) if such Computation Date is an Installment Computation Date, an amount that, together with any amount then held for the credit of the 2021D Senior Lien Rebate Account, is equal to at least 90% of the Rebate Amount as of such Installment Computation Date, less any "previous rebate payments" (determined in accordance with section 1.148-3(f)(1) of the Regulations), made to the United States of America or (2) if such Computation Date is the Final Computation Date, an amount that, together with any amount then held for the credit of the 2021D Senior Lien Rebate Account, is equal to the Rebate Amount as of such Final Computation Date, less any "previous rebate payments" (determined in accordance with section 1.148-3(f)(1) of the Regulations) made to the United States of America; and

(iii) an Internal Revenue Service Form 8038-T properly signed and completed as of such Computation Date.

(c) Not later than 60 days after each Computation Date, the Trustee shall withdraw from the 2021D Senior Lien Rebate Account and remit to the United States of America the Rebate Amount required to be paid on such respective dates to the United States of America in accordance with written instructions from the Authority, which shall be in compliance with sections 1.148-1 through 1.148-8 of the Regulations or any successor regulation. Each payment required to be made to the United States of America pursuant to this Section shall be submitted to the Internal Revenue Service Center, Ogden, Utah 84201-0027 or such other address as provided by law or regulation and shall be accompanied by Internal Revenue Service Form 8038-T properly completed by the Authority with respect to the Series 2021D Bonds.

(d) If the Authority discovers or is notified as of any date that any amount required to be paid to the United States of America pursuant to this Section 5.2 has not been paid as required or that any payment paid to the United States of America pursuant to this Section 5.2 will have failed to satisfy any requirement of section 148(f) of the Code or 1.148-3 of the Regulations

(whether or not such failure will be due to any default by the Authority or the Trustee), the Authority will (1) deliver to the Trustee (for deposit to the 2021D Senior Lien Rebate Account) and cause the Trustee to pay to the United States of America from the 2021D Senior Lien Rebate Account (A) the Rebate Amount that the Authority failed to pay, plus any interest specified in section 1.148-3(h)(2) of the Regulations, if such correction payment is delivered to and received by the Trustee within 175 days after such discovery or notice, or (B) if such correction payment is not delivered to and received by the Trustee within 175 days after such discovery or notice, the amount determined in accordance with clause (A) of this subparagraph plus the fifty percent penalty required by section 1.148-3(h)(1) of the Regulations, and (2) deliver to the Trustee an Internal Revenue Service Form 8038-T completed as of such date. If such Rebate Amount, together with any penalty and/or interest due, is not paid to the United States of America in the amount and manner and by the time specified in the Regulations the Authority will take such steps as are necessary to prevent the Series 2021D Bonds from becoming “arbitrage bonds,” within the meaning of section 148 of the Code.

(e) The Authority will retain calculations, made in preparing the statements described in this Section 5.2, whether prepared by the Authority or the Arbitrage Analyst, for at least three years after the later of (1) the final maturity of the Series 2021D Bonds or (2) the first date on which no Series 2021D Bonds are outstanding.

(f) The Authority will not indirectly pay any amount otherwise payable to the federal government pursuant to the foregoing requirements to any person other than the federal government by entering into any investment arrangement with respect to the gross proceeds of the Series 2021D Bonds that is not purchased at fair market value or includes terms that the Authority would not have included if the Series 2021D Bonds were not subject to section 148(f) of the Code.

(g) Notwithstanding the foregoing, the Authority will not be required to perform the obligations set forth in this Section 5.2 (except for the obligation to retain accounting records as described in Section 5.2(e)) if the Authority has not earned any rebatable arbitrage and, therefore, is not subject to the rebate obligation set forth in section 148(f) of the Code. To the extent that the Authority will not be required to perform such obligations, the Authority will send written notice to the Trustee within 55 days after the applicable Computation Date.

## **ARTICLE VI.**

### **CONTINUING DISCLOSURE**

Section 6.1. Definitions. As used in this Article, the following terms have the meanings assigned to such terms below:

“Financial Obligation” means a (a) debt obligation; (b) derivative instrument entered into in connection with, or pledged as security or a source of payment for, an existing or planned debt obligation; or (c) guarantee of a debt obligation or any such derivative instrument; provided that “Financial Obligation” shall not include municipal securities (as defined in the Securities Exchange Act of 1934, as amended) as to which a final official statement (as defined in the Rule) has been provided to the MSRB consistent with the Rule.

“MSRB” means the Municipal Securities Rulemaking Board.



“Rule” means SEC Rule 15c2-12, as amended from time to time.

“SEC” means the United States Securities and Exchange Commission.

Section 6.2. Annual Reports.

(a) The Authority shall provide annually to the MSRB, in an electronic format as prescribed by the MSRB, within six (6) months after the end of each fiscal year, financial information and operating data with respect to the Authority and the System of the general type included in the final Official Statement, being the information described in Exhibit A hereto. Any financial statements so to be provided shall be (i) prepared in accordance with the accounting principles described in Exhibit A hereto, and (ii) audited, if the Authority commissions an audit of such statements and the audit is completed within the period during which they must be provided. If the audit of such financial statements is not complete within such period, then the Authority shall provide notice that audited financial statements are not available and shall provide unaudited financial statements for the applicable fiscal year to the MSRB. Thereafter, when and if audited financial statements become available, the Authority shall provide such audited financial statements as required to the MSRB. In addition to the annual information described above, the Authority will provide certain information on a quarterly basis, as described in Exhibit A hereto.

(b) If the Authority changes its fiscal year, it will notify the MSRB of the change (and of the date of the new fiscal year end) prior to the next date by which the Authority otherwise would be required to provide financial information and operating data pursuant to this Section.

(c) The financial information and operating data to be provided pursuant to this Section may be set forth in full in one or more documents or may be included by specific reference to any document (including an official statement or other offering document, if it is available from the MSRB) that theretofore has been provided to the MSRB or filed with the SEC.

Section 6.3. Event Notices.

(a) As used in this Section, the term “obligated person” shall mean any person, including the Authority, who is either generally or through an enterprise, fund, or account of such person committed by contract or other arrangement to support payment of all or part of the obligations on the 2021 Senior Lien Bonds (other than providers of municipal bond insurance, letters of credit, or other liquidity facilities). The Authority shall provide notice of any of the following events with respect to the 2021 Senior Lien Bonds to the MSRB, in an electronic format as prescribed by the MSRB, in a timely manner and not more than 10 business days after the occurrence of the event:

- (i) principal and interest payment delinquencies;
- (ii) nonpayment related defaults, if material;
- (iii) unscheduled draws on debt service reserves reflecting financial difficulties;
- (iv) unscheduled draws on credit enhancements reflecting financial difficulties;
- (v) substitution of credit or liquidity providers, or their failure to perform;

(vi) adverse tax opinions, the issuance by the Internal Revenue Service of proposed or final determinations of taxability, Notices of Proposed Issue (IRS Form 5701-TEB) or other material notices or determinations with respect to the tax status of the 2021 Senior Lien Bonds, or other material events affecting the tax status of the 2021 Senior Lien Bonds;

(vii) modifications to rights of Owners, if material;

(viii) bond calls, if material and tender offers;

(ix) defeasances;

(x) release, substitution, or sale of property securing repayment of the 2021 Senior Lien Bonds, if material;

(xi) rating changes;

(xii) bankruptcy, insolvency, receivership, or similar event of any obligated person, which shall occur as described below;

(xiii) the consummation of a merger, consolidation, or acquisition involving an obligated person or the sale of all or substantially all of the assets of the obligated person, other than in the ordinary course of business, the entry into of a definitive agreement to undertake such an action or the termination of a definitive agreement relating to any such actions, other than pursuant to its terms, if material;

(xiv) appointment of a successor or additional Trustee or the change of name of a Trustee, if material;

(xv) incurrence of a Financial Obligation of the Authority, if material, or agreement to covenants, events of default, remedies, priority rights, or other similar terms of a Financial Obligation of the Authority, any of which affect security holders, if material; and

(xvi) default, event of acceleration, termination event, modification of terms, or other similar events under the terms of a Financial Obligation of the Authority, any of which reflect financial difficulties.

For these purposes, (A) any event described in the immediately preceding clause (xii) is considered to occur when any of the following occur: the appointment of a receiver, fiscal agent, or similar officer for an obligated person in a proceeding under the United States Bankruptcy Code or in any other proceeding under state or federal law in which a court or governmental authority has assumed jurisdiction over substantially all of the assets or business of the obligated person, or if such jurisdiction has been assumed by leaving the existing governing body and officials or officers in possession but subject to the supervision and orders of a court or governmental authority, or the entry of an order confirming a plan of reorganization, arrangement, or liquidation by a court or governmental authority having supervision or jurisdiction over substantially all of the assets or business of the obligated person, and (B) the Authority intends the words used in the immediately preceding clauses (xv) and (xvi) in this Section and in the definition of Financial

Obligation in this Section to have the meanings ascribed to them in SEC Release No. 34-83885 dated August 20, 2018.

The Authority shall notify the MSRB, in a timely manner, of any failure by the Authority to provide financial information or operating data in accordance with Section 6.2 of this Supplemental Indenture by the time required by such Section.

All documents provided to the MSRB shall be accompanied by identifying information as prescribed by the MSRB.

Section 6.4. Limitations, Disclaimers and Amendments. The Authority shall be obligated to observe and perform the covenants specified in this Article for so long as, but only for so long as, the Authority remains an “obligated person” with respect to the 2021 Senior Lien Bonds within the meaning of the Rule, except that the Authority in any event will give notice of any deposit of funds that causes 2021 Senior Lien Bonds no longer to be Outstanding.

(a) The provisions of this Article are for the sole benefit of the Holders and beneficial owners of the 2021 Senior Lien Bonds, and nothing in this Article, express or implied, shall give any benefit or any legal or equitable right, remedy, or claim hereunder to any other person. The Authority undertakes to provide only the financial information, operating data, financial statements, and notices which it has expressly agreed to provide pursuant to this Article and does not hereby undertake to provide any other information that may be relevant or material to a complete presentation of the Authority’s financial results, condition, or prospects or hereby undertake to update any information provided in accordance with this Article or otherwise, except as expressly provided herein. The Authority does not make any representation or warranty concerning such information or its usefulness to a decision to invest in or sell 2021 Senior Lien Bonds at any future date.

UNDER NO CIRCUMSTANCES SHALL THE AUTHORITY BE LIABLE TO THE HOLDER OR BENEFICIAL OWNER OF ANY 2021 SENIOR LIEN BONDS OR ANY OTHER PERSON, IN CONTRACT OR TORT, FOR DAMAGES RESULTING IN WHOLE OR IN PART FROM ANY BREACH BY THE AUTHORITY, WHETHER NEGLIGENT OR WITHOUT FAULT ON ITS PART, OF ANY COVENANT SPECIFIED IN THIS ARTICLE, BUT EVERY RIGHT AND REMEDY OF ANY SUCH PERSON, IN CONTRACT OR TORT, FOR OR ON ACCOUNT OF ANY SUCH BREACH SHALL BE LIMITED TO AN ACTION FOR MANDAMUS OR SPECIFIC PERFORMANCE.

(b) No default by the Authority in observing or performing its obligations under this Article shall comprise a breach of or default under the Indenture for purposes of any other provisions of this Supplemental Indenture.

(c) Nothing in this Article is intended or shall act to disclaim, waive, or otherwise limit the duties of the Authority under federal and state securities laws.

(d) The provisions of this Article may be amended by the Authority from time to time to adapt to changed circumstances that arise from a change in legal requirements, a change in law, or a change in the identity, nature or status of the Authority, or type of business or operations conducted by the Authority, but only if (1) the provisions of this Article, as so amended, would have permitted an underwriter to purchase or sell 2021 Senior Lien Bonds in the primary offering

of the 2021 Senior Lien Bonds in compliance with the Rule, taking into account any amendments or interpretations of the Rule to the date of such amendment, as well as such changed circumstances, and (2) either (a) the Holders of a majority in aggregate principal amount (or any greater amount required by any other provisions of this Supplemental Indenture that authorizes such an amendment) of the Outstanding 2021 Senior Lien Bonds consent to such amendment or (b) a person that is unaffiliated with the Authority (such as nationally recognized bond counsel) determines that such amendment will not materially impair the interests of the Holders and beneficial owners of the 2021 Senior Lien Bonds. If the Authority so amends the provisions of this Article, it shall include with any amended financial information or operating data next provided in accordance with Section 6.2 an explanation, in narrative form, of the reasons for the amendment and of the impact of any change in the type of financial information or operating data so provided.

## ARTICLE VII.

### OTHER MATTERS

Section 7.1. Execution in Several Counterparts. This Supplemental Indenture may be simultaneously executed in several counterparts, all of which shall constitute one and the same instrument and each of which shall be, and shall be deemed to be, an original.

Section 7.2. Confirmation of Funds and Accounts. The establishment of Funds and Accounts heretofore established in the Indenture is hereby ratified and confirmed.

Section 7.3. Compliance with Texas Government Code. (a) The Trustee hereby verifies that it and its parent company, wholly- or majority-owned subsidiaries, and other affiliates, if any, do not boycott Israel and, to the extent this Supplemental Indenture is a contract for goods or services, will not boycott Israel during the term of this Supplemental Indenture. The foregoing verification is made solely to comply with Section 2271.002, Texas Government Code, and to the extent such Section does not contravene applicable Federal law. As used in the foregoing verification, “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. The Trustee understands “affiliate” to mean an entity that controls, is controlled by, or is under common control with the Trustee and exists to make a profit.

(b) The Trustee represents that neither it nor any of its parent company, wholly- or majority-owned subsidiaries, and other affiliates is a company identified on a list prepared and maintained by the Texas Comptroller of Public Accounts under Section 2252.153 or Section 2270.0201, Texas Government Code, and posted on any of the following pages of such officer’s internet website:

<https://comptroller.texas.gov/purchasing/docs/sudan-list.pdf>,  
<https://comptroller.texas.gov/purchasing/docs/iran-list.pdf>,  
<https://comptroller.texas.gov/purchasing/docs/fto-list.pdf>.

The foregoing representation is made solely to comply with Section 2252.152, Texas Government Code, and to the extent such Section does not contravene applicable Federal law and excludes the Trustee and each of its parent company, wholly- or majority-owned subsidiaries, and other affiliates, if any, that the United States government has affirmatively declared to be excluded from its federal sanctions regime relating to Sudan or Iran or any federal sanctions regime relating to a foreign terrorist organization. The Trustee understands “affiliate” to mean any entity that controls, is controlled by, or is under common control with the Trustee and exists to make a profit.

(a) To the extent this Supplemental Indenture constitutes a contract for goods or services for which a written verification is required under Section 2274.002, Texas Government Code (as added by Senate Bill 13, 87th Texas Legislature, Regular Session) as amended, the Trustee hereby verifies that it and its parent company, wholly- or majority- owned subsidiaries, and other affiliates, if any, do not boycott energy companies and will not boycott energy companies during the term of this Supplemental Indenture. The foregoing verification is made solely to comply with Section 2274.002, Texas Government Code, as amended, to the extent Section 2274.002, Texas Government Code does not contravene applicable Texas or Federal law. As used in the foregoing verification, “boycott energy companies” shall have the meaning assigned to the term “boycott energy company” in Section 809.001, Texas Government Code. The Trustee understands “affiliate” to mean an entity that controls, is controlled by, or is under common control with the Trustee and exists to make a profit.

(b) To the extent this Supplemental Indenture constitutes a contract for the purchase of goods or services for which a written verification is required under Section 2274.002, Texas Government Code (as added by Senate Bill 19, 87th Texas Legislature, Regular Session, “SB 19”), as amended, the Trustee hereby verifies that it and its parent company, wholly- or majority- owned subsidiaries, and other affiliates, if any,

(1) do not have a practice, policy, guidance or directive that discriminates against a firearm entity or firearm trade association; and

(2) will not discriminate during the term of this Supplemental Indenture against a firearm entity or firearm trade association.

The foregoing verification is made solely to comply with Section 2274.002, Texas Government Code, as amended, to the extent Section 2274.002, Texas Government Code does not contravene applicable Texas or Federal law. As used in the foregoing verification, “discriminate against a firearm entity or firearm trade association” shall have the meaning assigned to such term in Section 2274.001(3), Texas Government Code (as added by SB 19). The Trustee understands “affiliate” to mean an entity that controls, is controlled by, or is under common control with the Trustee and exists to make a profit.

[Execution Pages Follow]

IN WITNESS WHEREOF, the Authority and the Trustee have caused this Supplemental Indenture to be signed and attested on their behalf by their duly authorized representatives, all as of the date first hereinabove written.

CENTRAL TEXAS REGIONAL MOBILITY  
AUTHORITY

By \_\_\_\_\_  
Chief Financial Officer

Attest:

\_\_\_\_\_  
Secretary

REGIONS BANK, Trustee

By \_\_\_\_\_  
Authorized Officer

## **EXHIBIT A**

### **CONTINUING DISCLOSURE**

#### **DESCRIPTION OF ANNUAL DISCLOSURE OF FINANCIAL INFORMATION**

The following information is referred to in Article VI of this Supplemental Indenture.

##### **Annual Financial Information and Operating Data**

The financial information and operating data with respect to the Authority and the System to be provided in accordance with such Article are as specified below:

1. All quantitative financial information and operating data with respect to the Authority and the System of the general type included in the Official Statement under the headings “AUTHORITY FINANCIAL INFORMATION – System Historical Cash Flow and Debt Service Coverage,” “– Toll Rates,” and “SCHEDULE II – DEBT SERVICE REQUIREMENTS,” and APPENDIX A – AUDITED FINANCIAL STATEMENTS OF THE AUTHORITY.”

2. In the annual filing, the Authority will also furnish a copy of each General Engineering Consultant’s annual report relating to its inspection of the System, which reports may be provided as one report prepared jointly by more than one General Engineering Consultant.

The Authority will update and provide the foregoing information within six (6) months after the end of each Fiscal Year. In addition to the annual information described above, the Authority will furnish on a quarterly basis, within 60 days after the end of each quarter of the Fiscal Year, unaudited information regarding the number of toll transactions for the System and the Revenues generated by such toll transactions for the previous quarter of the Fiscal Year.

##### **Accounting Principles**

The accounting principles referred to in such Article are the accounting principles described in the notes to the financial statements referred to in Paragraph 1 above.



---

ESCROW AGREEMENT

Between

CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY

and

REGIONS BANK,  
as Escrow Agent

Pertaining to

Central Texas Regional Mobility Authority  
Senior Lien Revenue Bonds  
Series 2015A

and

Central Texas Regional Mobility Authority  
Senior Lien Revenue Refunding Bonds  
Series 2016

Dated as of October 1, 2021

TABLE OF CONTENTS

Page

ARTICLE I  
DEFINITIONS AND INTERPRETATIONS

Section 1.01 Definitions.....3  
Section 1.02 Other Definitions .....3  
Section 1.03 Interpretations .....3

ARTICLE II  
DEPOSIT OF FUNDS AND DEFEASANCE SECURITIES

Section 2.01 Deposits in the Escrow Funds.....4

ARTICLE III  
CREATION AND OPERATION OF ESCROW FUNDS

Section 3.01 Escrow Funds.....4  
Section 3.02 Payment of Principal and Interest.....5  
Section 3.03 Sufficiency of Escrow Funds .....5  
Section 3.04 Trust Fund.....5  
Section 3.05 Security for Cash Balances .....6

ARTICLE IV  
SUBSTITUTION OF DEFEASANCE SECURITIES

Section 4.01 In General.....6  
Section 4.02 Substitution of Defeasance Securities at Bond Closing.....7  
Section 4.03 Substitution of Defeasance Securities following Bond Closing .....7  
Section 4.04 Allocation of Certain Defeasance Securities .....8  
Section 4.05 Arbitrage .....8

ARTICLE V  
APPLICATION OF CASH BALANCES

Section 5.01 In General.....8  
Section 5.02 Reinvestment in SLGS.....8  
Section 5.03 Reinvestment of Cash Balances .....8

ARTICLE VI  
RECORDS AND REPORTS

Section 6.01 Records .....8  
Section 6.02 Reports .....9  
Section 6.03 Notification .....9

ARTICLE VII  
CONCERNING THE ESCROW AGENT

Section 7.01 Representations .....9  
Section 7.02 Limitation on Liability .....9  
Section 7.03 Compensation .....10  
Section 7.04 Successor Escrow Agents .....10

ARTICLE VIII  
MISCELLANEOUS

Section 8.01 Notice .....11  
Section 8.02 Termination of Responsibilities .....12  
Section 8.03 Binding Agreement .....12  
Section 8.04 Severability .....12  
Section 8.05 Texas Law Governs .....12  
Section 8.06 Time of the Essence .....12  
Section 8.07 Effective Date of Agreement .....12  
Section 8.08 Modification of Agreement .....12  
Section 8.09 Compliance with Texas Government Code .....13

ARTICLE IX  
REDEMPTION OF REFUNDED OBLIGATIONS

Section 9.01 Redemption of Refunded Obligations .....14  
Section 9.02 Notice of Redemption .....14

INDEX TO EXHIBITS

## ESCROW AGREEMENT

THIS ESCROW AGREEMENT, dated as of October 1, 2021 (herein, together with any amendments or supplements hereto, called the or this “Agreement”), entered into by and between CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY (the “Issuer”), and REGIONS BANK, an Alabama state banking corporation, as escrow agent (herein, together with any successor or assign in such capacity, called the “Escrow Agent”).

### WITNESSETH:

WHEREAS, the Issuer has heretofore issued and there presently remain outstanding (i) its Senior Lien Revenue Bonds, Series 2015A, described in Exhibit A-1 (the “Series 2015A Refunded Bonds”) and (ii) its Senior Lien Revenue Refunding Bonds, Series 2016, described in Exhibit A-2 (the “Series 2016 Refunded Bonds” and, together with the Series 2015A Refunded Bonds, the “Refunded Obligations”); and

WHEREAS, the Refunded Obligations are scheduled to mature or have been called for early redemption, as applicable, in such years and in such amounts as are set forth in Exhibit B-1 and Exhibit B-2 attached hereto and made a part hereof; and

WHEREAS, Section 1102 of the Master Indenture (as hereinafter defined) provides that Obligations and the interest thereon shall be deemed to be paid, retired and no longer outstanding within the meaning of the Master Indenture at such time as funds sufficient for the payment of the principal of and interest on such Obligations to be defeased and/or refunded shall have been deposited with an escrow agent in accordance with an escrow agreement or other instrument for such payment; and

WHEREAS, Chapter 1207, Texas Government Code, as amended (“Chapter 1207”), authorizes the Issuer to issue refunding bonds for the purpose of refunding the Refunded Obligations in advance of their maturities, and to accomplish such refunding by depositing the proceeds of such refunding bonds with an entity authorized to receive such deposit under Chapter 1207 in an amount sufficient, together with other lawfully available funds of the Issuer, if any, to provide for the payment or redemption of the Refunded Obligations, and that such deposit shall constitute the making of firm banking and financial arrangements for the discharge and final payment or redemption of the Refunded Obligations; and

WHEREAS, when firm banking arrangements have been made for the payment of principal and interest to the maturity dates or redemption dates of the Refunded Obligations, then the Refunded Obligations shall no longer be regarded as outstanding except for the purpose of receiving payment from the funds provided for such purpose; and

WHEREAS, Chapter 1207 further authorizes the Issuer to enter into an escrow agreement with a trust company or commercial bank authorized to receive such deposit under Chapter 1207 with respect to the safekeeping, investment, administration and disposition of any such deposit for the Refunded Obligations, upon such terms and conditions as the Issuer and such trust company or commercial bank may agree, provided that such deposits may be invested only in obligations described in Section 1207.062(b) of Chapter 1207, and which may be in book entry form, and which shall mature and/or bear interest payable at such times and in such amounts as

will be sufficient to provide for the scheduled payment of principal and interest on the Refunded Obligations when due; and

WHEREAS, this Agreement constitutes an escrow agreement of the kind authorized and required by Chapter 1207; and

WHEREAS, the Escrow Agent is the trustee under and pursuant to that certain Master Trust Indenture, dated as of February 1, 2005 (as amended from time to time, the “Master Indenture”), between the Issuer and Regions Bank, as trustee (the “Trustee”); and

WHEREAS, Chapter 1207 makes it the duty of the Escrow Agent to comply with the terms of this Agreement and timely make available to the other places of payment, if any, for the Refunded Obligations the amounts required to provide for the payment of the principal of and interest on such obligations when due, and in accordance with their terms, but solely from the funds, in the manner, and to the extent provided in this Agreement; and

WHEREAS, the issuance, sale, and delivery of the Central Texas Regional Mobility Authority’s (i) Senior Lien Revenue Refunding Bonds, Series 2021D (the “Series 2021D Bonds”) and (ii) Senior Lien Revenue Refunding Bonds, Taxable Series 2021E (the “Taxable Series 2021E Bonds”) and, together with the Series 2021D Bonds, the “2021 Obligations”), have been duly authorized for the purpose, among others, of obtaining the funds required to provide for the payment of the principal of the Refunded Obligations at their respective maturity or redemption dates, as applicable, and the interest thereon to such dates; and

WHEREAS, concurrently with the issuance of the 2021 Obligations, (i) a portion of the proceeds of the Series 2021D Bonds shall be applied to the purchase of Defeasance Securities (as herein defined) for deposit to the credit of the Series 2016 Refunded Bonds Escrow Fund (as herein defined) created pursuant to this Agreement and to establish a beginning cash balance therein, if needed, and (ii) a portion of the proceeds of the Taxable Series 2021E Bonds shall be applied to the purchase of Defeasance Securities for deposit to the credit of the Series 2015A Refunded Bonds Escrow Fund (as herein defined) created pursuant to this Agreement and to establish a beginning balance therein, if needed; and

WHEREAS, to facilitate the receipt and transfer of proceeds of the Defeasance Securities the Issuer desires to establish the Escrow Funds (as herein defined) at the designated office of the Escrow Agent; and

WHEREAS, the Escrow Agent is a party to this Agreement and hereby acknowledges its acceptance of the terms and provisions hereof;

NOW, THEREFORE, in consideration of the mutual undertakings, promises and agreements herein contained, the sufficiency of which hereby is acknowledged, and to secure the full and timely payment of principal of and the interest on the Refunded Obligations, the Issuer and the Escrow Agent mutually undertake, promise, and agree for themselves and their respective representatives and successors, as follows:

ARTICLE I  
DEFINITIONS AND INTERPRETATIONS

Section 1.01 Definitions. Unless the context clearly indicates otherwise, the following terms shall have the meanings assigned to them below when they are used in this Agreement:

“Beginning Cash Balance” means the funds described as such in Exhibit C-1 and Exhibit C-2 attached to this Agreement.

“Code” means the Internal Revenue Code of 1986, as amended, including applicable regulations, published rulings and court decisions thereunder.

“Defeasance Securities” means (i) Government Obligations and (ii) noncallable obligations of an agency or instrumentality of the United States of America, including obligations that are unconditionally guaranteed by an agency or instrumentality and that, on the date of the purchase thereof, are rated as to investment quality by a nationally recognized investment rating firm not less than “AAA” or its equivalent.

“Escrow Fund” or “Escrow Funds” means one or more of the Series 2015A Refunded Bonds Escrow Fund and the Series 2016 Refunded Bonds Escrow Fund created and described in Section 3.01 of this Agreement.

“Government Obligations” mean direct obligations of, or obligations the principal of and interest on which are guaranteed by the full faith and credit of, the United States of America.

“Series 2015A Refunded Bonds Escrow Fund” means the escrow fund created in Section 3.01(a) of this Agreement to be administered by the Escrow Agent pursuant to the provisions of this Agreement for the payment and redemption of the Series 2015A Refunded Bonds described in Exhibit A-1.

“Series 2016 Refunded Bonds Escrow Fund” means the escrow fund created in Section 3.01(b) of this Agreement to be administered by the Escrow Agent pursuant to the provisions of this Agreement for the payment and redemption of the Series 2016 Refunded Bonds described in Exhibit A-2.

Section 1.02 Other Definitions. The terms “Agreement,” “Issuer,” “Escrow Agent,” “Series 2015A Refunded Bonds,” “Series 2016 Refunded Bonds,” “Refunded Obligations,” “Master Indenture,” “Chapter 1207,” “Trustee,” “Series 2021D Bonds,” “Taxable Series 2021E Bonds,” and “2021 Obligations,” when they are used in this Agreement, shall have the meanings assigned to them in the preamble to this Agreement.

Section 1.03 Interpretations. The titles and headings of the articles and sections of this Agreement have been inserted for convenience and reference only and are not to be considered a part hereof and shall not in any way modify or restrict the terms hereof. This Agreement and all of the terms and provisions hereof shall be liberally construed to effectuate the purposes set forth herein and to achieve the intended purpose of providing for the refunding of the Refunded Obligations in accordance with applicable law.

ARTICLE II  
DEPOSIT OF FUNDS AND DEFEASANCE SECURITIES

Section 2.01 Deposits in the Escrow Funds. Concurrently with the sale and delivery of the 2021 Obligations the Issuer shall deposit, or cause to be deposited, with the Escrow Agent (i) for deposit in the Series 2015A Refunded Bonds Escrow Fund, the Beginning Cash Balance and the Defeasance Securities described in Exhibit C-1; and (ii) for deposit in the Series 2016 Refunded Bonds Escrow Fund, the Beginning Cash Balance and the Defeasance Securities described in Exhibit C-2. The Escrow Agent shall, upon the receipt thereof, acknowledge such receipt to the Issuer in writing.

ARTICLE III  
CREATION AND OPERATION OF ESCROW FUNDS

Section 3.01 Escrow Funds. (a) The Escrow Agent hereby creates on its books a special trust and irrevocable escrow fund to be known as the Central Texas Regional Mobility Authority Series 2015A Refunded Bonds Escrow Fund (the “Series 2015A Refunded Bonds Escrow Fund”), for the purpose of making firm banking arrangements for the payment of the principal of and interest on the Series 2015A Refunded Bonds described in Exhibit A-1. The Escrow Agent hereby agrees that upon receipt thereof it will deposit to the credit of the Series 2015A Refunded Bonds Escrow Fund the Beginning Cash Balance and the Defeasance Securities described in Exhibit C-1 attached hereto. Such deposit, all proceeds therefrom, and all cash balances from time to time on deposit therein (a) shall be the property of the Series 2015A Refunded Bonds Escrow Fund, (b) shall be applied only in strict conformity with the terms and conditions of this Agreement, and (c) to the extent needed to pay the principal and interest requirements on the Series 2015A Refunded Bonds, are hereby irrevocably pledged to the payment of the principal of and interest on the Series 2015A Refunded Bonds, which payment shall be made by timely transfers of such amounts at such times as are provided for in Section 3.02(a) hereof. When the final transfers have been made for the payment of such principal of and interest on the Series 2015A Refunded Bonds, any balance then remaining in the Series 2015A Refunded Bonds Escrow Fund shall be transferred to the Issuer, and the Escrow Agent shall thereupon be discharged from any further duties hereunder with respect to the Series 2015A Refunded Bonds Escrow Fund.

(b) The Escrow Agent hereby creates on its books a special trust and irrevocable escrow fund to be known as the Central Texas Regional Mobility Authority Series 2016 Refunded Bonds Escrow Fund (the “Series 2016 Refunded Bonds Escrow Fund”), for the purpose of making firm banking arrangements for the payment of the principal of and interest on the Series 2016 Refunded Bonds described in Exhibit A-2. The Escrow Agent hereby agrees that upon receipt thereof it will deposit to the credit of the Series 2016 Refunded Bonds Escrow Fund the Beginning Cash Balance and the Defeasance Securities described in Exhibit C-2 attached hereto. Such deposit, all proceeds therefrom, and all cash balances from time to time on deposit therein (a) shall be the property of the Series 2016 Refunded Bonds Escrow Fund, (b) shall be applied only in strict conformity with the terms and conditions of this Agreement, and (c) to the extent needed to pay the principal and interest requirements on the Series 2016 Refunded Bonds, are hereby irrevocably pledged to the payment of the principal of and interest on the Series 2016 Refunded Bonds, which payment shall be made by timely transfers of such amounts at such times as are provided for in Section 3.02(b) hereof. When the final transfers have been made for

the payment of such principal of and interest on the Series 2016 Refunded Bonds, any balance then remaining in the Series 2016 Refunded Bonds Escrow Fund shall be transferred to the Issuer, and the Escrow Agent shall thereupon be discharged from any further duties hereunder with respect to the Series 2016 Refunded Bonds Escrow Fund.

Section 3.02 Payment of Principal and Interest. (a) The Escrow Agent is hereby irrevocably instructed to transfer, from the cash balances from time to time on deposit in the Series 2015A Refunded Bonds Escrow Fund, the amounts required to pay the principal of the Series 2015A Refunded Bonds at their respective maturity date or dates as of which such Series 2015A Refunded Bonds have been called for earlier redemption, and to pay interest thereon when due, in the amounts and at the times shown in Exhibit B-1 attached hereto.

(b) The Escrow Agent is hereby irrevocably instructed to transfer, from the cash balances from time to time on deposit in the Series 2016 Refunded Bonds Escrow Fund, the amounts required to pay the principal of the Series 2016 Refunded Bonds at their respective maturity date or dates as of which such Series 2016 Refunded Bonds have been called for earlier redemption, and to pay interest thereon when due, in the amounts and at the times shown in Exhibit B-2 attached hereto.

Section 3.03 Sufficiency of Escrow Funds. (a) On the basis of a report (the "Report") delivered by [Public Finance Partners LLC], a copy of which has been delivered to the Escrow Agent, the Issuer represents that the successive receipts of the principal of and interest on the Defeasance Securities described in Exhibit C-1 will assure that the cash balance on deposit from time to time in the Series 2015A Refunded Bonds Escrow Fund will be at all times sufficient to provide moneys for transfer to each place of payment for the Series 2015A Refunded Bonds, at the times and in the amounts required to pay the interest on the Series 2015A Refunded Bonds as such interest comes due and the principal of the Series 2015A Refunded Bonds as such principal comes due, all as more fully set forth in Exhibit D-1 attached hereto. Notice of any such insufficiency shall be given promptly to the Issuer as hereinafter provided. The Escrow Agent shall not in any manner be responsible for any insufficiency of funds in the Series 2015A Refunded Bonds Escrow Fund.

(b) On the basis of the Report, the Issuer represents that the successive receipts of the principal of and interest on the Defeasance Securities described in Exhibit C-2 will assure that the cash balance on deposit from time to time in the Series 2016 Refunded Bonds Escrow Fund will be at all times sufficient to provide moneys for transfer to each place of payment for the Series 2016 Refunded Bonds, at the times and in the amounts required to pay the interest on the Series 2016 Refunded Bonds as such interest comes due and the principal of the Series 2016 Refunded Bonds as such principal comes due, all as more fully set forth in Exhibit D-2 attached hereto. Notice of any such insufficiency shall be given promptly to the Issuer as hereinafter provided. The Escrow Agent shall not in any manner be responsible for any insufficiency of funds in the Series 2016 Refunded Bonds Escrow Fund.

Section 3.04 Trust Fund. (a) The Escrow Agent shall hold at all times the Series 2015A Refunded Bonds Escrow Fund, the Defeasance Securities on deposit therein and all other assets of the Series 2015A Refunded Bonds Escrow Fund wholly segregated from all other funds and securities on deposit with the Escrow Agent; it shall never allow the Defeasance Securities or any other assets of the Series 2015A Refunded Bonds Escrow Fund to be commingled with any



other funds or securities of the Escrow Agent; and it shall hold and dispose of the assets of the Series 2015A Refunded Bonds Escrow Fund only as set forth herein. The Defeasance Securities and other assets of the Series 2015A Refunded Bonds Escrow Fund shall always be maintained by the Escrow Agent as trust funds for the benefit of the owners of the Series 2015A Refunded Bonds, and a special account thereof shall at all times be maintained on the books of the Escrow Agent. The owners of the Series 2015A Refunded Bonds shall be entitled to a preferred claim and first lien upon the Defeasance Securities, the proceeds thereof, and all other assets of the Series 2015A Refunded Bonds Escrow Fund. The amounts received by the Escrow Agent under this Agreement shall not be considered as a banking deposit by the Issuer, and the Escrow Agent shall have no right or title with respect thereto except as a trustee and Escrow Agent under the terms of this Agreement. The amounts received by the Escrow Agent under this Agreement shall not be subject to warrants, drafts or checks drawn by the Issuer or, except to the extent expressly herein provided, by a place of payment for the Series 2015A Refunded Bonds.

(b) The Escrow Agent shall hold at all times the Series 2016 Refunded Bonds Escrow Fund, the Defeasance Securities on deposit therein and all other assets of the Series 2016 Refunded Bonds Escrow Fund wholly segregated from all other funds and securities on deposit with the Escrow Agent; it shall never allow the Defeasance Securities or any other assets of the Series 2016 Refunded Bonds Escrow Fund to be commingled with any other funds or securities of the Escrow Agent; and it shall hold and dispose of the assets of the Series 2016 Refunded Bonds Escrow Fund only as set forth herein. The Defeasance Securities and other assets of the Series 2016 Refunded Bonds Escrow Fund shall always be maintained by the Escrow Agent as trust funds for the benefit of the owners of the Series 2016 Refunded Bonds, and a special account thereof shall at all times be maintained on the books of the Escrow Agent. The owners of the Series 2016 Refunded Bonds shall be entitled to a preferred claim and first lien upon the Defeasance Securities, the proceeds thereof, and all other assets of the Series 2016 Refunded Bonds Escrow Fund. The amounts received by the Escrow Agent under this Agreement shall not be considered as a banking deposit by the Issuer, and the Escrow Agent shall have no right or title with respect thereto except as a trustee and Escrow Agent under the terms of this Agreement. The amounts received by the Escrow Agent under this Agreement shall not be subject to warrants, drafts or checks drawn by the Issuer or, except to the extent expressly herein provided, by a place of payment for the Series 2016 Refunded Bonds.

Section 3.05 Security for Cash Balances. Cash balances from time to time on deposit in the Escrow Funds shall, to the extent not insured by the Federal Deposit Insurance Corporation or its successor, be continuously secured by a pledge of direct noncallable obligations of, or noncallable obligations unconditionally guaranteed by, the United States of America, having a market value at least equal to such cash balances.

#### ARTICLE IV SUBSTITUTION OF DEFEASANCE SECURITIES

Section 4.01 In General. Except as provided in Section 4.02 and 4.03 hereof, the Escrow Agent shall not have any power or duty to make substitutions for the Defeasance Securities described in Exhibit C-1 and Exhibit C-2 hereto, or to sell, transfer, or otherwise dispose of such Defeasance Securities.

Section 4.02 Substitution of Defeasance Securities at Bond Closing. Concurrently with the sale and delivery of the 2021 Obligations, the Issuer, at its option, may substitute cash or Defeasance Securities for the Defeasance Securities listed in part III of Exhibit C-1 or Exhibit C-2 attached hereto, but only if such cash and/or Defeasance Securities:

(a) are in an amount, and/or mature in an amount, which, together with any cash substituted for such obligations, is equal to or greater than the amount payable on the maturity date of the obligation listed in part III of Exhibit C-1 or Exhibit C-2 for which such obligation is substituted, and

(b) mature on or before the maturity date of the obligation listed in part III of Exhibit C-1 or Exhibit C-2 for which such obligation is substituted.

The Issuer may at any time substitute the Defeasance Securities listed in part III of Exhibit C-1 or Exhibit C-2 which, as permitted by the preceding sentence, were not deposited to the credit of the Escrow Fund, for the cash and/or obligations that were substituted concurrently with the sale and delivery of the 2021 Obligations for such Defeasance Securities, provided, that upon any such substitution the Escrow Agent receives (i) a new verification report from a firm of independent certified public accountants as to the sufficiency of the Defeasance Securities to provide for the payment of the applicable Refunded Obligations (assuming such substitution has been made and assuming a zero percent reinvestment rate) and (ii) an opinion of bond counsel to the effect that such substitution shall not affect the tax-exempt status of interest on the applicable Refunded Obligations or the 2021 Obligations, if applicable.

Section 4.03 Substitution of Defeasance Securities following Bond Closing. (a) At the written request of the Issuer, and upon compliance with the conditions hereinafter stated, the Escrow Agent shall sell, transfer, otherwise dispose of or request the redemption of all or any portion of the Defeasance Securities and apply the proceeds therefrom to purchase related Refunded Obligations or other Defeasance Securities described in Exhibit C-1 or Exhibit C-2. Any such transaction may be effected by the Escrow Agent only if (1) the Escrow Agent shall have received a written opinion from a firm of independent certified public accountants that such transaction will not cause the amount of money and securities in the affected Escrow Fund to be reduced below an amount which will be sufficient, when added to the interest to accrue thereon and assuming a zero percent reinvestment rate, to provide for the payment of principal of and interest on the remaining related Refunded Obligations as they become due, and (2) the Escrow Agent shall have received the unqualified written legal opinion of nationally recognized bond counsel or tax counsel acceptable to the Issuer and the Escrow Agent to the effect that (A) such transaction will not cause any of the 2021 Obligations to be an “arbitrage bond” within the meaning of the Code, if applicable, or otherwise adversely affect the tax-exempt status of the related Refunded Obligations or the 2021 Obligations, if applicable, and (B) that such transaction complies with the Constitution and laws of the State of Texas.

(b) The foregoing provisions of substitution notwithstanding, the Escrow Agent shall be under no obligation to effect the substitution of the Defeasance Securities in the manner contemplated by Subsection 4.03(a) if the Issuer fails to deliver or cause to be delivered to the Escrow Agent no later than three Business Days prior to the proposed date such substitution is to be effected a written certificate setting forth in reasonable detail the maturity dates and maturity

amounts of the Defeasance Securities to be substituted and the proposed date such substitution is to occur.

Section 4.04 Allocation of Certain Defeasance Securities. With respect to each Escrow Fund, the maturing principal of and interest on the Defeasance Securities on deposit in such Escrow Fund may be applied to the payment of any Refunded Obligations to which such Escrow Fund relates and no allocation or segregation of the receipts of principal or interest from such Defeasance Securities is required.

Section 4.05 Arbitrage. The Issuer hereby covenants and agrees that it shall never request the Escrow Agent to exercise any power hereunder or permit any part of the money in the Escrow Funds or proceeds from the sale of Defeasance Securities to be used directly or indirectly to acquire any securities or obligations if the exercise of such power or the acquisition of such securities or obligations would cause any 2021 Obligations, if applicable, or Refunded Obligations to be an “arbitrage bond” within the meaning of Section 148 of the Code.

#### ARTICLE V APPLICATION OF CASH BALANCES

Section 5.01 In General. Except as provided in Sections 5.02 and 5.03 hereof, neither the Issuer nor the Escrow Agent shall reinvest any moneys deposited to or held as part of the Escrow Funds.

Section 5.02 Reinvestment in SLGS. Cash balances in the Escrow Funds shall be reinvested as set forth on Exhibit E attached hereto.

Section 5.03 Reinvestment of Cash Balances. At the written request of the Issuer, and upon compliance with the conditions hereinafter stated, the Escrow Agent shall permit or cause the reinvestment of cash balances in the Escrow Funds, pending the use thereof to pay when due the principal of and interest on the Refunded Obligations, in Defeasance Securities which obligations must mature on or before the respective dates needed for payment of the Refunded Obligations. Any such modification must include (i) an opinion of nationally recognized bond counsel that such transaction does not adversely affect the tax-exempt nature of the 2021 Obligations or the Refunded Obligations, if applicable, and complies with the Constitution and laws of the State of Texas and (ii) a verification report by a firm of independent certified public accountants verifying the sufficiency of the Escrow Fund and the yield on the investment thereof.

#### ARTICLE VI RECORDS AND REPORTS

Section 6.01 Records. The Escrow Agent will keep books of record and account in which complete and correct entries shall be made of all transactions relating to the receipts, disbursements, allocations and application of the money and Defeasance Securities deposited to each Escrow Fund and all proceeds thereof, and such books shall be available for inspection at reasonable hours and under reasonable conditions by the Issuer and the owners of the related Refunded Obligations.

Section 6.02 Reports. While this Agreement remains in effect, the Escrow Agent at least annually shall prepare and send to the Issuer a written report summarizing all transactions relating to each Escrow Fund during the preceding year, including, without limitation, credits to each Escrow Fund as a result of interest payments on or maturities of the Defeasance Securities and transfers from each Escrow Fund for payments on the Refunded Obligations or otherwise, together with a detailed statement of all Defeasance Securities and the cash balance on deposit in each Escrow Fund as of the end of such period.

Section 6.03 Notification. The Escrow Agent shall notify the Issuer immediately if at any time during the term of this Escrow Agreement it determines that the cash and Defeasance Securities in any Escrow Fund are not sufficient to provide for the timely payment of all interest on and principal of the related Refunded Obligations, but the Escrow Agent shall not be responsible for any insufficiency of funds in the Escrow Funds.

## ARTICLE VII CONCERNING THE ESCROW AGENT

Section 7.01 Representations. The Escrow Agent hereby represents that it has all necessary power and authority to enter into this Agreement and undertake the obligations and responsibilities imposed upon it herein, and that it will carry out all of its obligations hereunder.

Section 7.02 Limitation on Liability. The liability of the Escrow Agent to transfer funds for the payment of the principal of and interest on the Refunded Obligations shall be limited to the proceeds of the Defeasance Securities and the cash balances from time to time on deposit in the Escrow Funds. Notwithstanding any provision contained herein to the contrary, neither the Escrow Agent nor any place of payment for the Refunded Obligations shall have any liability whatsoever for the insufficiency of funds from time to time in the Escrow Funds or any failure of the obligors of the Defeasance Securities to make timely payment thereon, except for the obligation to notify the Issuer promptly of any such occurrence.

The recitals herein and in the proceedings authorizing the 2021 Obligations shall be taken as the statements of the Issuer and shall not be considered as made by, or imposing any obligation or liability upon, the Escrow Agent. In its capacity as Escrow Agent, it is agreed that the Escrow Agent need look only to the terms and provisions of this Agreement.

The Escrow Agent makes no representations as to the value, conditions or sufficiency of the Escrow Funds, or any part thereof, or as to the title of the Issuer thereto, or as to the security afforded thereby or hereby, and the Escrow Agent shall not incur any liability or responsibility in respect to any of such matters.

It is the intention of the parties hereto that the Escrow Agent shall never be required to use or advance its own funds or otherwise incur personal financial liability in the performance of any of its duties or the exercise of any of its rights and powers hereunder.

The Escrow Agent shall not be liable for any action taken or neglected to be taken by it in good faith in any exercise of reasonable care and believed by it to be within the discretion or power conferred upon it by this Agreement, nor shall the Escrow Agent be responsible for the consequences of any error of judgment; and the Escrow Agent shall not be answerable for any loss unless the same shall have been through its negligence or want of good faith.

Unless it is specifically otherwise provided herein, the Escrow Agent has no duty to determine or inquire into the happening or occurrence of any event or contingency or the performance or failure of performance of the Issuer with respect to arrangements or contracts with others, with the Escrow Agent's sole duty hereunder being to safeguard the Escrow Funds, to dispose of and deliver the same in accordance with this Agreement. If, however, the Escrow Agent is called upon by the terms of this Agreement to determine the occurrence of any event or contingency, the Escrow Agent shall be obligated, in making such determination, only to exercise reasonable care and diligence, and in event of error in making such determination the Escrow Agent shall be liable only for its own willful misconduct or its negligence. In determining the occurrence of any such event or contingency the Escrow Agent may request from the Issuer or any other person such reasonable additional evidence as the Escrow Agent in its discretion may deem necessary to determine any fact relating to the occurrence of such event or contingency, and in this connection may make inquiries of, and consult with, among others, the Issuer at any time. The Issuer and the Escrow Agent agree that the Escrow Agent shall have the right (but not the obligation) to file a bill of interpleader in any court of competent jurisdiction within the State of Texas to determine the rights of any person claiming any interest in this Agreement or the Escrow Funds, and the costs and expenses incurred by the Escrow Agent in connection therewith shall constitute extraordinary services payable by the Issuer in accordance with Section 7.03 hereof.

Section 7.03 Compensation. (a) Concurrently with the sale and delivery of the 2021 Obligations, the Issuer shall pay to the Escrow Agent the sum of \$\_\_\_\_\_, the sufficiency of which is hereby acknowledged by the Escrow Agent to pay its fee for performing the services of Escrow Agent hereunder and for all expenses incurred or to be incurred by it as Escrow Agent in the administration of this Agreement. In the event that the Escrow Agent is requested to perform any extraordinary services hereunder, the Issuer hereby agrees to pay reasonable fees to the Escrow Agent for such extraordinary services and to reimburse the Escrow Agent for all reasonable expenses incurred by the Escrow Agent in performing such extraordinary services, and the Escrow Agent hereby agrees to look only to the Issuer for the payment of such fees and reimbursement of such expenses. The Escrow Agent, and in its capacity as trustee and paying agent for the Refunded Obligations, hereby agrees that in no event shall it ever assert any claim or lien against the Escrow Funds for any fees for its services, whether regular or extraordinary, as Escrow Agent, or in any other capacity, or for reimbursement for any of its expenses. All amounts due and owing or to be owed to the Escrow Agent for its services as trustee and as paying agent for the Refunded Obligations have been paid by the Issuer.

(b) Upon receipt of the aforesaid specific sum stated in subsection (a) of this Section, the Escrow Agent shall acknowledge such receipt to the Issuer in writing.

Section 7.04 Successor Escrow Agents. (a) If at any time the Escrow Agent or its legal successor or successors should become unable, through operation of law or otherwise, to act as Escrow Agent hereunder, or if its property and affairs shall be taken under the control of any state or federal court or administrative body because of insolvency or bankruptcy or for any other reason, a vacancy shall forthwith exist in the office of Escrow Agent hereunder. In such event, the Issuer, by appropriate action, promptly shall appoint an Escrow Agent to fill such vacancy. If no successor Escrow Agent shall have been appointed by the Issuer within 60 days, a successor may be appointed by the owners of a majority in principal amount of the Refunded Obligations then outstanding by an instrument or instruments in writing filed with the Issuer,

signed by such owners or by their duly authorized attorneys-in-fact. If, in a proper case, no appointment of a successor Escrow Agent shall be made pursuant to the foregoing provisions of this section within three months after a vacancy shall have occurred, the owner of any Refunded Obligation, or the Escrow Agent, may apply to any court of competent jurisdiction to appoint a successor Escrow Agent. Such court may thereupon, after such notice, if any, as it may deem proper, prescribe and appoint a successor Escrow Agent.

(b) The Escrow Agent may at any time resign and be discharged from the trust hereby created by giving not less than 60 days' written notice to the Issuer; provided, that, no such resignation shall take effect unless: (i) a successor Escrow Agent shall have been appointed by the owners of the Refunded Obligations or by the Issuer as herein provided; (ii) such successor Escrow Agent shall have accepted such appointment; (iii) such successor Escrow Agent shall have agreed to accept the fees currently in effect for this Agreement; and (iv) such Escrow Agent shall have paid over to the successor Escrow Agent a proportional part of the Escrow Agent's fee hereunder. Such resignation shall take effect immediately upon compliance with the foregoing requirements. The Escrow Agent, however, reserves the right to petition a court of competent jurisdiction to appoint a successor Escrow Agent.

(c) Any successor Escrow Agent shall be: (i) a corporation organized and doing business under the laws of the United States or the State of Texas; (ii) authorized under such laws to exercise corporate trust powers; (iii) have its principal office and place of business in the State of Texas; (iv) have a combined capital and surplus of at least \$5,000,000; (v) subject to the supervision or examination by Federal or State authority; and (vi) qualified to serve as Escrow Agent under the provisions of Chapter 1207.

(d) Any successor Escrow Agent shall execute, acknowledge and deliver to the Issuer and the Escrow Agent an instrument accepting such appointment hereunder, and the Escrow Agent shall execute and deliver an instrument transferring to such successor Escrow Agent, subject to the terms of this Agreement, all the rights, powers and trusts of the Escrow Agent hereunder. Upon the request of any such successor Escrow Agent, the Issuer shall execute any and all instruments in writing for more fully and certainly vesting in and confirming to such successor Escrow Agent all such rights, powers and duties. The Escrow Agent shall pay over to its successor Escrow Agent a proportional part of the Escrow Agent's fee hereunder.

#### ARTICLE VIII MISCELLANEOUS

Section 8.01 Notice. Any notice, authorization, request, or demand required or permitted to be given hereunder, shall be in writing and shall be deemed to have been duly given when mailed by registered or certified mail, postage prepaid, addressed as follows:

To the Escrow Agent:	Regions Bank 3773 Richmond Avenue, Suite 1100 Houston, Texas 77046 Attention: Corporate Trust
----------------------	--

To the Issuer: Central Texas Regional Mobility Authority  
3300 N IH-35, Suite 300  
Austin, Texas 78705  
Attention: Chief Financial Officer

To the Rating Agencies: Moody's Investors Service, Inc.  
99 Church Street  
New York, New York 10007-2796  
  
Standard & Poor's Rating Group  
55 Water Street  
New York, New York 10041

Receipt of delivery of courier service or the United States Post Office registered or certified mail receipt showing delivery of the aforesaid shall be conclusive evidence of the date and fact of delivery. Either party hereto may change the address to which notices are to be delivered by giving to the other party not less than ten (10) days prior notice thereof.

Section 8.02 Termination of Responsibilities. Upon the taking of all the actions as described herein by the Escrow Agent, the Escrow Agent shall have no further obligations or responsibilities hereunder to the Issuer, the owners of the Refunded Obligations or to any other person or persons in connection with this Agreement.

Section 8.03 Binding Agreement. This Agreement shall be binding upon the Issuer and the Escrow Agent and their respective successors and legal representatives, and shall inure solely to the benefit of the owners of the Refunded Obligations, the Issuer, the Escrow Agent and their respective successors and legal representatives.

Section 8.04 Severability. In case any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provision of this Agreement, but this Agreement shall be construed as if such invalid or illegal or unenforceable provision had never been contained herein. In the event any one or more provisions hereof are held to be invalid, illegal or unenforceable the Issuer shall promptly notify each of the rating agencies then maintaining a rating on the Refunded Obligations.

Section 8.05 Texas Law Governs. This Agreement shall be governed exclusively by the provisions hereof and by the applicable laws of the State of Texas.

Section 8.06 Time of the Essence. Time shall be of the essence in the performance of obligations from time to time imposed upon the Escrow Agent by this Agreement.

Section 8.07 Effective Date of Agreement. This Agreement shall be effective upon receipt by the Escrow Agent of the funds described in Exhibit C-1 and Exhibit C-2 attached hereto and the Defeasance Securities, together with the specific sum stated in subsection (a) of Section 7.03 for Escrow Agent and paying agency fees, expenses, and services.

Section 8.08 Modification of Agreement. This Agreement shall be binding upon the Issuer and the Escrow Agent and their respective successors and legal representatives and shall

inure solely to the benefit of the holders of the Refunded Obligations, the Issuer, the Escrow Agent and their respective successors and legal representatives. Furthermore, no alteration, amendment or modification of any provision of this Agreement (1) shall alter the firm financial arrangements made for the payment of the Refunded Obligations or (2) shall be effective unless (i) prior written consent of such alteration, amendment or modification shall have been obtained from the holders of all Refunded Obligations outstanding at the time of such alteration, amendment or modification and (ii) such alteration, amendment or modification is in writing and signed by the parties hereto; provided, however, the Issuer and the Escrow Agent may, without the consent of holders of the Refunded Obligations, amend or modify the terms and provisions of this Agreement to cure in a manner not adverse to the holders of the Refunded Obligations any ambiguity, formal defect or omission in this Agreement. Prior notice of any such modification shall be given to each rating agency then maintaining a rating on the Refunded Obligations.

Section 8.09 Compliance with Texas Government Code. (a) The Escrow Agent hereby verifies that it and its parent company, wholly- or majority-owned subsidiaries, and other affiliates, if any, do not boycott Israel and, to the extent this Agreement is a contract for goods or services, will not boycott Israel during the term of this Agreement. The foregoing verification is made solely to comply with Section 2271.002, Texas Government Code, and to the extent such Section does not contravene applicable Federal law. As used in the foregoing verification, “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. The Escrow Agent understands “affiliate” to mean an entity that controls, is controlled by, or is under common control with the Escrow Agent and exists to make a profit.

(b) The Escrow Agent represents that neither it nor any of its parent company, wholly- or majority-owned subsidiaries, and other affiliates is a company identified on a list prepared and maintained by the Texas Comptroller of Public Accounts under Section 2252.153 or Section 2270.0201, Texas Government Code, and posted on any of the following pages of such officer’s internet website:

<https://comptroller.texas.gov/purchasing/docs/sudan-list.pdf>,  
<https://comptroller.texas.gov/purchasing/docs/iran-list.pdf>,  
<https://comptroller.texas.gov/purchasing/docs/fto-list.pdf>.

The foregoing representation is made solely to comply with Section 2252.152, Texas Government Code, and to the extent such Section does not contravene applicable Federal law and excludes the Escrow Agent and each of its parent company, wholly- or majority-owned subsidiaries, and other affiliates, if any, that the United States government has affirmatively declared to be excluded from its federal sanctions regime relating to Sudan or Iran or any federal sanctions regime relating to a foreign terrorist organization. The Escrow Agent understands “affiliate” to mean any entity that controls, is controlled by, or is under common control with the Escrow Agent and exists to make a profit.

(c) To the extent this Agreement constitutes a contract for goods or services for which a written verification is required under Section 2274.002, Texas Government Code (as added by Senate Bill 13, 87th Texas Legislature, Regular Session) as amended, the Trustee



hereby verifies that it and its parent company, wholly- or majority- owned subsidiaries, and other affiliates, if any, do not boycott energy companies and will not boycott energy companies during the term of this Agreement. The foregoing verification is made solely to comply with Section 2274.002, Texas Government Code, as amended, to the extent Section 2274.002, Texas Government Code does not contravene applicable Texas or Federal law. As used in the foregoing verification, “boycott energy companies” shall have the meaning assigned to the term “boycott energy company” in Section 809.001, Texas Government Code. The Escrow Agent understands “affiliate” to mean an entity that controls, is controlled by, or is under common control with the Escrow Agent and exists to make a profit.

(d) To the extent this Agreement constitutes a contract for the purchase of goods or services for which a written verification is required under Section 2274.002, Texas Government Code (as added by Senate Bill 19, 87th Texas Legislature, Regular Session, “SB 19”), as amended, the Escrow Agent hereby verifies that it and its parent company, wholly- or majority-owned subsidiaries, and other affiliates, if any,

(1) do not have a practice, policy, guidance or directive that discriminates against a firearm entity or firearm trade association; and

(2) will not discriminate during the term of this Agreement against a firearm entity or firearm trade association.

The foregoing verification is made solely to comply with Section 2274.002, Texas Government Code, as amended, to the extent Section 2274.002, Texas Government Code does not contravene applicable Texas or Federal law. As used in the foregoing verification, “discriminate against a firearm entity or firearm trade association” shall have the meaning assigned to such term in Section 2274.001(3), Texas Government Code (as added by SB 19). The Escrow Agent understands “affiliate” to mean an entity that controls, is controlled by, or is under common control with the Escrow Agent and exists to make a profit.

## ARTICLE IX REDEMPTION OF REFUNDED OBLIGATIONS

Section 9.01 Redemption of Refunded Obligations. The Issuer has irrevocably exercised its option to call the Refunded Obligations for redemption, prior to maturity, on the dates and at the redemption prices set forth on Exhibit A-1 and Exhibit A-2 hereto. Such redemption shall be carried out in accordance with the Master Indenture and the supplemental trust indenture pursuant to which each series of Refunded Obligations were issued. The Escrow Agent is hereby authorized to provide funds therefor as set forth in Section 3.02 hereof.

Section 9.02 Notice of Redemption. In its capacity as trustee under the Master Indenture, the Escrow Agent is hereby authorized and directed to give notice of defeasance and notice of redemption, as applicable, to the registered owners of the Refunded Obligations in the form and manner prescribed in the Master Indenture and the respective supplemental trust indenture pursuant to which the Refunded Obligations were issued. By its execution and delivery hereof, the Escrow Agent, as trustee under the Master Indenture, hereby acknowledges receipt of notice of redemption of the Refunded Obligations.

[Execution Page Follows]

IN WITNESS WHEREOF, this Agreement has been executed in multiple counterparts, each one of which shall constitute one and the same original Agreement, as of the date and year appearing on the first page of this Agreement.

CENTRAL TEXAS REGIONAL MOBILITY  
AUTHORITY

By: \_\_\_\_\_  
Authorized Officer

REGIONS BANK, as Escrow Agent

By: \_\_\_\_\_  
Title: \_\_\_\_\_

## **INDEX TO EXHIBITS**

- Exhibit A-1 Description of Series 2015A Refunded Bonds
- Exhibit A-2 Description of Series 2016 Refunded Bonds
- Exhibit B-1 Schedule of Debt Service on Series 2015A Refunded Bonds
- Exhibit B-2 Schedule of Debt Service on Series 2016 Refunded Bonds
- Exhibit C-1 Description of Beginning Cash Balance and Defeasance Securities – Series 2015A Refunded Bonds Escrow Fund
- Exhibit C-2 Description of Beginning Cash Balance and Defeasance Securities– Series 2016 Refunded Bonds Escrow Fund
- Exhibit D-1 Escrow Fund Cash Flow - Series 2015A Refunded Bonds Escrow Fund
- Exhibit D-2 Escrow Fund Cash Flow - Series 2016 Refunded Bonds Escrow Fund
- Exhibit E Reinvestments in Zero Interest Rate SLGS

**EXHIBIT A-1**

**DESCRIPTION OF SERIES 2015A REFUNDED BONDS**

(See attached schedules)

**EXHIBIT A-2**

**DESCRIPTION OF SERIES 2016 REFUNDED BONDS**

(See attached schedules)

**EXHIBIT B-1**

**SCHEDULE OF DEBT SERVICE ON SERIES 2015A REFUNDED BONDS**

(See attached schedules)

**EXHIBIT B-2**

**SCHEDULE OF DEBT SERVICE ON SERIES 2016 REFUNDED BONDS**

(See attached schedules)



**EXHIBIT C-1**

**DESCRIPTION OF BEGINNING CASH BALANCE AND DEFEASANCE SECURITIES  
– SERIES 2015A REFUNDED BONDS ESCROW FUND**

I. Cash

\$ \_\_\_\_\_

II. State and Local Government Series Obligations

\$ \_\_\_\_\_

III. Open Market Securities

\$ \_\_\_\_\_

**EXHIBIT C-2**

**DESCRIPTION OF BEGINNING CASH BALANCE AND DEFEASANCE SECURITIES  
– SERIES 2016 REFUNDED BONDS ESCROW FUND**

I. Cash

\$ \_\_\_\_\_

II. State and Local Government Series Obligations

\$ \_\_\_\_\_

III. Open Market Securities

\$ \_\_\_\_\_

**EXHIBIT D-1**

**ESCROW FUND CASH FLOW -  
SERIES 2015A REFUNDED BONDS ESCROW FUND**

(See attached schedules)

**EXHIBIT D-2**

**ESCROW FUND CASH FLOW -  
SERIES 2016 REFUNDED BONDS ESCROW FUND**

(See attached schedules)

**EXHIBIT E**

**REINVESTMENTS IN ZERO INTEREST RATE SLGS**

None



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

## September 29, 2021 AGENDA ITEM #9

---

Discuss and consider approving a contract with Deloitte Consulting LLP for continued development of the data platform and associated transaction routing and system interfaces to support toll transaction management

Strategic Plan Relevance:	Explore and Invest in Transformative Technology and Adopt Industry Best Practices; Deliver Multi-faceted Mobility Solutions; Invest in Effort that Extends Beyond Roadways
Department:	Operations
Contact:	Tracie Brown, Director of Operations
Associated Costs:	\$2,069,364
Funding Source:	183A Phase III Other Project funds
Action Requested:	Consider and act on draft resolution

**Project Description/Background:** Toll transaction management is a critical business process area within a tolling agency. The process begins when a vehicle travelling on a toll agency maintained and operated toll road passes through a toll gantry. Equipment at the toll gantry captures a suite of data that uniquely identifies the toll transaction. This data includes an image of the license plate used to extract the license plate number and state, vehicle axles, or class, date/time, location, and transponder device information. The resulting data set serves as inputs necessary to determine the toll amount, the individual responsible for paying the toll, and the payment path used to submit a request for payment. Additionally, toll transaction data is used for traffic and customer pattern analysis, monitoring and validation of toll system performance and accuracy, revenue and financial analysis, and other data points for the toll agency to make informed business decisions.

The Mobility Authority currently uses an outsourced solution developed by Kapsch TrafficCom to handle the end-to-end toll transaction management processes and workflow. To provide more flexibility in the future, in March 2021, the Mobility

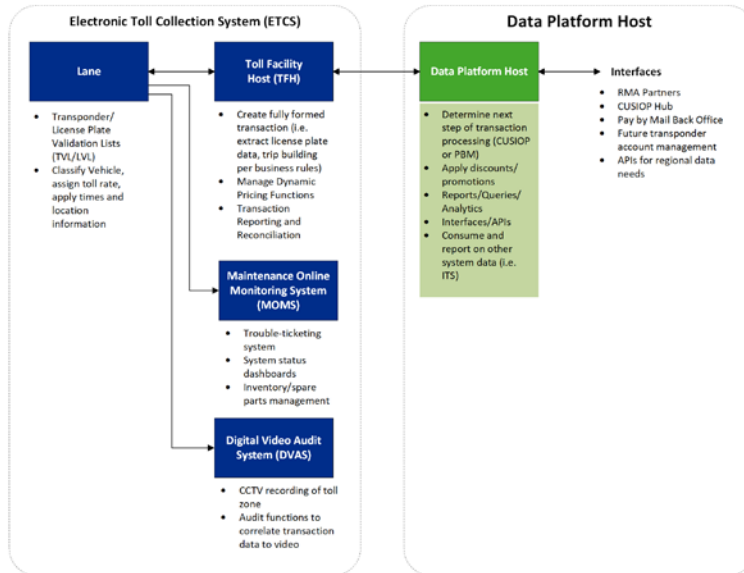
Authority awarded a contract to Deloitte Consulting LLP to begin development of the data platform to move to a stratagem wherein all toll transaction processing and data management capabilities after the point of transaction creation is advanced to a Mobility Authority-managed solution. A third-party vendor would continue to collect and create the toll transaction data set at the roadside, then pass the toll transaction data to the data platform within the Mobility Authority's network. The new approach gives the Mobility Authority more control of the data which will lead to better informed decision-making.

#### *The Data Platform Project Explained*

The objective of the data platform project is to transition all toll transaction data processing and data management capabilities after the point of transaction creation to a Mobility Authority-managed solution. A third-party vendor will continue to collect and create the toll transaction at the roadside, then pass the fully formed toll transaction to the data platform. Business logic and rules will then consume the transaction and route the payment request to either the Central United States Interoperability (CUSIOP) Hub or the Pay by Mail (PBM) vendor.

The Mobility Authority-managed data platform will also support additional business capabilities such as external reporting and internal data analytics. A connection to the Texas Department of Motor Vehicles' datasets will enable the Mobility Authority to better understand its customer base and their travel habits. Future development could include adding promotions and discount program logic.

This new configuration is depicted below.



The Data Platform Project is a component of the Mobility Authority’s *Roadway Technology Plan*. The *Roadway Technology Plan* is part of a larger initiative to modernize the Mobility Authority’s toll and roadway technology systems, and to thoughtfully expand the use of technology to maximize road capacity. The *Roadway Technology Plan* was first presented to the Mobility Authority’s Board at its February 2020 meeting.

# Mobility Innovation Roadmap

INNOVATION BRIEF

### Moving Forward

Innovation is not a means to an end, but a set of goals, tools and methods that lead us on a path to work better and differently using new ideas, processes and technology. CTRMA’s new positions, processes and innovation strategy in place signal an embrace of technology and a

Technology Plan \*Status: ● Planning Stage ◐ In Progress ● Complete

Technology Plan	Target Innovation Goal	Status
Technology Plan (Backoffice / Data Platform)	Efficiency & Safety	●
Roadway Technology Plan (Cameras, sensors, communications, incident detection, wrongway detection, etc.)	Efficiency & Safety	◐
Toll Systems Integrator	Efficiency	◐
Roadway Technology Integrator	Efficiency & Safety	◐
Integrated Real Time Data and Predictive Services	Efficiency & Safety	◐
Data Sharing Platform	Efficiency	◐
Traffic Management Center Expansion	Efficiency & Safety	◐

Business Improvements



### The Solution Approach

To achieve the new transaction processing arrangement, the Mobility Authority defined a multi-faceted strategic plan to implement an end-to-end scalable tolling transaction system to meet current and future business capabilities. This architecture design provides solutions for:

- Centralized, secure, and redundant data hosting for all data entities owned by the Mobility Authority and necessary for toll transaction processing;
- External data exchange points that provide flexible structured transaction data transmissions to and from third parties such as service providers, universities, or research institutions;
- Multi-step modular pricing and discounting business logic;
- Auditable data governance and security;
- User driven self-service data updates and business process administration; and
- Public, external, and internal reporting.

The Mobility Authority has chosen a modular approach to complete the Data Platform Project. Development for Release 1 and 2 will complete in September 2021 on schedule. The current recommendation is related to development for Release 3.

- Release 1 established the platform.
- Release 2 created the routing and exchange processes.
- Release 3 supports development for pricing and billing transactions, defines how data governance is handled in the new processing schema, and will identify the suite of reports necessary to account for the agency's revenue and monitor performance.
- Release 4 will define promotions and discount programs, and provide reporting and analytics for secure internal and external data access.

A Statement of Work (SOW) for Data Platform Release 3 was developed, in a format matching that outlined by Texas Department of Information Resources (DIR), and released to Deloitte Consulting LLP in July 2021. Deloitte responded to the SOW in August 2021. After additional discussions, Deloitte submitted an updated response in September 2021.

**The total not to exceed cost for development of Releases 3 is \$2,069,364.** This includes a 10% project contingency as outlined below.

Release 3	\$ 1,881,240
Project Contingency	\$188,124
<b>TOTAL PROJECT COST</b>	<b>\$ 2,069,364</b>

**Previous Actions & Brief History of the Program/Project:**

The initial contract with Deloitte was awarded by the Mobility Authority’s Board of Directors in February 2021; the contract with Deloitte was approved by the Board of Directors in March 2021. Completion of the work provided by Deloitte related to Releases 1 and 2 is planned to complete on time on September 17, 2021. The purchase of additional software, hardware and hosting in support of the agreed upon scope has been estimated and partially completed.

**Financing:** 183A Phase III Other Project funds

**Action requested/Staff Recommendation:** Staff recommends contracting with Deloitte Consulting LLP for continued development of a data platform with the scope identified as Release 3 through their contract with the Texas Department of Information Resources. Pursuant to Government Code Section 2054.0565 and the Mobility Authority Policy Code, use of the DIR contract with Deloitte Consulting LLP satisfies all competitive purchasing requirements.

**Backup provided:** Draft Resolution  
Deloitte Consulting Release 3 Response  
Data Platform Release 3 Scope of Work

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

**RESOLUTION NO. 21-0XX**

**APPROVING A CONTRACT WITH DELOITTE CONSULTING LLP  
FOR CONTINUED DEVELOPMENT OF A DATA PLATFORM AND ASSOCIATED  
TRANSACTION ROUTING AND SYSTEM INTERFACES TO SUPPORT TOLL  
TRANSACTION MANAGEMENT**

WHEREAS, Mobility Authority staff is developing a data platform to transition all toll transaction data processing and data management capabilities after the point of transaction creation from a third-party vendor to the Mobility Authority (the “Data Platform Project”); and

WHEREAS, a Mobility Authority managed data platform will support new business capabilities such as external reporting, data analytics and a connection to the Texas Department of Motor Vehicles’ datasets to allow better informed agency decision making; and

WHEREAS, by Resolution No. 21-018, dated March 31, 2021, the Board of Directors approved a contract with Deloitte Consulting LLP for the first phase of the Data Platform Project to establish the data platform and create the routing and exchange processes; and

WHEREAS, the Executive Director has negotiated a scope of work for the next phase of the Data Platform Project to support development for pricing and billing transactions, define how data governance is handled in the new processing schema, and identify the suite of reports necessary to account for the Mobility Authority’s revenue and monitor performance which is attached hereto as Exhibit A; and

WHEREAS, Deloitte Consulting LLP has submitted pricing for the next phase of the Data Platform Project which is attached hereto as Exhibit B; and

WHEREAS, Deloitte Consulting LLP currently provides services to the State of Texas through Texas Department of Information Resources (DIR) Contract No. #DIR-TSO-431

WHEREAS, pursuant to Texas Government Code Section 2054.0565 and Mobility Authority Policy Code Section 401.008, the Mobility Authority may use the DIR contract with Deloitte Consulting LLP to implement the next phase of the Data Platform Project; and

WHEREAS, the Executive Director recommends entering into an agreement with Deloitte Consulting LLP for continued development of the Data Platform Project in a total amount not to exceed \$2,069,364, including contingency, through their DIR cooperative contract.

NOW THEREFORE BE IT RESOLVED that the Board of Directors hereby approves the scope of work and pricing for the next phase of the Data Platform Project which are attached hereto as Exhibit A and Exhibit B, respectively; and

BE IT FURTHER RESOLVED, that the Executive Director is authorized to enter into an agreement with Deloitte Consulting LLP in a total amount not to exceed \$2,069,364, including contingency, through their contract with the Texas Department of Information Resources for continued development of the Data Platform Project.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 29<sup>th</sup> day of September 2021.

Submitted and reviewed by:

Approved:

---

Geoffrey Petrov, General Counsel

---

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

**Exhibit A**



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

## **Statement of Work**

### **Data Platform Release 3 Requirements**

*Technology Upgrade/Migration Transformation*

**July 6, 2021**

---

List of Figures .....	3
List of Tables.....	3
List of Appendices .....	3
1. Introduction .....	4
2. Background .....	5
2.1. Roadmap.....	7
3. Data Platform Release 3 Requirements Scope .....	8
3.1. Tolling Product Management .....	8
3.2. Discount Management.....	8
3.3. Invoice Management .....	8
3.4. Data Exchange Management .....	8
3.5. Reporting Cache & Reporting Management.....	9
3.6. Data Governance & SOC 2 Compliance.....	9
3.7. IT Enterprise Management .....	9
4. Deliverables.....	9
5. Project Management Requirements.....	10
6. Acceptance Criteria .....	11
7. Period of Performance.....	11
8. Invoices .....	12
9. CTRMA Provided Services .....	12
10. Location of Work, Hours and Conditions .....	12
11. Additional Terms and Conditions.....	12
11.1. Development and Testing Environments.....	13
11.2. Compliance with CTRMA Information Security Guidelines .....	13
12. Process Details .....	13
12.1. Submittal Format .....	13
12.2. Page Limits/Fonts.....	14
12.3. Section Headings.....	14
12.4. Contact Information.....	14
13. Vendor Response .....	14
13.1. Staff Capabilities .....	14
13.2. Relevant Experience and References.....	15
13.3. Project Work Plan .....	15

13.4. Additional Considerations..... 15

13.5. Trust Services Criteria ..... 15

13.6. Financial Ability to Implement Project..... 16

14. Pricing..... 16

15. Schedule of Events and Response Guidelines..... 16

15.1. Questions and Answers..... 17

16. Response Submission Requirements ..... 17

Appendix B ..... 16-1

Conflict of Interest Disclosure Statement..... 16-1

Appendix C ..... 16-1

CTRMA Information Security Policy ..... 16-1

Appendix D..... 16-1

Trust Services Criteria ..... 16-1

**List of Figures**

Figure 1-1: ETCS vs. Data Platform Host ..... 4

Figure 2-1: Strategic Goals ..... 6

Figure 2-2: Data Platform Modular Approach ..... 6

**List of Tables**

Table 15-1: Planned Schedule of Events ..... 16

Table 16-1: SOW Response Submittal Requirements..... 17

**List of Appendices**

Appendix A: Table of Acronyms ..... A-1

Appendix B: Conflict of Interest Disclosure ..... B-1

Appendix C: CTRMA Information Security Policy..... C-1

Appendix D: Trust Services Criteria..... D-1

Appendix E: Pricing Form ..... E-1



# 1. Introduction

The Central Texas Regional Mobility Authority (CTRMA) seeks Texas Department of Information Resources (TxDIR) Vendors or teams (individually or collectively, the Vendors) to provide data platform services included in Data Platform Release 3 Requirements, as more fully described in Section 3. This Statement of Work (SOW) does not include items in the Electronic Toll Collections System (ETCS).

The delineation of services is shown in Figure 1-1 below.

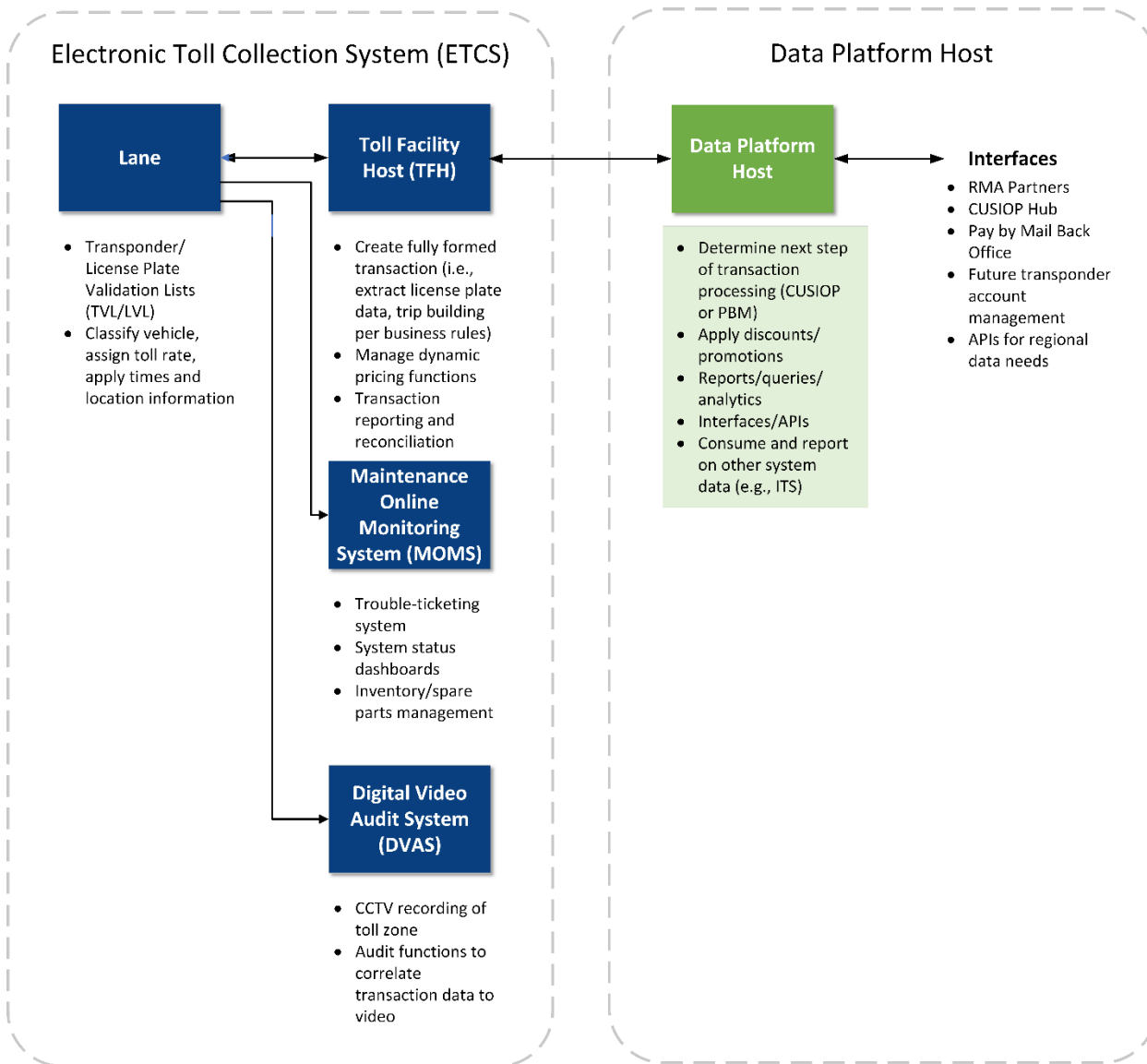


Figure 1-1: ETCS vs. Data Platform Host

## 2. Background

Toll transaction management is a critical business process area within a tolling agency. The process is triggered when a vehicle travelling on a toll agency maintained and operated toll road passes through a toll gantry. Equipment at the toll gantry captures a suite of data that uniquely identifies the toll transaction. This data includes an image of the license plate used to extract the license plate number and state, vehicle axles, or class, date/time, location, and Automatic Vehicle Identification (AVI) transponder device information. The resulting data set serves as inputs necessary to determine the toll amount, the individual responsible for paying the toll and the payment path used to submit a request for payment. Additionally, toll transaction data is used for traffic and customer pattern analysis, monitoring and validation of toll system performance and accuracy, revenue and financial analysis, and other data points for the toll agency to make informed business decisions.

In the current-state, CTRMA has deployed an outsourced solution to handle the end-to-end toll transaction management processes and workflow. The objective of this program is to transition all toll transaction data processing and data management capabilities after the point of toll transaction creation to a CTRMA-managed solution. A third-party vendor will continue to collect and create the toll transaction data set at the roadside, then pass the toll transaction data to a data platform within the CTRMA network. CTRMA business logic and rules will then consume the transaction data to price and route the payment request. The data platform will require additional data sets such as the Texas Department of Motor Vehicles (Texas DMV) database and the Central United States Interoperability Hub (CUSIOP Hub) data to properly route the toll transaction and complete the process. The resulting CTRMA-managed data platform will also support additional business capabilities such as external reporting and internal data analytics.

To achieve this objective, CTRMA has defined a multi-faceted strategic plan to implement an end-to-end scalable tolling transaction system to meet current and future business capabilities. Using a Service Oriented Architecture (SOA) approach, the CTRMA developed a back-office architecture design that provides solutions for:

- Centralized, secure, and redundant data hosting for all data entities necessary for toll transaction processing
- External data exchange points that provide flexible structured transaction data transmissions to and from third parties
- Multi-step modular pricing and discounting business logic
- Auditable data governance and security
- UX/UI-driven data and business process administration
- Public, external, and internal fixed reporting and cached data access



Figure 2-1: Strategic Goals

Key Features:

Data Platform

- Design and deployment of all internally managed data sources (master record)
- Send and receive data exchanges (flat file and API solutions)
- Data Governance (Use, Retention, Recovery)

Routing and Exchanges

- Automated Payor identification and transaction payment request routing

Reporting and Analytics

- Public, Internal and External tools, and files

Invoicing and Pricing

- Adjusted and Discount rate design and automation

To accomplish this objective, CTRMA has chosen to scope the releases to support a modular approach. Figure 2-2 below illustrates the linear process in scope and the planned release number for each capability area.

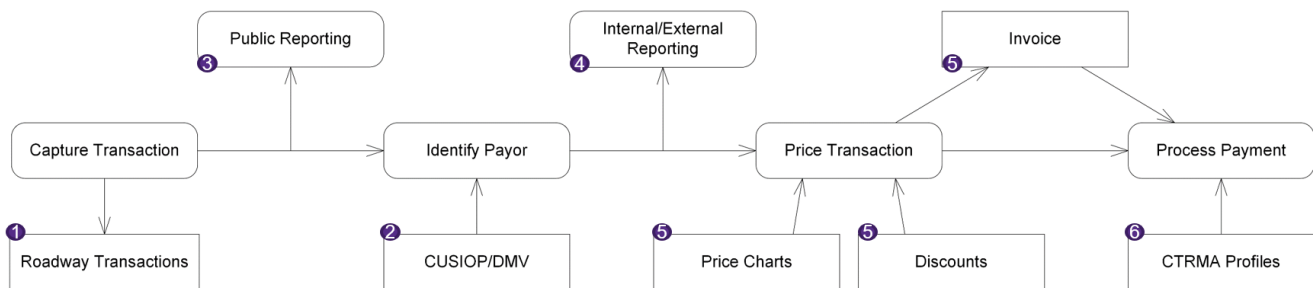


Figure 2-2: Data Platform Modular Approach

## 2.1. Roadmap

CTRMA has organized the program into multiple releases spanning several calendar years. The current program includes a total of four (4) releases in scope. This SOW is scoped to include Data Platform Release 3 Requirements.

Release	Release 1 & 2 (Combined)		Release 3		Release 4
Portfolios	1 Establish Platform	2 Routing & Exchanges	3 Pricing & Invoicing	4 Data Governance	5 Reporting
<b>Work Streams</b>	<ul style="list-style-type: none"> <li>Roadway Transaction Data</li> <li>Data Transformation</li> <li>Periodic SLA Review</li> </ul>	<ul style="list-style-type: none"> <li>CUSIOP DB &amp; TCS</li> <li>Transaction Routing</li> <li>Transaction Exchanges</li> </ul>	<ul style="list-style-type: none"> <li>Product Management</li> <li>Discount Program</li> <li>Pricing &amp; Invoicing</li> </ul>	<ul style="list-style-type: none"> <li>Reporting Data Cache</li> <li>Data Governance</li> <li>DMV</li> </ul>	<ul style="list-style-type: none"> <li>External Reporting</li> <li>Internal Reporting</li> <li>Reporting &amp; Analytics</li> </ul>
<b>Projects</b>	<ul style="list-style-type: none"> <li>Data Platform Solution</li> <li>Toll Transaction Database(s)</li> <li>Roadway Transaction Data</li> <li>Data Transformation</li> <li>Roadway Data SLA Monitoring</li> </ul>	<ul style="list-style-type: none"> <li>CUSIOP Database(s)</li> <li>Source Data Exchange &amp; Transformation</li> <li>Exemp. Vets. Habits. datasources &amp; (UI/UX)</li> <li>Transaction Routing Logic, Rules, &amp; Price Adjustments</li> <li>IOP Exchange</li> <li>PBM Exchange</li> <li>Current TCS Exchange</li> <li>Future TCS Exchange</li> </ul>	<ul style="list-style-type: none"> <li>Transaction Operations Management Solution (TOMS)</li> <li>Product Management Strategy</li> <li>Product Database(s)</li> <li>Product Pricing Process</li> <li>Discount Program Strategy</li> <li>Discount Program Database(s)</li> <li>Discount Pricing Process</li> <li>Discount Program Marketing &amp; Communication</li> <li>Invoice Database(s)</li> <li>Automated Invoicing Logic</li> <li>Invoice Data Exchanges</li> </ul>	<ul style="list-style-type: none"> <li>DMV DB</li> <li>DMV Exchange</li> <li>Reporting Cache Platform Solution</li> <li>Public Reporting Data Exchanges</li> <li>Public Report Generation</li> <li>Public Data Reporting</li> <li>Data Governance - Strategy</li> <li>Data Governance Solution – Data Use</li> <li>Data Governance – Availability</li> <li>Data Governance - Policies &amp; Education</li> </ul>	<ul style="list-style-type: none"> <li>External Data Reporting Database(s)</li> <li>Internal Data Reporting Database(s)</li> <li>External Reporting Data Exchanges</li> <li>Report Generation</li> <li>Internal &amp; External Data Exchange</li> <li>Internal Reporting &amp; Analytics Tool(s)</li> </ul>
<b>Key Outcomes</b>	<ul style="list-style-type: none"> <li>Data Platform Environment</li> <li>Internal Roadway Transaction Data</li> <li>SLA-driven quality</li> </ul>	<ul style="list-style-type: none"> <li>Transaction &amp; Payment Path routing</li> <li>IOP Exchange</li> <li>PBM Exchange</li> <li>Tolling Exchange (TCS)</li> <li>Other Exchanges</li> </ul>	<ul style="list-style-type: none"> <li>Internal pricing controls</li> <li>Transaction Operations Management</li> <li>Discount programs</li> <li>Consistent invoicing</li> <li>Transaction Processing Independence</li> </ul>	<ul style="list-style-type: none"> <li>Fixed &amp; Dynamic Reporting*</li> <li>Data governance</li> <li>SOC 2 Compliance</li> </ul>	<ul style="list-style-type: none"> <li>Internal &amp; external data access*</li> <li>Data Governance</li> <li>Public data availability</li> </ul>

### 3. Data Platform Release 3 Requirements Scope

#### 3.1. Tolling Product Management

- 3.1.1. Development and deployment of Product database(s) and relationships
- 3.1.2. Design and development of automated Product Management process(es)
  - 3.1.1.1. Manage Tolling Product Types
  - 3.1.1.2. Manage Tolling Products
  - 3.1.1.3. Manage Tolling Product Items
  - 3.1.1.4. Manage Tolling Product Pricing (Base Price, Price Window Hierarchy, and Business Rules)
- 3.1.3. Development of automated business process(es) for payor ID and payment path routing logic
  - 3.1.2.1. Manage Tolling Price Adjustments

#### 3.2. Discount Management

- 3.2.1. Development and deployment of Discount database(s) and relationships
- 3.2.2. Design and development of automated Discount Management process(es)
  - 3.1.3.1. Manage Tolling Discount Types (Active & Passive)
  - 3.1.3.2. Manage Tolling Discount Programs (Veterans, Student, Frequency, Members, Holiday, et al)
  - 3.1.3.3. Manage Tolling Discounts (Discount Price, Discount Window Hierarchy, and Business Rules)
- 3.2.3. Integration of Discount Management with Product Management processes

#### 3.3. Invoice Management

- 3.3.1. Development and deployment of Invoice database(s) and relationships
- 3.3.2. Design and development of automated Invoice Management process(es)
  - 3.1.4.1. Manage Invoices
- 3.3.3. Integration of Invoice Management with Product and Discount Management

#### 3.4. Data Exchange Management

- 3.4.1. Design, development, and testing for Pay by Mail('PBM') Invoice data exchange modifications (Fixed file, API, XML, JSON)
- 3.4.2. Design, development, and testing for IOP Hub Invoice data exchange modifications (Fixed file, API, XML, JSON)
- 3.4.3. Development of DMV Hub database(s) and relationships
- 3.4.4. Design, development, and testing for external DMV Hub data exchanges (Fixed file, API, XML, JSON)
- 3.4.5. Design, development, and testing for Public Reporting data exchange (Fixed file, API, XML, JSON, GitHub)

### **3.5. Reporting Cache & Reporting Management**

- 3.5.1. Development of Reporting Cache data platform
- 3.5.2. Development of Public Reporting database(s) and relationships
- 3.5.3. Implementation and testing of Public Reporting data push from master data source to Reporting Cache
  - 3.5.3.1. Manage Reporting Cache
- 3.5.4. Development of automated Public Report(s) generation
  - 3.5.4.1. Manage Public Reporting
- 3.5.5. End-to-end testing of Reporting Cache and Public Reporting exchange solutions
  - 3.5.5.1. Manage Public Reporting Data Exchange(es) (API, Fixed File, GitHub)

### **3.6. Data Governance & SOC 2 Compliance**

- 3.6.1. SOC 2 Risk Objectives, Control Objectives, and Policies
- 3.6.2. SOC 2 Compliance Processes & Procedures
- 3.6.3. Support for establishment of Data Governance strategy and approach
- 3.6.4. Definition of Data Use criteria
- 3.6.5. Automation of Data Governance process(es) including Certification and Attestation for data use
- 3.6.6. Documentation of Data Use Governance Policies & Procedures
- 3.6.7. Development of Data Governance Awareness training, compliance, and certification
- 3.6.8. Declaration and implementation of Data Governance Audit(s)

### **3.7. IT Enterprise Management**

- 3.7.1. Policies & Procedures documentation
- 3.7.2. Revision of Source Data Entity Catalog
- 3.7.3. Data Platform IT Service Catalog(s) and Service Level definition & documentation

## **4. Deliverables**

Deliverables must be provided on the dates specified in Section 13.3. Any changes to the delivery date must have prior approval (in writing) by the Data Platform Program Manager or designee. All deliverables must be submitted in a format approved by the Data Platform Program Manager.

If the deliverable cannot be provided within the scheduled timeframe, the Vendor is required to contact the Data Platform Program Manager in writing with a reason for the delay and the proposed revised schedule. The request for a revised schedule must include the impact on related tasks and the overall project.

A request for a revised schedule must be reviewed and approved by the Data Platform Program Manager before placed in effect. Contract Terms and Conditions may dictate remedies, costs, and other actions based on the facts related to the request for a revised schedule. CTRMA will complete a review of each submitted deliverable within fourteen (14) days from the date of receipt.

The required *Production-Ready* deliverables for Data Platform Release 3 Requirements include:

- Development and deployment of Product database(s) and relationships
- Design and development of automated Product Management process(es)
- Development of automated business process(es) for payor ID and payment path routing logic
- Development and deployment of Discount database(s) and relationships
- Design and development of automated Discount Management process(es)
- Integration of Discount Management with Product Management processes
- Development and deployment of Invoice database(s) and relationships
- Design and development of automated Invoice Management process(es)
- Integration of Invoice Management with Product and Discount Management
- Design, development, and testing for Pay by Mail('PBM') Invoice data exchange modifications (Fixed file, API, XML, JSON)
- Design, development, and testing for IOP Hub Invoice data exchange modifications (Fixed file, API, XML, JSON)
- Development of DMV Hub database(s) and relationships
- Design, development, and testing for external DMV Hub data exchanges (Fixed file, API, XML, JSON)
- Design, development, and testing for Public Reporting data exchange (Fixed file, API, XML, JSON, GitHub)
- Development of Reporting Cache data platform
- Development of Public Reporting database(s) and relationships
- Implementation and testing of Public Reporting data push from master data source to Reporting Cache
- Development of automated Public Report(s) generation
- End-to-end testing of Reporting Cache and Public Reporting exchange solutions
- SOC 2 Risk Objectives, Control Objectives, and Policies
- SOC 2 Compliance Processes & Procedures
- Support for establishment of Data Governance strategy and approach
- Definition of Data Use criteria
- Automation of Data Governance process(es) including certification and affirmation for data use
- Documentation of Data Governance Policies & Procedures
- Development of Data Governance Awareness training, compliance, and certification
- Declaration and implementation of Data Governance Audit(s)
- Policies & Procedures documentation
- Revision of Source Data Entity Catalog
- Data Platform IT Service Catalog(s) and Service Level definition & documentation

## 5. Project Management Requirements

Vendor personnel will ordinarily perform services under the direction of the CTRMA Data Platform Program Manager. Such interaction will normally be limited to ensuring that deliverables meet the requirements, periods of Releases, reviewing and approving of all invoices, contract compliance, and coordinating the Vendor's access to needed CTRMA resources and information.

The Vendor shall ensure that the Release is effectively and efficiently managed to the mutual benefit of the Vendor and CTRMA. Vendor shall employ as necessary the personnel, personnel hours, tools, and systems to properly manage and deliver the project.

CTRMA considers an effective project management program to be capable of identifying and addressing program issues at the earliest opportunity to minimize or eliminate Change Orders and changes to the project plan or schedule. It is

therefore incumbent upon the Vendor to have an established and fully effective project management program in place at the initiation of the contract and be implemented for each Release.

For each Release, the Vendor shall designate a Project Manager (consistent Project Management Institute – Project Management Body of Knowledge (PMI-PMBOK) practices), subject to CTRMA approval, who shall be responsive to the needs of CTRMA as required by the contract. The Project Manager shall ensure that the project tasks are completed on time and within budget. The Project Manager shall keep CTRMA fully informed of the status of the project, shall promptly, and regularly notify CTRMA of any problems or difficulties that may affect the timely or effective completion of the task, milestone, or project. The Project Manager shall have full authority to assign task priority as required to meet the requirements of the Release project.

The Project Manager shall be competent and fully qualified in all aspects of the Release project. Removal or replacement of the Project Manager(s) by the Vendor shall only be with prior approval of CTRMA.

A Project Management Plan shall be submitted as part of each Release. The plan shall include a description of the management techniques, including the overall management, staffing, and measurable controls, used to meet the Data Platform Release 3 Requirements scope. The plan shall be reviewed and modified as necessary during the execution of the contract.

The CTRMA Data Platform Program Manager will determine the intervals and form for status reports at the time a Release is negotiated and occasionally may be requested ad-hoc. Each Release status report shall consist of a brief description of the project, progress, any problems, concerns or other issues that need to be addressed, expected activities during the next reporting period, and any other information deemed appropriate and relevant by the Vendor or requested by the CTRMA Data Platform Program Manager. It is anticipated weekly status meeting with the CTRMA Data Platform Manager will be required.

## **6. Acceptance Criteria**

For any Release assignment requiring hardware/software integration, development and/or installation, the Vendor shall develop an acceptance test plan and procedure to verify intended functionality, the completion of the deliverable milestones provided by the Vendor. Approval from CTRMA project management is required before proceeding.

Vendor shall work with CTRMA to perform the acceptance testing. Should any problems arise during the testing, the Vendor shall be responsible to make necessary corrections before CTRMA acceptance of the work. If the Vendor determines the problem is not caused by the Vendor supplied work, it shall provide CTRMA a detailed description of the problem and the reason why it is not caused by the Vendor's work. If CTRMA agrees the problem lies elsewhere, then CTRMA will provide the correction. After the correction, the acceptance test will be restarted until successful completion.

For deliverable milestones where production readiness is identified, the work product is fully developed, tested, and in the production environment. This includes any and all CTRMA policy requirements such as vulnerability scanning.

## **7. Period of Performance**

Data Platform Services Release 3 Requirements is expected to occur during Fall 2021 to early Summer 2022.



## 8. Invoices

The Vendor should invoice the CTRMA after each Payment Deliverable Milestone is accepted. CTRMA will not make partial payments for deliverable milestone subtasks. Payments will be made in accordance with Appendix A of the Contract.

## 9. 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

## 10. 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.

## 11. 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.

### **11.1. Development and Testing Environments**

Vendor shall be responsible for providing all development, sandbox, testing and pre-production environments during the duration of each release.

### **11.2. 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 C).

## **12. Process Details**

The procurement process outlined herein is in accordance with CTRMA's Policy Code and all other applicable rules and laws.

### **12.1. Submittal Format**

All Responses must be responsive to the general format and guidelines outlined within this SOW. A responsive submittal is one that:

- Follows the general guidelines of this SOW,
- Includes all documentation requested,
- Is submitted following the general format outlined herein,
- Displays sound justification for recommendations,

- Is submitted by the deadline, and
- Has the appropriate signatures as may be required.

Failure to comply may result in the Response being deemed non-responsive.

## 12.2. Page Limits/Fonts

Responses must not exceed page limits listed in Section 13 (8.5 x 11 inches with 1-inch margins from all sides), type font size not less than 11 points, and printed on one side. Response shall be submitted as a bound document and printed single-sided on standard 8½" x 11" paper. Graphics, charts, photographs, and/or exhibits may be on 11" x 17" paper but must be folded to the standard size; foldout pages count as one page.

The page limit does not include the cover letter (limited to one (1) page), front/back cover sheets, dividers, table of contents, résumés (limited to two (2) pages each), the Conflict of Interest Disclosure Statement (provided as Appendix B), or other items requested to be included in an appendix. Font sizes in graphics or attachments can be less than the body of the SOW Response but should be reasonably legible.

Materials submitted exceeding the page limits specified in Section 13 will not be reviewed.

## 12.3. Section Headings

Vendors should follow the outline in Section 13, using section headings and subheadings. Vendors should clearly identify each request being addressed and answer each specifically and succinctly. Please provide a response to every question or request for information identified. If no response is given, clearly explain why.

## 12.4. Contact Information

In the cover letter, include the name, phone number, and email address of the Vendor's designated point of contact.

# 13. Vendor Response

CTRMA will select the Vendor(s) that offers the best value as determined by the information provided in the Vendor's Response. The following information shall be provided in the Vendor's Response:

## 13.1. Staff Capabilities

- a. Brief history of the responding firm.
- b. Personnel and team. Vendor must demonstrate key personnel and staff roles possess the skills necessary to perform services outlined in this SOW.
  - i. For key personnel in leadership positions, provide the names and résumés of the consultants that Vendor is committing to this engagement.
  - ii. For staff roles, provide resume(s) of representative consulting resources that would staff each role should your firm be awarded this project.
- c. Corporate address.
- d. Other office locations and addresses.
- e. A summary of the firm's experience providing services for governmental entities for 2017, 2018, 2019, and to date.
- f. This section may not exceed ten (10) pages, excluding Vendor resumes.

### 13.2. Relevant Experience and References

- a. Provide a listing of at least three (3) relevant projects to substantiate the qualifications and experience requirements for similar services completed for three (3) years within the past five (5) years, including the following:
  - i. Project name and location
  - ii. Firm(s) and key staff who worked on the project
  - iii. Name, address, and telephone number of client contact. [The Vendor unconditionally authorizes CTRMA to contact and confer with the indicated client contact(s) and other current or past employees of that client. Input received may be considered as part of the scoring. A reasonable effort will be made to contact all references.]
  - iv. Relevant projects must be of similar size and scale. Similar size and scale is defined as demonstrated knowledge of transaction processing systems with a minimum of 50 million records and/or transactions processed annually.
- b. Provide a listing of any transaction processing contracts won in the last three (3) years with scheduled go-live dates and status of each project.
- c. This section may not exceed six (6) pages.

### 13.3. Project Work Plan

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

- a. A description of key activities and milestones.
- b. Any assumptions and dependencies of the project.
- c. A detailed methodology description of the Vendor's approach to analyze, assess, validate, document and complete each deliverable milestone.
- d. 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.
- e. Provide estimated due dates for each deliverable specified in Section 4.
- f. All key activities, milestones and methodologies must be phrased in terms and language that can be easily understood by non-technical personnel (e.g., laypersons without subject matter expertise).
- g. This section may not exceed twenty (20) pages.

### 13.4. Additional Considerations

- a. Vendor shall indicate their agreement to comply with the Conflict of Interest Disclosure Statement (provided as Appendix B).
- b. All items of this agreement shall be done in accordance with the Acceptance Criteria.
- c. CTRMA will schedule an oral presentation and interview date.

### 13.5. Trust Services Criteria

As part of a larger SOC Compliance initiative within CTRMA, the enterprise solution for the scope within this SOW must meet the AICPA Trust Service Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy where applicable. Vendors should include in their response to this SOW an understanding of the five (5) criteria areas and any relevant client experience that included the development of policies that govern systems and data with respect to the five (5) Trust Services Criteria areas. [See Appendix D - Trust Services Criteria]

This section may not exceed five (5) pages.

### 13.6. Financial Ability to Implement Project

To demonstrate the Vendor possesses the adequate financial resources necessary for this project, each Vendor shall deliver to CTRMA, at the time of submission of its response, a complete set of the Vendor's then previous three (3) years of consolidated financial statements, including, without limitation, balance sheet and income statements, and notes related thereto. Financial statements should demonstrate positive cash flow from operating activities for the then previous three (3) years. If an audited financial statement for the prior year is not available, an unaudited financial statement may be provided.

Financial statements may be retrieved following the announcement of contract award. Financial statements submitted that have not been retrieved within five business (5) days of the announcement of contract award will be destroyed.

By submitting a response, each Vendor, if awarded the SOW, agrees to deliver to CTRMA, current and updated financial statements, certified as true, complete, and accurate by the Vendor's Chief Financial Officer, reasonably requested by CTRMA from time to time.

Financial statements must be included separately and be clearly marked. This information does not count toward any page limit.

## 14. 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. The Vendor must provide a separate price for each Milestone Deliverable in this SOW based on expected hours and hourly rates by position as approved in the Vendor's current TxDIR contract. An example representation of this price breakdown can be found in Appendix E.

## 15. Schedule of Events and Response Guidelines

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

Table 15-1: Planned Schedule of Events

<b>SOW Issue Date</b>	<b>July 6, 2021</b>
Deadline for Intent to Respond	July 13, 2021
Deadline for SOW Questions submitted to CTRMA	July 19, 2021
Responses by CTRMA to SOW Questions received by deadline	July 26, 2021
<b>Deadline for Submitting Responses to this SOW</b>	<b>August 4, 2021</b>
Presentation and Interview Dates	August 10, 2021
Anticipated Selection Date – CTRMA Board Approval	September 22, 2021
<b>Anticipated Selected Team Notice to Proceed Date</b>	<b>October 2021</b>

**15.1. Questions and Answers**

**An emailed confirmation of the Vendor’s intent to respond to this SOW is required by July 13, 2021.**

**All questions regarding the SOW must be submitted in writing.** Informal verbal inquiries are not allowed. Written questions concerning this SOW must be submitted via [DataPlatform@CTRMA.org](mailto:DataPlatform@CTRMA.org).

The deadline for receipt of questions is **July 19, 2021 4:00 p.m. C.S.T.** Absent any change to deadlines evidenced through a subsequently issued addenda to this SOW, no questions will be accepted after this deadline.

CTRMA anticipates that it will post responses to questions received before the deadline on **July 26, 2021**. Responses will be emailed to all potential Vendors.

CTRMA reserves the right to contact the person submitting a question to clarify the question received, if necessary. CTRMA further reserves the right to modify, summarize or otherwise alter the content of a question to protect the identity of the requestor and to provide responses that CTRMA believes will best inform interested parties of potentially relevant information. CTRMA further reserves the right to decline to answer questions.

Each clarification, supplement, or addenda to this SOW, if any, will be emailed to all Vendors.

**16. Response Submission Requirements**

Responses must be received in the offices of CTRMA by or before **August 4, 2021 4:00 p.m. C.S.T.**, to be eligible for consideration. Responses must meet the format requirements set forth in Section 13, and the following submittal requirements:

Table 16-1: SOW Response Submittal Requirements

<b>Number of Hard Copies</b>	Two (2) bound copies of the SOW Response. One (1) of the two (2) copies of the Responses must be marked “original” and bear all the original signatures.
<b>Number of Electronic Copies</b>	One (1) electronic copy of the SOW Response emailed to <a href="mailto:DataPlatform@CTRMA.org">DataPlatform@CTRMA.org</a> . The file must be labeled as follows: DP2021-SOW_ Firm Name.pdf Example: “DP2021-SOW _DP-R3 Firm.pdf”
<b>Mailing Address</b>	Central Texas Regional Mobility Authority 3300 N IH-35, Suite 300 Austin, TX 78705
<b>Attention</b>	Labelled, “Attention: Greg Mack”
<b>Package Label</b>	Data Platform Services <Firm Name> <Date>

In the event of a discrepancy/conflict between a hard copy and electronic version, the hardcopy version will govern. SOW Responses may be hand delivered to the address noted above.

Responses must be provided in a sealed envelope or package with the package label and the firm’s name and address clearly visible on the outside of the envelope or package. *Responses received after the deadline will not be considered.*

The responsibility for submitting an SOW Response to CTRMA on or before the stated time and date will be solely and strictly the responsibility of the Vendor. CTRMA will in no way be responsible for delays caused by the United States mail delivery, common carrier, or by any other occurrence.

CTRMA reserves the right to request additional information or clarifications from any Vendors or to allow corrections of errors or omissions.

If the size of the SOW Response exceeds either CTRMA's 20MB email limit or Vendor email limits, the Vendor must provide a location, e.g. an FTP site, where the SOW Response may be accessed by CTRMA.

## APPENDIX A

### Table of Acronyms

AICPA	American Institute of CPAs
API	Application Programming Interface
AVI	Automatic Vehicle Identification
CTRMA	Central Texas Regional Mobility Authority
CUSIOP	Central United States Interoperability Hub
DMV	Texas Department of Motor Vehicles
ERD	Entity Relationship Diagram
ETCS	Electronic Toll Collection System
ICD	Interface Control Document
IOP	Interoperability
JSON	JavaScript Object Notion
PMI-PMBOK	Project Management Institute – Project Management Body of Knowledge
SOA	Service Oriented Architecture
SOC	Service Organization Control
SOW	Statement of Work
SQL	Structured Query Language
TSP	Trust Services Protocol
TxDIR	Texas Department of Information Resources
UI	User Interface
UX	User Experience
XML	eXtensible Markup Language



## Appendix B

### Conflict of Interest Disclosure Statement

This Disclosure Statement outlines potential conflicts of interest as a result of a previous or current business relationship between the undersigned individual (and/or the firm for which the individual works) and an individual or firm submitting a Proposal or otherwise under consideration for a contract associated with \_\_\_\_\_ . Section I of this Disclosure Statement Form describes the potential conflicts of interest. Section II of this Disclosure Statement Form describes the proposer's management plan for dealing with the potential conflicts of interest as described in Section I of this form. This Disclosure Statement is being submitted in compliance with the Central Texas Regional Mobility Authority's Conflict of Interest Policy for Consultants. The undersigned acknowledges that approval of the proposed management plan is within the sole discretion of the Central Texas Regional Mobility Authority.

SECTION I. Description of Potential Conflicts of Interest.

---

---

---

---

---

SECTION II. Management Plan for Dealing with Potential Conflicts of Interest.

---

---

---

---

---

SIGNED: \_\_\_\_\_ DATE: \_\_\_\_\_

NAME AND TITLE: \_\_\_\_\_

REPRESENTING: \_\_\_\_\_

APPROVED BY THE CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY:

SIGNED: \_\_\_\_\_ DATE: \_\_\_\_\_

NAME AND TITLE: \_\_\_\_\_

## **Appendix C**

### **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 <a href="#">RFC6090</a> compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. <a href="#">PKCS#7 padding scheme</a> is recommended. Message hashing required.
LDWM	SHA256	Refer to <a href="#">LDWM Hash-based Signatures Draft</a>

### 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](mailto: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](mailto: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](mailto: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](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](mailto: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

<b>Date of Change</b>	<b>Responsible</b>	<b>Summary of Change</b>
June 2014	SANS Policy Team	Updated and converted to new format.

Public key pairs

- Symmetric cryptography

## 33 Revision History

<b>Date of Change</b>	<b>Responsible</b>	<b>Summary of Change</b>
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

<b>Date of Change</b>	<b>Responsible</b>	<b>Summary of Change</b>
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

<b>Date of Change</b>	<b>Responsible</b>	<b>Summary of Change</b>
June 2014	SANS Policy Team	Updated and converted to new format.

## **Appendix D**

### **Trust Services Criteria**



TSP Section 100

# 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

Includes March 2020 updates



---

## TSP Section 100

### *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*

---

(This version includes revisions made in March 2020, as discussed in the Notice to Readers.)

#### Notice to Readers

The *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* presents control criteria established by the Assurance Services Executive Committee (ASEC) of the AICPA for use in attestation or consulting engagements to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy of information and systems (a) across an entire entity; (b) at a subsidiary, division, or operating unit level; (c) within a function relevant to the entity's operational, reporting, or compliance objectives; or (d) for a particular type of information used by the entity.

In developing and establishing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. [BL section 360R, \*Implementing Resolutions Under Section 3.6 Committees\*](#),<sup>fn 1</sup> designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA council or the board of directors. [Paragraph .A44 of AT-C section 105, \*Concepts Common to All Attestation Engagements\*](#),<sup>fn 2</sup> indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable.

This version of the trust services criteria has been modified by AICPA staff to include conforming changes necessary because of the issuance, in March 2020, of a new SOC examination. In a SOC for Supply Chain examination, a practitioner examines and reports on the effectiveness of controls (suitability of design and operating effectiveness) relevant to the security, availability, or processing integrity of a system or the confidentiality or privacy of information processed by a system that produces, manufactures, or distributes products.

These changes, which have been reviewed by the ASEC chair, were made to provide greater flexibility for use of the trust services criteria in a SOC for Supply Chain examination. It is important to note that these changes do not alter in any way the trust services criteria used to evaluate controls in a SOC 2<sup>®</sup>, SOC 3<sup>®</sup>, or SOC for Cybersecurity examination.

---

<sup>fn 1</sup> All BL sections can be found in AICPA [Professional Standards](#).

<sup>fn 2</sup> All AT-C sections can be found in AICPA [Professional Standards](#).

For users who want to see all conforming changes made to this version of the trust services criteria, a red-lined version is available at <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria-redline-2019.pdf>.

## Background

**.01** The AICPA Assurance Services Executive Committee (ASEC) has developed a set of criteria (trust services criteria) to be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the systems at an entity, a division, or an operating unit of an entity. In addition, the trust services criteria may be used when evaluating the design and operating effectiveness of controls relevant to the security, availability, processing integrity, confidentiality or privacy of a particular type of information processed by one or more of an entity's systems or one or more systems used to support a particular function within the entity. This document presents the trust services criteria.

**.02** As in any system of internal control, an entity faces risks that threaten its ability to achieve its objectives based on the trust services criteria. Such risks arise because of factors such as the following:

- The nature of the entity's operations
- The environment in which it operates
- The types of information generated, used, or stored by the entity
- The types of commitments made to customers and other third parties
- Responsibilities entailed in operating and maintaining the entity's systems and processes
- The technologies, connection types, and delivery channels used by the entity
- The use of third parties (such as service providers and suppliers), who have access to the entity's system, to provide the entity with critical raw materials or components or operate controls that are necessary, in combination with the entity's controls, to achieve the system's objectives
- Changes to the following:
  - System operations and related controls
  - Processing volume
  - Key management personnel of a business unit, supporting IT, or related personnel
  - Legal and regulatory requirements with which the entity needs to comply
- Introduction of new services, products, or technologies

An entity addresses these risks through the implementation of suitably designed controls that, if operating effectively, provide reasonable assurance of achieving the entity's objectives.

**.03** Applying the trust services criteria in actual situations requires judgment. Therefore, in addition to the trust services criteria, this document presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), in its *Internal Control — Integrated Framework* (the COSO framework),<sup>fn 3</sup> states that points of focus represent important characteristics of the criteria. Consistent with the COSO framework, the points of focus in this document may assist management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, and privacy. In addition, the points of focus may assist both management and the practitioner when they are evaluating whether the controls were suitably designed and operated effectively to achieve the entity's objectives based on the trust services criteria.

**.04** Some points of focus may not be suitable or relevant to the entity or to the engagement to be performed. In such situations, management may customize a particular point of focus or identify and consider other characteristics based on the specific circumstances of the entity. Use of the trust services criteria does not require an assessment of whether each point of focus is addressed. Users are advised to consider the facts and circumstances of the entity and its environment in actual situations when applying the trust services criteria.

## Organization of the Trust Services Criteria

**.05** The trust services criteria presented in this document have been aligned to the 17 criteria (known as *principles*) presented in the COSO framework, which was revised in 2013. In addition to the 17 principles, the trust services criteria include additional criteria supplementing COSO principle 12: *The entity deploys control activities through policies that establish what is expected and procedures that put policies into action* (supplemental criteria). The supplemental criteria, which apply to the achievement of the entity's objectives relevant to a trust services engagement, are organized as follows:

- *Logical and physical access controls.* The criteria relevant to how an entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access
- *System operations.* The criteria relevant to how an entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations
- *Change management.* The criteria relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made
- *Risk mitigation.* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners

**.06** In addition to the 17 principles in the COSO framework, certain of the supplemental criteria are shared amongst all the trust services categories (see the section "[Trust Services Categories](#)"). For example, the

---

<sup>fn 3</sup> ©2019, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. See [www.coso.org](http://www.coso.org).

criteria related to logical access apply to the security, availability, processing integrity, confidentiality, and privacy categories. As a result, the trust services criteria consist of

- criteria common to all five of the trust services categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

**.07** The common criteria provide specific criteria for addressing the following:

- The control environment (CC1 series)
- Communication and information (CC2 series)
- Risk assessment (CC3 series)
- Monitoring of controls (CC4 series)
- Control activities related to the design and implementation of controls (CC5 series)

The common criteria are suitable for evaluating the effectiveness of controls to achieve an entity’s system objectives related to security; no additional control activity criteria are needed. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (a) the common criteria and (b) the control activity criteria applicable to the specific trust services category or categories addressed by the engagement. The criteria for each trust services category addressed by the engagement are considered complete only if all the criteria associated with that category are addressed by the engagement.

<i>Trust Services Category</i>	<i>Common Criteria</i>	<i>Additional Category-Specific Criteria</i>
Security	X	N/A
Availability	X	X (A series)
Processing Integrity (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods)	X	X (PI series)
Confidentiality	X	X (C series)
Privacy	X	X (P series)

**.08** The practitioner may report on any of the trust services categories of security, availability, processing integrity, confidentiality, or privacy, either individually or in combination with one or more of the other trust services categories. For each category addressed by the engagement, all criteria for that category are usually addressed. However, in limited circumstances, such as when the scope of the engagement is to report on a system and a particular criterion is not relevant to the services provided by a service organization, one or more criteria may not be applicable to the engagement. For example, when reporting on

privacy for a service organization's system, criterion P3.1, *Personal information is collected consistent with the entity's objectives related to privacy*, is not applicable for a service organization that does not directly collect personal information from data subjects.

## Trust Services Categories

.09 The [table](#) in paragraph .24 presents the trust services criteria and the related points of focus. In that table, the trust services criteria are classified into the following categories:

- a. *Security*. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

*Security* refers to the protection of

- i. information during its collection or creation, use, processing, transmission, and storage and
  - ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.
- b. *Availability*. Information and systems are available for operation and use to meet the entity's objectives.

*Availability* refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

- c. *Processing integrity (over the provision of services or the production, manufacturing, or distribution of goods)*. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

*Processing integrity* refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity. In a SOC for Supply Chain examination, processing integrity refers to whether processing is complete, valid, accurate, timely, and authorized to produce, manufacture, or distribute goods that meet the products' specifications.

- d. *Confidentiality*. Information designated as confidential is protected to meet the entity's objectives.

*Confidentiality* addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

- e. *Privacy*. Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Although confidentiality applies to various types of sensitive information, *privacy* applies only to personal information.

The privacy criteria are organized as follows:

- i. *Notice and communication of objectives*. The entity provides notice to data subjects about its objectives related to privacy.
- ii. *Choice and consent*. The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
- iii. *Collection*. The entity collects personal information to meet its objectives related to privacy.
- iv. *Use, retention, and disposal*. The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.
- v. *Access*. The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
- vi. *Disclosure and notification*. The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.
- vii. *Quality*. The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.

viii. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

.10 As previously stated, the trust services criteria may be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the entity. As such, they may be used when evaluating whether the entity's controls were effective to meet the criteria relevant to any of those categories (security, availability, processing integrity, confidentiality, or privacy), either individually or in combination with controls in other categories.

## Application and Use of the Trust Services Criteria

.11 The trust services criteria were designed to provide flexibility in application and use for a variety of different subject matters. The following are the types of subject matters a practitioner may be engaged to report on using the trust services criteria:

- The effectiveness of controls within an entity's cybersecurity risk management program to achieve the entity's cybersecurity objectives using the trust services criteria relevant to security, availability, and confidentiality as *control criteria* in a SOC for Cybersecurity examination.<sup>fn 4</sup>
- The suitability of design and operating effectiveness of controls included in management's description of a service organization's system relevant to one or more of the trust services criteria over security, availability, processing integrity, confidentiality, or privacy throughout a specified period to achieve the entity's objectives based on those criteria in a type 2 SOC 2 engagement. A type 2 SOC 2 engagement, which includes an opinion on the operating effectiveness of controls, also includes a detailed description of tests of controls performed by the service auditor and the results of those tests. A type 1 SOC 2 engagement addresses the same subject matter as a type 2 SOC 2 engagement; however, a type 1 SOC 2 report does not contain an opinion on the operating effectiveness of controls nor a detailed description of tests of controls performed by the service auditor and the results of those tests.<sup>fn 5</sup>
- The design and operating effectiveness of a service organization's controls over a system relevant to one or more of the trust services criteria over security, availability, processing integrity, confidentiality, and privacy in a SOC 3 engagement. A SOC 3 report contains an opinion on the operating effectiveness of controls but does not include a detailed description of tests of controls performed by the service auditor and the results of those tests.

---

<sup>fn 4</sup> AICPA Guide [Reporting on an Entity's Cybersecurity Risk Management Program and Controls](#) (the cybersecurity guide) provides practitioners with performance and reporting guidance for a SOC for Cybersecurity examination.

<sup>fn 5</sup> AICPA Guide [SOC 2<sup>®</sup> Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy](#), issued in 2018, contains performance and reporting guidance for SOC 2 examinations.

- The suitability of design and operating effectiveness of controls of an entity, other than a service organization, over one or more systems relevant to one or more of the trust services categories of security, availability, processing integrity, confidentiality, or privacy (for example, a SOC for Supply Chain examination).
- The suitability of the design of an entity’s controls over security, availability, processing integrity, confidentiality, or privacy to achieve the entity’s objectives based on the related trust services criteria.<sup>fn 6</sup>

**.12** Practitioners generally do not use the trust services criteria when engaged to report on an entity’s compliance, or on an entity’s internal control over compliance with laws, regulations, rules, contracts, or grant agreements. If the practitioner is engaged to report on compliance with laws, regulations, rules, contracts, or grant agreements in connection with an examination of the design and operating effectiveness of an entity’s controls (for example, in a privacy engagement performed in accordance with [AT-C section 105](#) and [AT-C section 205](#), *Examination Engagements*), the compliance portion of the engagement would be performed in accordance with [AT-C section 105](#) and [AT-C section 315](#), *Compliance Attestation*.

**.13** Many of the trust services criteria include the phrase *to meet the entity’s objectives*. Because the trust services criteria may be used to evaluate controls relevant to a variety of different subject matters (see [paragraph .11](#)) in a variety of different types of engagements (see [paragraphs .20–.23](#)), interpretation of that phrase depends upon the specific circumstances of the engagement. Therefore, when using the trust services criteria, consideration is given to how the *entity’s objectives* referred to in the criteria are affected by the subject matter and scope of the particular engagement.

**.14** For example, consider the following engagements:

- In a SOC 2 engagement to examine and report on a service organization’s controls over the security, availability, processing integrity, confidentiality, or privacy of a *system*, management is responsible for meeting its commitments to customers. Therefore, the *objectives* in a SOC 2 engagement relate *to meeting its commitments to customers and system requirements*. *Commitments* are the declarations made by management to customers regarding the performance of one or more of the entity’s systems. Such commitments generally are included in written contracts, service level agreements, or public statements (for example, a privacy notice). Some commitments are applicable to all customers (baseline commitments), whereas others are designed to meet individual customer needs and result in the implementation of processes or controls, in addition to those required to meet the baseline commitments. *System requirements* refer to how the system should function to achieve the entity’s commitments to customers, relevant laws and regulations, or guidelines of industry groups, such as trade or business associations.

---

<sup>fn 6</sup> [AT-C section 9205](#), *Examination Engagements: Attestation Interpretations of Section 205*, addresses an engagement such as this in [Interpretation No. 2](#), “Reporting on the Design of Internal Control” (AT-C sec. 9205 par. .04–.14). That document states that a practitioner may examine the suitability of the design of controls under [AT-C section 205](#), *Examination Engagements*. [Paragraph .10](#) of AT-C section 205 provides guidance on how a practitioner should report when the engagement is over controls that have not yet been implemented.



- In a SOC for Supply Chain engagement to examine and report on an entity's controls over the security, availability, processing integrity, confidentiality, or privacy of a system used to produce, manufacture, or distribute products, management is responsible for establishing principal system objectives. Such objectives are embodied in the product commitments the entity makes to customers, including producing or manufacturing a product that meets product performance specifications and other production, manufacturing, or distribution specifications. Commitments may also relate to other matters (for example, conforming with a variety of other standards and criteria such as the risk entity management framework issued by the National Institute of Standards and Technology, the cybersecurity standards issued by the International Organization for Standardization [ISO], or the Food and Drug Administration regulations on electronic records and electronic signatures included in Code of Federal Regulations, *Electronic Records; Electronic Signatures*, Title 21, Part 11).
- In an entity-wide SOC for Cybersecurity examination, the entity establishes *cybersecurity objectives*. *Cybersecurity objectives* are those that could be affected by cybersecurity risk and, therefore, affect the achievement of the entity's compliance, reporting, and operational objectives. The nature of an entity's cybersecurity objectives will vary depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, and other factors. For example, a telecommunication entity may have a cybersecurity objective related to the reliable functioning of those aspects of its operations that are deemed to be critical infrastructure, whereas an online dating entity is likely to regard the privacy of the personal information collected from customers to be a critical factor in achieving its operating objectives.<sup>fn 7</sup>

**.15** As an example of how the different subject matters and engagement scopes affect the use of the trust services criteria, consider trust services criterion CC6.4:

The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

**.16** In the SOC 2 engagement example discussed in [paragraph .14](#), the phrase *to meet the entity's objectives* in CC6.4 usually would be interpreted as follows:

The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel *to meet the service organization's commitments and system requirements*.

**.17** In addition, criterion CC6.4 would only be applied as it relates to controls over the trust services category(ies) relevant to the system(s) included within the scope of the SOC 2 engagement.

---

<sup>fn 7</sup> The practitioner's responsibility is similar to that in [AT-C section 320](#), *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, which requires the service auditor in a SOC 1<sup>®</sup> engagement to determine whether the control objectives stated in management's description of the service organization's system are reasonable in the circumstances.

.18 In the SOC for Cybersecurity examination example in [paragraph .14](#), the phrase *to meet the entity's objectives* in CC6.4 usually would be interpreted as follows:

The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's cybersecurity objectives.

.19 In addition, criterion CC6.4 would be applied as it relates to controls within the cybersecurity risk management program (a) across an entire entity; (b) at a subsidiary, division, or operating unit level; (c) within a function relevant to the entity's operations, reporting, or compliance objectives; or (d) for a particular type of information used by the entity, depending on the scope of the SOC for Cybersecurity examination.

## Professional Standards Governing Engagements Using the Trust Services Criteria

### Attestation Engagements

.20 Examination engagements and engagements to apply agreed-upon procedures performed in accordance with the AICPA Statements on Standards for Attestation Engagements<sup>fn 8</sup> (SSAEs or attestation standards) may use the trust services criteria as the evaluation criteria. The attestation standards provide guidance on performing and reporting in connection with an examination, review,<sup>fn 9</sup> and agreed-upon procedures engagements. Under the attestation standards, the CPA performing an attestation engagement is known as a *practitioner*. In an examination engagement, the practitioner provides a report in which he or she expresses an opinion on subject matter or an assertion about the subject matter in relation to an identified set of criteria. In an agreed-upon procedures engagement, the practitioner does not express an opinion but, rather, performs procedures agreed upon by the specified parties and reports the results of those procedures. Examination engagements are performed in accordance with [AT-C sections 105](#) and [205](#); agreed-upon procedures engagements are performed in accordance with [AT-C section 105](#) and [AT-C section 215](#), *Agreed-Upon Procedures Engagements*.

.21 According to the attestation standards, the criteria used in an attestation engagement should be suitable and available to report users. Attributes of suitable criteria are as follows:<sup>fn 10</sup>

---

<sup>fn 8</sup> [Statement on Standards for Attestation Engagements No. 18](#), *Attestation Standards: Clarification and Recodification*, is effective for practitioners' reports dated on or after May 1, 2017.

<sup>fn 9</sup> [Paragraph .07](#) of AT-C section 305, *Prospective Financial Information*, prohibits a practitioner from performing a review of internal control; therefore, practitioners may not perform a review engagement in accordance with the attestation standards using the trust services criteria.

<sup>fn 10</sup> [Paragraph .25b](#) of AT-C section 105, *Concepts Common to All Attestation Engagements*.

- *Relevance*. Criteria are relevant to the subject matter.
- *Objectivity*. Criteria are free from bias.
- *Measurability*. Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- *Completeness*. Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users made on the basis of that subject matter.

.22 In addition to being suitable, [AT-C section 105](#) indicates that the criteria used in an attestation engagement must be available to users. The publication of the trust services criteria makes the criteria available to report users. Accordingly, ASEC has concluded that the trust services criteria are suitable criteria in accordance with the attestation standards.

## Consulting Engagements

.23 Sometimes, the trust services criteria may be used in engagements that involve the performance of readiness services, in which a practitioner may assist management with the implementation of one or more new information systems within an organization.<sup>fn 11</sup> Such engagements typically are performed under the consulting standards. In a consulting engagement, the practitioner develops findings and makes recommendations for the consideration and use of management; the practitioner does not form a conclusion about or express an opinion on the subject matter of the engagement. Generally, consulting services are performed only for the use and benefit of the client. Practitioners providing such services follow [CS section 100](#), *Consulting Services: Definitions and Standards*.<sup>fn 12</sup>

## Trust Services Criteria

.24 The following table presents the trust services criteria and the related points of focus. In the table, criteria and related points of focus that come directly from the COSO framework are presented using a normal font. In contrast, supplemental criteria and points of focus that apply to engagements using the trust services criteria are presented in *italics*. Finally, criteria and points of focus that apply only when engagements using the trust services criteria are performed at a system level are presented in ***bold italics***.

---

<sup>fn 11</sup> When a practitioner provides information systems design, implementation, or integration services to an attest client, threats to the practitioner's independence may exist. The "[Information Systems Design, Implementation, or Integration](#)" interpretation (ET sec. 1.295.145) of the AICPA Code of Professional Conduct, provides guidance to practitioners on evaluating the effect of such threats to their independence.

All ET sections can be found in AICPA [Professional Standards](#).

<sup>fn 12</sup> All CS sections can be found in AICPA [Professional Standards](#).

	<b>CONTROL ENVIRONMENT</b>
<b>CC1.1</b>	<b>COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Sets the Tone at the Top</u> — The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Establishes Standards of Conduct</u> — The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity’s standards of conduct and understood at all levels of the entity and by out-sourced service providers and business partners.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Evaluates Adherence to Standards of Conduct</u> — Processes are in place to evaluate the performance of individuals and teams against the entity’s expected standards of conduct.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Addresses Deviations in a Timely Manner</u> — Deviations from the entity’s expected standards of conduct are identified and remedied in a timely and consistent manner.</li> </ul>
	<b>Additional point of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <i>Considers Contractors and Vendor Employees in Demonstrating Its Commitment</i> — Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.</li> </ul>
<b>CC1.2</b>	<b>COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>

	<ul style="list-style-type: none"> <li>• <u>Establishes Oversight Responsibilities</u> — The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Applies Relevant Expertise</u> — The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Operates Independently</u> — The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.</li> </ul>
	<b>Additional point of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Supplements Board Expertise</u> — The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.</i></li> </ul>
<b>CC1.3</b>	<b>COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Considers All Structures of the Entity</u> — Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Establishes Reporting Lines</u> — Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Defines, Assigns, and Limits Authorities and Responsibilities</u> — Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.</li> </ul>

	<b>Additional points of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <u>Addresses Specific Requirements When Defining Authorities and Responsibilities</u> — Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities</u> — Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.</li> </ul>
<b>CC1.4</b>	<b>COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Establishes Policies and Practices</u> — Policies and practices reflect expectations of competence necessary to support the achievement of objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Evaluates Competence and Addresses Shortcomings</u> — The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Attracts, Develops, and Retains Individuals</u> — The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Plans and Prepares for Succession</u> — Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.</li> </ul>
	<b>Additional point of focus specifically related to all engagements using the trust services criteria:</b>

	<ul style="list-style-type: none"> <li>• <u>Considers the Background of Individuals</u> — The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers the Technical Competency of Individuals</u> — The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Provides Training to Maintain Technical Competencies</u> — The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.</li> </ul>
<b>CC1.5</b>	<b>COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</b>
	<b>The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Enforces Accountability Through Structures, Authorities, and Responsibilities</u> — Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Establishes Performance Measures, Incentives, and Rewards</u> — Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance</u> — Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers Excessive Pressures</u> — Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Evaluates Performance and Rewards or Disciplines Individuals</u> — Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and</li> </ul>

	provide rewards or exercise disciplinary action, as appropriate.
	<b>COMMUNICATION AND INFORMATION</b>
<b>CC2.1</b>	<b>COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.</b>
	<b>The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Identifies Information Requirements</u> — A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity’s objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Captures Internal and External Sources of Data</u> — Information systems capture internal and external sources of data.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Processes Relevant Data Into Information</u> — Information systems process and transform relevant data into information.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Maintains Quality Throughout Processing</u> — Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.</li> </ul>
<b>CC2.2</b>	<b>COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Communicates Internal Control Information</u> — A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Communicates With the Board of Directors</u> — Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity’s objectives.</li> </ul>



	<ul style="list-style-type: none"> <li>• <u>Provides Separate Communication Lines</u> — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Selects Relevant Method of Communication</u> — The method of communication considers the timing, audience, and nature of the information.</li> </ul>
	<b>Additional points of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Responsibilities</u> — Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters</u> — Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Objectives and Changes to Objectives</u> — The entity communicates its objectives and changes to those objectives to personnel in a timely manner.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Information to Improve Security Knowledge and Awareness</u> — The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.</i></li> </ul>
	<b>Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Information About System Operation and Boundaries</u> — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates System Objectives</u> — The entity communicates its objectives to personnel to enable them to carry out their responsibilities.</i></li> </ul>

	<ul style="list-style-type: none"> <li>• <i><u>Communicates System Changes</u> — System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.</i></li> </ul>
CC2.3	<b>COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Communicates to External Parties</u> — Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Enables Inbound Communications</u> — Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Communicates With the Board of Directors</u> — Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Provides Separate Communication Lines</u> — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Selects Relevant Method of Communication</u> — The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.</li> </ul>
	<b>Additional point of focus that applies only to an engagement using the trust services criteria for confidentiality:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Objectives Related to Confidentiality and Changes to Objectives</u> — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.</i></li> </ul>

	<b>Additional point of focus that applies only to an engagement using the trust services criteria for privacy:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Objectives Related to Privacy and Changes to Objectives</u> — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.</i></li> </ul>
	<b>Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Information About System Operation and Boundaries</u> — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates System Objectives</u> — The entity communicates its system objectives to appropriate external users.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates System Responsibilities</u> — External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters</u> — External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.</i></li> </ul>
	<b>RISK ASSESSMENT</b>
<b>CC3.1</b>	<b>COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<b><u>Operations Objectives</u></b>

	<ul style="list-style-type: none"> <li>• <u>Reflects Management's Choices</u> — Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers Tolerances for Risk</u> — Management considers the acceptable levels of variation relative to the achievement of operations objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Includes Operations and Financial Performance Goals</u> — The organization reflects the desired level of operations and financial performance for the entity within operations objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Forms a Basis for Committing of Resources</u> — Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.</li> </ul>
	<p><b><u>External Financial Reporting Objectives</u></b></p> <ul style="list-style-type: none"> <li>• <u>Complies With Applicable Accounting Standards</u> — Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers Materiality</u> — Management considers materiality in financial statement presentation.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Reflects Entity Activities</u> — External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.</li> </ul>
	<p><b><u>External Nonfinancial Reporting Objectives</u></b></p> <ul style="list-style-type: none"> <li>• <u>Complies With Externally Established Frameworks</u> — Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers the Required Level of Precision</u> — Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Reflects Entity Activities</u> — External reporting reflects the underlying transactions and events within a range of acceptable limits.</li> </ul>
	<p><b><u>Internal Reporting Objectives</u></b></p> <ul style="list-style-type: none"> <li>• <u>Reflects Management's Choices</u> — Internal reporting provides management with accurate and complete information regarding management's choices and information</li> </ul>

	needed in managing the entity.
	<ul style="list-style-type: none"> <li>• <u>Considers the Required Level of Precision</u> — Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Reflects Entity Activities</u> — Internal reporting reflects the underlying transactions and events within a range of acceptable limits.</li> </ul>
	<p><b><u>Compliance Objectives</u></b></p> <ul style="list-style-type: none"> <li>• <u>Reflects External Laws and Regulations</u> — Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers Tolerances for Risk</u> — Management considers the acceptable levels of variation relative to the achievement of operations objectives.</li> </ul>
	<b>Additional point of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Establishes Sub-objectives to Support Objectives</u> — Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity’s objectives related to reporting, operations, and compliance.</i></li> </ul>
<b>CC3.2</b>	<b>COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels</u> — The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Analyzes Internal and External Factors</u> — Risk identification considers both internal and external factors and their impact on the achievement of objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Involves Appropriate Levels of Management</u> — The entity puts into place effective</li> </ul>

	risk assessment mechanisms that involve appropriate levels of management.
	<ul style="list-style-type: none"> <li>• <u>Estimates Significance of Risks Identified</u> — Identified risks are analyzed through a process that includes estimating the potential significance of the risk.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Determines How to Respond to Risks</u> — Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.</li> </ul>
	<b>Additional points of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <u>Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities</u> — The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties</u> — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers the Significance of the Risk</u> — The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.</li> </ul>
<b>CC3.3</b>	<b>COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Considers Various Types of Fraud</u> — The assessment of fraud considers fraudulent</li> </ul>

	reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
	<ul style="list-style-type: none"> <li>• <u>Assesses Incentives and Pressures</u> — The assessment of fraud risks considers incentives and pressures.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Assesses Opportunities</u> — The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity’s reporting records, or committing other inappropriate acts.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Assesses Attitudes and Rationalizations</u> — The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.</li> </ul>
	<b>Additional point of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Considers the Risks Related to the Use of IT and Access to Information</u> — The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.</i></li> </ul>
<b>CC3.4</b>	<b>COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Assesses Changes in the External Environment</u> — The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Assesses Changes in the Business Model</u> — The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Assesses Changes in Leadership</u> — The entity considers changes in management and respective attitudes and philosophies on the system of internal control.</li> </ul>

	<b>Additional point of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <u>Assesses Changes in Systems and Technology</u> — The risk identification process considers changes arising from changes in the entity’s systems and changes in the technology environment.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Assesses Changes in Vendor and Business Partner Relationships</u> — The risk identification process considers changes in vendor and business partner relationships.</li> </ul>
	<b>MONITORING ACTIVITIES</b>
<b>CC4.1</b>	<b>COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</b>
	<b>The following points of focus highlight important characteristics relating to this criterion:</b>
	<b>Points of focus specified in the COSO framework:</b>
	<ul style="list-style-type: none"> <li>• <u>Considers a Mix of Ongoing and Separate Evaluations</u> — Management includes a balance of ongoing and separate evaluations.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers Rate of Change</u> — Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Establishes Baseline Understanding</u> — The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Uses Knowledgeable Personnel</u> — Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Integrates With Business Processes</u> — Ongoing evaluations are built into the business processes and adjust to changing conditions.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Adjusts Scope and Frequency</u> — Management varies the scope and frequency of separate evaluations depending on risk.</li> </ul>



	<ul style="list-style-type: none"> <li>• <u>Objectively Evaluates</u> — Separate evaluations are performed periodically to provide objective feedback.</li> </ul>
	<b>Additional point of focus specifically related to all engagements using the trust services criteria:</b>
	<ul style="list-style-type: none"> <li>• <i>Considers Different Types of Ongoing and Separate Evaluations</i> — Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.</li> </ul>
<b>CC4.2</b>	<b>COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.</b>
	<b>The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Assesses Results</u> — Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Communicates Deficiencies</u> — Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Monitors Corrective Action</u> — Management tracks whether deficiencies are remedied on a timely basis.</li> </ul>
	<b>CONTROL ACTIVITIES</b>
<b>CC5.1</b>	<b>COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</b>
	<b>The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Integrates With Risk Assessment</u> — Control activities help ensure that risk responses that address and mitigate risks are carried out.</li> </ul>

	<ul style="list-style-type: none"> <li>• <u>Considers Entity-Specific Factors</u> — Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Determines Relevant Business Processes</u> — Management determines which relevant business processes require control activities.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Evaluates a Mix of Control Activity Types</u> — Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Considers at What Level Activities Are Applied</u> — Management considers control activities at various levels in the entity.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Addresses Segregation of Duties</u> — Management segregates incompatible duties and, where such segregation is not practical, management selects and develops alternative control activities.</li> </ul>
<b>CC5.2</b>	<b>COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.</b>
	<b>The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls</u> — Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Establishes Relevant Technology Infrastructure Control Activities</u> — Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Establishes Relevant Security Management Process Controls Activities</u> — Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity’s assets from external threats.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities</u> — Management selects and develops control activities over</li> </ul>

	the acquisition, development, and maintenance of technology and its infrastructure to achieve management’s objectives.
<b>CC5.3</b>	<b>COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.</b>
	<b>The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Establishes Policies and Procedures to Support Deployment of Management’s Directives</u> — Management establishes control activities that are built into business processes and employees’ day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Establishes Responsibility and Accountability for Executing Policies and Procedures</u> — Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Performs in a Timely Manner</u> — Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Takes Corrective Action</u> — Responsible personnel investigate and act on matters identified as a result of executing control activities.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Performs Using Competent Personnel</u> — Competent personnel with sufficient authority perform control activities with diligence and continuing focus.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Reassesses Policies and Procedures</u> — Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.</li> </ul>
	<b>Logical and Physical Access Controls</b>
<b>CC6.1</b>	<b><i>The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</i></b>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Identifies and Manages the Inventory of Information Assets</u> — <i>The entity identifies,</i></li> </ul>

	<i>inventories, classifies, and manages information assets.</i>
	<ul style="list-style-type: none"> <li>• <i><u>Restricts Logical Access</u> — Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Identifies and Authenticates Users</u> — Persons, infrastructure, and software are identified and authenticated prior to accessing information assets, whether locally or remotely.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Considers Network Segmentation</u> — Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Manages Points of Access</u> — Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Restricts Access to Information Assets</u> — Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access-control rules for information assets.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Manages Identification and Authentication</u> — Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Manages Credentials for Infrastructure and Software</u> — New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Uses Encryption to Protect Data</u> — The entity uses encryption to supplement other measures used to protect data at rest, when such protections are deemed appropriate based on assessed risk.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Protects Encryption Keys</u> — Processes are in place to protect encryption keys during generation, storage, use, and destruction.</i></li> </ul>
<b>CC6.2</b>	<b><i>Prior to issuing system credentials and granting system access, the entity registers and authorizes</i></b>

	<i>new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</i>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Controls Access Credentials to Protected Assets</u> — Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Removes Access to Protected Assets When Appropriate</u> — Processes are in place to remove credential access when an individual no longer requires such access.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Reviews Appropriateness of Access Credentials</u> — The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.</i></li> </ul>
<b>CC6.3</b>	<i>The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.</i>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Creates or Modifies Access to Protected Information Assets</u> — Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Removes Access to Protected Information Assets</u> — Processes are in place to remove access to protected information assets when an individual no longer requires access.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Uses Role-Based Access Controls</u> — Role-based access control is utilized to support segregation of incompatible functions.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Reviews Access Roles and Rules</u> — The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals with access and access rules are modified as appropriate.</i></li> </ul>

<b>CC6.4</b>	<i>The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</i>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Creates or Modifies Physical Access</u> — Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Removes Physical Access</u> — Processes are in place to remove access to physical resources when an individual no longer requires access.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Reviews Physical Access</u> — Processes are in place to periodically review physical access to ensure consistency with job responsibilities.</i></li> </ul>
<b>CC6.5</b>	<i>The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.</i>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Identifies Data and Software for Disposal</u> — Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Removes Data and Software From Entity Control</u> — Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.</i></li> </ul>
<b>CC6.6</b>	<i>The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</i>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Restricts Access</u> — The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.</i></li> </ul>

	<ul style="list-style-type: none"> <li>• <u>Protects Identification and Authentication Credentials</u> — Identification and authentication credentials are protected during transmission outside its system boundaries.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Requires Additional Authentication or Credentials</u> — Additional authentication information or credentials are required when accessing the system from outside its boundaries.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Implements Boundary Protection Systems</u> — Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.</li> </ul>
<b>CC6.7</b>	<b><i>The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.</i></b>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Restricts the Ability to Perform Transmission</u> — Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Uses Encryption Technologies or Secure Communication Channels to Protect Data</u> — Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Protects Removal Media</u> — Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes), as appropriate.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Protects Mobile Devices</u> — Processes are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.</li> </ul>
<b>CC6.8</b>	<b><i>The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.</i></b>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>

	<ul style="list-style-type: none"> <li>• <u>Restricts Application and Software Installation</u> — The ability to install applications and software is restricted to authorized individuals.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Detects Unauthorized Changes to Software and Configuration Parameters</u> — Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Uses a Defined Change Control Process</u> — A management-defined change control process is used for the implementation of software.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Uses Antivirus and Anti-Malware Software</u> — Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software</u> — Procedures are in place to scan information assets that have been transferred or returned to the entity’s custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.</li> </ul>
	<b>System Operations</b>
<b>CC7.1</b>	<b>To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</b>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Uses Defined Configuration Standards</u> — Management has defined configuration standards.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Monitors Infrastructure and Software</u> — The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Implements Change-Detection Mechanisms</u> — The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Detects Unknown or Unauthorized Components</u> — Procedures are in place to de-</li> </ul>



	<i>test the introduction of unknown or unauthorized components.</i>
	<ul style="list-style-type: none"> <li>• <i><u>Conducts Vulnerability Scans</u> — The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.</i></li> </ul>
<b>CC7.2</b>	<b><i>The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</i></b>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Implements Detection Policies, Procedures, and Tools</u> — Detection policies and procedures are defined and implemented and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Designs Detection Measures</u> — Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Implements Filters to Analyze Anomalies</u> — Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Monitors Detection Tools for Effective Operation</u> — Management has implemented processes to monitor the effectiveness of detection tools.</i></li> </ul>
<b>CC7.3</b>	<b><i>The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</i></b>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>

	<ul style="list-style-type: none"> <li>• <u>Responds to Security Incidents</u> — Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Communicates and Reviews Detected Security Events</u> — Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Develops and Implements Procedures to Analyze Security Incidents</u> — Procedures are in place to analyze security incidents and determine system impact.</li> </ul>
	<b>Additional points of focus that apply only in an engagement using the trust services criteria for privacy:</b>
	<ul style="list-style-type: none"> <li>• <u>Assesses the Impact on Personal Information</u> — Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Determines Personal Information Used or Disclosed</u> — When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.</li> </ul>
<b>CC7.4</b>	<b><i>The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.</i></b>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Assigns Roles and Responsibilities</u> — Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Contains Security Incidents</u> — Procedures are in place to contain security incidents that actively threaten entity objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Mitigates Ongoing Security Incidents</u> — Procedures are in place to mitigate the effects of ongoing security incidents.</li> </ul>

	<ul style="list-style-type: none"> <li>• <u>Ends Threats Posed by Security Incidents</u> — Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Restores Operations</u> — Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Develops and Implements Communication Protocols for Security Incidents</u> — Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Obtains Understanding of Nature of Incident and Determines Containment Strategy</u> — An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Remediates Identified Vulnerabilities</u> — Identified vulnerabilities are remediated through the development and execution of remediation activities.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Communicates Remediation Activities</u> — Remediation activities are documented and communicated in accordance with the incident-response program.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Evaluates the Effectiveness of Incident Response</u> — The design of incident-response activities is evaluated for effectiveness on a periodic basis.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Periodically Evaluates Incidents</u> — Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.</li> </ul>
	<b>Additional points of focus that apply only in an engagement using the trust services criteria for privacy:</b>
	<ul style="list-style-type: none"> <li>• <u>Communicates Unauthorized Use and Disclosure</u> — Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Application of Sanctions</u> — The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance</li> </ul>

	<i>with entity policies and legal and regulatory requirements.</i>
CC7.5	<i>The entity identifies, develops, and implements activities to recover from identified security incidents.</i>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Restores the Affected Environment</u> — <i>The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Communicates Information About the Event</u> — <i>Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Determines Root Cause of the Event</u> — <i>The root cause of the event is determined.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Implements Changes to Prevent and Detect Recurrences</u> — <i>Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Improves Response and Recovery Procedures</u> — <i>Lessons learned are analyzed and the incident-response plan and recovery procedures are improved.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Implements Incident-Recovery Plan Testing</u> — <i>Incident-recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.</i></li> </ul>
	<b>Change Management</b>
CC8.1	<i>The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</i>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>

	<ul style="list-style-type: none"> <li>• <u>Manages Changes Throughout the System Life Cycle</u> — A process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Authorizes Changes</u> — A process is in place to authorize system changes prior to development.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Designs and Develops Changes</u> — A process is in place to design and develop system changes.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Documents Changes</u> — A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Tracks System Changes</u> — A process is in place to track system changes prior to implementation.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Configures Software</u> — A process is in place to select and implement the configuration parameters used to control the functionality of software.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Tests System Changes</u> — A process is in place to test system changes prior to implementation.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Approves System Changes</u> — A process is in place to approve system changes prior to implementation.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Deploys System Changes</u> — A process is in place to implement system changes.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Identifies and Evaluates System Changes</u> — Objectives affected by system changes are identified and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents</u> — Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified and the change process is initiated upon identification.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Creates Baseline Configuration of IT Technology</u> — A baseline configuration of IT</li> </ul>

	<i>and control systems is created and maintained.</i>
	<ul style="list-style-type: none"> <li>• <i><u>Provides for Changes Necessary in Emergency Situations</u> — A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame).</i></li> </ul>
	<b>Additional points of focus that apply only in an engagement using the trust services criteria for confidentiality:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Protects Confidential Information</u> — The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity’s objectives related to confidentiality.</i></li> </ul>
	<b>Additional points of focus that apply only in an engagement using the trust services criteria for privacy:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Protects Personal Information</u> — The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity’s objectives related to privacy.</i></li> </ul>
	<b>Risk Mitigation</b>
<b>CC9.1</b>	<i>The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</i>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Considers Mitigation of Risks of Business Disruption</u> — Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes, information, and communications to meet the entity's objectives during response, mitigation, and recovery efforts.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Considers the Use of Insurance to Mitigate Financial Impact Risks</u> — The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.</i></li> </ul>

<b>CC9.2</b>	<b><i>The entity assesses and manages risks associated with vendors and business partners.</i></b>
	<b>The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u><i>Establishes Requirements for Vendor and Business Partner Engagements</i></u> — <i>The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u><i>Assesses Vendor and Business Partner Risks</i></u> — <i>The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u><i>Assigns Responsibility and Accountability for Managing Vendors and Business Partners</i></u> — <i>The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u><i>Establishes Communication Protocols for Vendors and Business Partners</i></u> — <i>The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u><i>Establishes Exception Handling Procedures From Vendors and Business Partners</i></u> — <i>The entity establishes exception handling procedures for service or product issues related to vendors and business partners.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u><i>Assesses Vendor and Business Partner Performance</i></u> — <i>The entity periodically assesses the performance of vendors and business partners.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u><i>Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments</i></u> — <i>The entity implements procedures for addressing issues identified with vendor and business partner relationships.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <u><i>Implements Procedures for Terminating Vendor and Business Partner Relationships</i></u> — <i>The entity implements procedures for terminating vendor and business partner relationships.</i></li> </ul>
	<b>Additional points of focus that apply only to an engagement using the trust services criteria for confidentiality:</b>

	<ul style="list-style-type: none"> <li>• <u>Obtains Confidentiality Commitments from Vendors and Business Partners</u> — The entity obtains confidentiality commitments that are consistent with the entity’s confidentiality commitments and requirements from vendors and business partners who have access to confidential information.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners</u> — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity’s confidentiality commitments and requirements.</li> </ul>
	<b>Additional points of focus that apply only to an engagement using the trust services criteria for privacy:</b>
	<ul style="list-style-type: none"> <li>• <u>Obtains Privacy Commitments from Vendors and Business Partners</u> — The entity obtains privacy commitments, consistent with the entity’s privacy commitments and requirements, from vendors and business partners who have access to personal information.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Assesses Compliance with Privacy Commitments of Vendors and Business Partners</u> — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity’s privacy commitments and requirements and takes corrective action as necessary.</li> </ul>
	<b>ADDITIONAL CRITERIA FOR AVAILABILITY</b>
<b>A1.1</b>	<i>The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Measures Current Usage</u> — The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Forecasts Capacity</u> — The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Makes Changes Based on Forecasts</u> — The system change management process is</li> </ul>



	<i>initiated when forecasted usage exceeds capacity tolerances.</i>
<b>A1.2</b>	<b><i>The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.</i></b>
	<b>The following points of focus, which apply only to an engagement using the trust services availability criteria, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Identifies Environmental Threats</u> — As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Designs Detection Measures</u> — Detection measures are implemented to identify anomalies that could result from environmental threat events.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Implements and Maintains Environmental Protection Mechanisms</u> — Management implements and maintains environmental protection mechanisms to prevent and mitigate environmental events.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Implements Alerts to Analyze Anomalies</u> — Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Responds to Environmental Threat Events</u> — Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator backup subsystem).</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates and Reviews Detected Environmental Threat Events</u> — Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system and actions are taken, if necessary.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Determines Data Requiring Backup</u> — Data is evaluated to determine whether backup is required.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Performs Data Backup</u> — Procedures are in place for backing up data, monitoring to detect backup failures, and initiating corrective action when such failures occur.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Addresses Offsite Storage</u> — Backup data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environ-</i></li> </ul>

	<i>mental threat event affecting both sets of data is reduced to an appropriate level.</i>
	<ul style="list-style-type: none"> <li>• <i>Implements Alternate Processing Infrastructure — Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.</i></li> </ul>
<b>A1.3</b>	<b><i>The entity tests recovery plan procedures supporting system recovery to meet its objectives.</i></b>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i>Implements Business Continuity Plan Testing — Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i>Tests Integrity and Completeness of Backup Data — The integrity and completeness of backup information is tested on a periodic basis.</i></li> </ul>
	<b>ADDITIONAL CRITERIA FOR CONFIDENTIALITY</b>
<b>C1.1</b>	<b><i>The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.</i></b>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i>Identifies Confidential information — Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i>Protects Confidential Information From Destruction — Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.</i></li> </ul>
<b>C1.2</b>	<b><i>The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.</i></b>

	<b>The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Identifies Confidential Information for Destruction</u> — Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Destroys Confidential Information</u> — Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.</i></li> </ul>
	<b>ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY (OVER THE PROVISION OF SERVICES OR THE PRODUCTION, MANUFACTURING, OR DISTRIBUTION OF GOODS)</b>
<b>PI1.1</b>	<i>The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Identifies Information Specifications</u> — The entity identifies information specifications required to support the use of products and services.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Defines Data Necessary to Support a Product or Service</u> — When data is provided as part of a service or product or as part of a reporting obligation related to a product or service:</i> <ol style="list-style-type: none"> <li>1. <i>The definition of the data is available to the users of the data</i></li> <li>2. <i>The definition of the data includes the following information:</i> <ol style="list-style-type: none"> <li>a. <i>The population of events or instances included in the data</i></li> <li>b. <i>The nature of each element (for example, field) of the data (that is, the event or instance to which the data element relates, for example, transaction price of a sale of XYZ Corporation stock for the last trade in that stock on a given day)</i></li> <li>c. <i>Source(s) of the data</i></li> <li>d. <i>The unit(s) of measurement of data elements (for example, fields)</i></li> <li>e. <i>The accuracy/correctness/precision of measurement</i></li> <li>f. <i>The uncertainty or confidence interval inherent in each data element and in the population of those elements</i></li> <li>g. <i>The date the data was observed or the period of time during which the events relevant to the data occurred</i></li> <li>h. <i>The factors in addition to the date and period of time used to determine the inclusion and exclusion of items in the data elements</i></li> </ol> </li> </ol> </li> </ul>

	<p style="text-align: center;"><i>and population</i></p> <ol style="list-style-type: none"> <li>3. <i>The definition is complete and accurate.</i></li> <li>4. <i>The description of the data identifies any information that is necessary to understand each data element and the population in a manner consistent with its definition and intended purpose (metadata) that has not been included within the data.</i></li> </ol>
	<p><b>The following point of focus, which applies only to an engagement using the trust services criteria for processing integrity for a system that produces, manufactures, or distributes products, highlights important characteristics relating to this criterion:</b></p>
	<ul style="list-style-type: none"> <li>• <i><u>Defines Information Necessary to Support the Use of a Good or Product</u> — When information provided by the entity is needed to use the good or product in accordance with its specifications:</i> <ol style="list-style-type: none"> <li>1. <i>The required information is available to the user of the good or product.</i></li> <li>2. <i>The required information is clearly identifiable.</i></li> <li>3. <i>The required information is validated for completeness and accuracy.</i></li> </ol> </li> </ul>
<b>PI1.2</b>	<b><i>The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity’s objectives.</i></b>
	<p><b>The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:</b></p>
	<ul style="list-style-type: none"> <li>• <i><u>Defines Characteristics of Processing Inputs</u> — The characteristics of processing inputs that are necessary to meet requirements are defined.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Evaluates Processing Inputs</u> — Processing inputs are evaluated for compliance with defined input requirements.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Creates and Maintains Records of System Inputs</u> — Records of system input activities are created and maintained completely and accurately in a timely manner.</i></li> </ul>
<b>PI1.3</b>	<b><i>The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity’s objectives.</i></b>
	<p><b>The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:</b></p>
	<ul style="list-style-type: none"> <li>• <i><u>Defines Processing Specifications</u> — The processing specifications that are necessary to meet product or service requirements are defined.</i></li> </ul>

	<ul style="list-style-type: none"> <li>• <u>Defines Processing Activities</u> — Processing activities are defined to result in products or services that meet specifications.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Detects and Corrects Production Errors</u> — Errors in the production process are detected and corrected in a timely manner.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Records System Processing Activities</u> — System processing activities are recorded completely and accurately in a timely manner.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Processes Inputs</u> — Inputs are processed completely, accurately, and timely as authorized in accordance with defined processing activities.</li> </ul>
<b>PI1.4</b>	<b><i>The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity’s objectives.</i></b>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <u>Protects Output</u> — Output is protected when stored or delivered, or both, to prevent theft, destruction, corruption, or deterioration that would prevent output from meeting specifications.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Distributes Output Only to Intended Parties</u> — Output is distributed or made available only to intended parties.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Distributes Output Completely and Accurately</u> — Procedures are in place to provide for the completeness, accuracy, and timeliness of distributed output.</li> </ul>
	<ul style="list-style-type: none"> <li>• <u>Creates and Maintains Records of System Output Activities</u> — Records of system output activities are created and maintained completely and accurately in a timely manner.</li> </ul>
<b>PI1.5</b>	<b><i>The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity’s objectives.</i></b>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:</b>

	<ul style="list-style-type: none"> <li>• <i><u>Protects Stored Items</u> — Stored items are protected to prevent theft, corruption, destruction, or deterioration that would prevent output from meeting specifications.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Archives and Protects System Records</u> — System records are archived and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Stores Data Completely and Accurately</u> — Procedures are in place to provide for the complete, accurate, and timely storage of data.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Creates and Maintains Records of System Storage Activities</u> — Records of system storage activities are created and maintained completely and accurately in a timely manner.</i></li> </ul>
	<b>ADDITIONAL CRITERIA FOR PRIVACY</b>
<b>P1.0</b>	<b>Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy</b>
<b>P1.1</b>	<i>The entity provides notice to data subjects about its privacy practices to meet the entity’s objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity’s privacy practices, including changes in the use of personal information, to meet the entity’s objectives related to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates to Data Subjects</u> — Notice is provided to data subjects regarding the following:</i> <ul style="list-style-type: none"> <li>— <i>Purpose for collecting personal information</i></li> <li>— <i>Choice and consent</i></li> <li>— <i>Types of personal information collected</i></li> <li>— <i>Methods of collection (for example, use of cookies or other tracking techniques)</i></li> <li>— <i>Use, retention, and disposal</i></li> <li>— <i>Access</i></li> <li>— <i>Disclosure to third parties</i></li> <li>— <i>Security for privacy</i></li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>— <i>Quality, including data subjects’ responsibilities for quality</i></li> <li>— <i>Monitoring and enforcement</i></li> </ul> <p><i>If personal information is collected from sources other than the individual, such sources are described in the privacy notice.</i></p>
	<ul style="list-style-type: none"> <li>• <i><u>Provides Notice to Data Subjects</u> — Notice is provided to data subjects (1) at or before the time personal information is collected or as soon as practical thereafter, (2) at or before the entity changes its privacy notice or as soon as practical thereafter, or (3) before personal information is used for new purposes not previously identified.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Covers Entities and Activities in Notice</u> — An objective description of the entities and activities covered is included in the entity’s privacy notice.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Uses Clear and Conspicuous Language</u> — The entity’s privacy notice is conspicuous and uses clear language.</i></li> </ul>
<b>P2.0</b>	<b>Privacy Criteria Related to Choice and Consent</b>
<b>P2.1</b>	<i>The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity’s objectives related to privacy. The entity’s basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates to Data Subjects</u> — Data subjects are informed (a) about the choices available to them with respect to the collection, use, and disclosure of personal information and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Consequences of Denying or Withdrawing Consent</u> — When personal information is collected, data subjects are informed of the consequences of refusing to provide personal information or denying or withdrawing consent to use personal information for purposes identified in the notice.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Obtains Implicit or Explicit Consent</u> — Implicit or explicit consent is obtained from data subjects at or before the time personal information is collected or soon there-</i></li> </ul>

	<i>after. The individual’s preferences expressed in his or her consent are confirmed and implemented.</i>
	<ul style="list-style-type: none"> <li>• <i><u>Documents and Obtains Consent for New Purposes and Uses</u> — If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Obtains Explicit Consent for Sensitive Information</u> — Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Obtains Consent for Data Transfers</u> — Consent is obtained before personal information is transferred to or from an individual’s computer or other similar device.</i></li> </ul>
<b>P3.0</b>	<b>Privacy Criteria Related to Collection</b>
<b>P3.1</b>	<b><i>Personal information is collected consistent with the entity’s objectives related to privacy.</i></b>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Limits the Collection of Personal Information</u> — The collection of personal information is limited to that necessary to meet the entity’s objectives.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Collects Information by Fair and Lawful Means</u> — Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Collects Information From Reliable Sources</u> — Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Informs Data Subjects When Additional Information Is Acquired</u> — Data subjects are informed if the entity develops or acquires additional information about them for its use.</i></li> </ul>
<b>P3.2</b>	<b><i>For information requiring explicit consent, the entity communicates the need for such consent as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity’s objectives re-</i></b>



	<i>lated to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Obtains Explicit Consent for Sensitive Information</u> — Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Documents Explicit Consent to Retain Information</u> — Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained in accordance with objectives related to privacy.</i></li> </ul>
<b>P4.0</b>	<b>Privacy Criteria Related to Use, Retention, and Disposal</b>
<b>P4.1</b>	<i>The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.</i>
	<b>The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Uses Personal Information for Intended Purposes</u> — Personal information is used only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained, unless a law or regulation specifically requires otherwise.</i></li> </ul>
<b>P4.2</b>	<i>The entity retains personal information consistent with the entity's objectives related to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Retains Personal Information</u> — Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Protects Personal Information</u> — Policies and procedures have been implemented to protect personal information from erasure or destruction during the specified retention period of the information.</i></li> </ul>
<b>P4.3</b>	<i>The entity securely disposes of personal information to meet the entity's objectives related to privacy.</i>

	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Captures, Identifies, and Flags Requests for Deletion</u> — Requests for deletion of personal information are captured and information related to the requests is identified and flagged for destruction to meet the entity’s objectives related to privacy.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Disposes of, Destroys, and Redacts Personal Information</u> — Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Destroys Personal Information</u> — Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.</i></li> </ul>
<b>P5.0</b>	<b>Privacy Criteria Related to Access</b>
<b>P5.1</b>	<i>The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity’s objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity’s objectives related to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Authenticates Data Subjects’ Identity</u> — The identity of data subjects who request access to their personal information is authenticated before they are given access to that information.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Permits Data Subjects Access to Their Personal Information</u> — Data subjects are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Provides Understandable Personal Information Within Reasonable Time</u> — Personal information is provided to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Informs Data Subjects If Access Is Denied</u> — When data subjects are denied access to their personal information, the entity informs them of the denial and the reason for the denial in a timely manner, unless prohibited by law or regulation.</i></li> </ul>

<b>P5.2</b>	<i>The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity’s objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity’s objectives related to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Denial of Access Requests</u> — Data subjects are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity’s legal right to deny such access, if applicable, and the individual’s right, if any, to challenge such denial, as specifically permitted or required by law or regulation.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Permits Data Subjects to Update or Correct Personal Information</u> — Data subjects are able to update or correct personal information held by the entity. The entity provides such updated or corrected information to third parties that were previously provided with the data subject’s personal information consistent with the entity’s objectives related to privacy.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Denial of Correction Requests</u> — Data subjects are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal.</i></li> </ul>
<b>P6.0</b>	<b>Privacy Criteria Related to Disclosure and Notification</b>
<b>P6.1</b>	<i>The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity’s objectives related to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates Privacy Policies to Third Parties</u> — Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Discloses Personal Information Only When Appropriate</u> — Personal information is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless a law or regulation specifically requires otherwise.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Discloses Personal Information Only to Appropriate Third Parties</u> — Personal information is disclosed only to third parties who have agreements with the entity to</i></li> </ul>

	<i>protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.</i>
	<ul style="list-style-type: none"> <li>• <i><u>Discloses Information to Third Parties for New Purposes and Uses</u> — Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects.</i></li> </ul>
<b>P6.2</b>	<b><i>The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.</i></b>
	<b>The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Creates and Retains Record of Authorized Disclosures</u> — The entity creates and maintains a record of authorized disclosures of personal information that is complete, accurate, and timely.</i></li> </ul>
<b>P6.3</b>	<b><i>The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.</i></b>
	<b>The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Creates and Retains Record of Detected or Reported Unauthorized Disclosures</u> — The entity creates and maintains a record of detected or reported unauthorized disclosures of personal information that is complete, accurate, and timely.</i></li> </ul>
<b>P6.4</b>	<b><i>The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.</i></b>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Discloses Personal Information Only to Appropriate Third Parties</u> — Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet</i></li> </ul>

	<i>the terms of the agreement, instructions, or requirements.</i>
	<ul style="list-style-type: none"> <li>• <i><u>Remediates Misuse of Personal Information by a Third Party</u> — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.</i></li> </ul>
<b>P6.5</b>	<i>The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity’s objectives related to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Remediates Misuse of Personal Information by a Third Party</u> — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Reports Actual or Suspected Unauthorized Disclosures</u> — A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.</i></li> </ul>
<b>P6.6</b>	<i>The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Remediates Misuse of Personal Information by a Third Party</u> — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Provides Notice of Breaches and Incidents</u> — The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy.</i></li> </ul>
<b>P6.7</b>	<i>The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects’ personal information, upon the data subjects’ request, to meet the entity’s objectives related to privacy.</i>

	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Identifies Types of Personal Information and Handling Process</u> — The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Captures, Identifies, and Communicates Requests for Information</u> — Requests for an accounting of personal information held and disclosures of the data subjects' personal information are captured and information related to the requests is identified and communicated to data subjects to meet the entity's objectives related to privacy.</i></li> </ul>
<b>P7.0</b>	<b>Privacy Criteria Related to Quality</b>
<b>P7.1</b>	<i>The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Ensures Accuracy and Completeness of Personal Information</u> — Personal information is accurate and complete for the purposes for which it is to be used.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Ensures Relevance of Personal Information</u> — Personal information is relevant to the purposes for which it is to be used.</i></li> </ul>
<b>P8.0</b>	<b>Privacy Criteria Related to Monitoring and Enforcement</b>
<b>P8.1</b>	<i>The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.</i>
	<b>The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:</b>
	<ul style="list-style-type: none"> <li>• <i><u>Communicates to Data Subjects</u> — Data subjects are informed about how to contact the entity with inquiries, complaints, and disputes.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Addresses Inquiries, Complaints, and Disputes</u> — A process is in place to address</i></li> </ul>

	<i>inquiries, complaints, and disputes.</i>
	<ul style="list-style-type: none"> <li>• <i><u>Documents and Communicates Dispute Resolution and Recourse</u> — Each complaint is addressed and the resolution is documented and communicated to the individual.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Documents and Reports Compliance Review Results</u> — Compliance with objectives related to privacy are reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Documents and Reports Instances of Noncompliance</u> — Instances of noncompliance with objectives related to privacy are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.</i></li> </ul>
	<ul style="list-style-type: none"> <li>• <i><u>Performs Ongoing Monitoring</u> — Ongoing procedures are performed for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.</i></li> </ul>

## Appendix A — Glossary

.25

**access to personal information.** The ability to view personal information held by an organization. This ability may be complemented by an ability to update or correct the information. Access defines the intersection of identity and data, that is, who can do what to which data. Access is one of the fair information practice principles. Individuals need to be able to find out what personal information an entity has on file about them and how the information is being used. Individuals need to be able to correct erroneous information in such records.

**architecture.** The design of the structure of a system, including logical components, and the logical interrelationships of a computer, its operating system, a network, or other elements.

**authentication.** The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

**authorization.** The process of granting access privileges to a user, program, or process by a person that has the authority to grant such access.

**board or board of directors.** Individuals with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. Depending on the nature of the entity, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit entity, a board of governors or commissioners for a government entity, general partners for a partnership, or an owner for a small business.

**business partner.** An individual or business (and its employees), other than a vendor, that has some degree of involvement with the entity's business dealings or agrees to cooperate, to any degree, with the entity (for example, a computer manufacturer who works with another company who supplies it with parts).

**collection.** The process of obtaining personal information from the individual directly (for example, through the individual's submission of an internet form or a registration form) or from another party such as a business partner.

**commitments.** Declarations made by management to customers regarding the performance of one or more systems that provide services or products. Commitments can be communicated in written individualized agreements, standardized contracts, service level agreements, or published statements (for example, a security practices statement). A commitment may relate to one or more trust services categories. Commitments may be made on many different aspects of the service being provided or the product, production, manufacturing, or distribution specifications.

**component.** One of five elements of internal control, including the control environment, risk assessment, control activities, information and communication, and monitoring activities.

**compromise.** Refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of systems or (2) the integrity or availability of system inputs or outputs.

**controls.** Policies and procedures that are part of the entity's system of internal control. The objective of an entity's system of internal control is to provide reasonable assurance that principal system objectives are achieved.

**control activity.** An action established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

**consent.** This privacy requirement is one of the fair information practice objectives. Individuals must be able to prevent the collection of their personal data, unless legally required. If an individual has a choice about the use or disclosure of his or her information, consent is the individual's way of giving permission for the use or disclosure. Consent may be affirmative (for example, opting in) or implied (for example, not opting out). There are two types of consent:

- **explicit consent.** A requirement that an individual "signifies" his or her agreement with a data controller by some active communication between the parties.
- **implied consent.** When consent may reasonably be inferred from the action or inaction of the individual.

**COSO.** The Committee of Sponsoring Organizations of the Treadway Commission. COSO is a joint initiative of five private-sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. (See [www.coso.org](http://www.coso.org).)

**criteria.** The benchmarks used to measure or evaluate the subject matter.



**cybersecurity objectives.** Objectives that address the cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting, and operational objectives).

**design.** As used in the COSO definition of internal control, the internal control system design is intended to provide reasonable assurance of the achievement of an entity's objectives.

**data subject.** The individual about whom personal information is collected.

**disclosure.** The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. Disclosure is often used interchangeably with the terms *sharing* and *onward transfer*.

**disposal.** A phase of the data life cycle that pertains to how an entity removes or destroys data or information.

**effectiveness (of controls).** Encompasses both the suitability of the design of controls and the operating effectiveness of controls to provide reasonable assurance that the entity's principal system objectives are achieved.

**entity.** A legal entity or management operating model of any size established for a particular purpose. A legal entity may, for example, be a business enterprise, a not-for-profit organization, a government body, or an academic institution. The management operating model may follow product or service lines, divisions, or operating units, with geographic markets providing for further subdivisions or aggregations of performance.

**entity-wide.** Activities that apply across the entity — most commonly in relation to entity-wide controls.

**environmental.** Of or having to do with the matters that can damage the physical elements of information systems (for example, fire, flood, wind, earthquake, power surges, or power outages). An entity implements controls and other activities to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system from environmental elements.

**external users.** Users, other than entity personnel, who are authorized by entity management, customers, or other authorized persons to interact with the entity's information system.

**information and systems.** Refers to information in electronic form (electronic information) during its use, processing, transmission, and storage and systems that use, process, transmit or transfer, and store information or that produce, manufacture, or distribute products.

**information assets.** Data and the associated software and infrastructure used to process, transmit, and store information or to produce, manufacture, or distribute products.

**infrastructure.** The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, and network elements.

**internal control.** A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

**outsourced service providers.** A service provider that performs business processes, operations, or controls on behalf of the entity when such business processes, operations, or controls are necessary to achieve the entity's objectives.

**personal information.** Information that is or can be about or related to an identifiable individual.

**policies.** Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the bases for procedures.

**practitioner.** As used in this document, a CPA who performs an examination of controls within an entity's system relevant to security, availability, processing integrity, confidentiality, or privacy.

**principal system objectives.** System objectives that relate to the trust services category or categories addressed by the examination and that could reasonably be expected to influence the relevant decisions of intended users. (See *system objectives*.)

**privacy commitments.** Declarations made by management regarding the performance of a system processing personal information. Such commitments can be communicated in written agreements, standardized contracts, service level agreements, or published statements (for example, a privacy practices statement). In addition, privacy commitments may be made on many different aspects of the service being provided.

**privacy notice.** A written communication by entities that collect personal information, to the individuals about whom personal information is collected, about the entity's (a) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (b) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

**products.** Tangible or intangible goods manufactured or produced by an entity. Throughout this document, the term is used interchangeably with *goods*.

**report users.** Intended users of the practitioner's report in accordance with [AT-C section 205](#), *Examination Engagements*.<sup>fn 1</sup> There may be a broad range of report users for a general-purpose report but only a limited number of specified parties for a report that is restricted in accordance with [paragraph .64](#) of AT-C section 205.

**retention.** A phase of the data life cycle that pertains to how long an entity stores information for future use or reference.

---

<sup>fn 1</sup> All AT-C sections can be found in AICPA [Professional Standards](#).

**risk.** The possibility that an event will occur and adversely affect the achievement of objectives.

**risk response.** The decision to accept, avoid, reduce, or share a risk.

**security event.** An occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems, result in unauthorized disclosure or theft of information or other assets, or cause damage to systems.

**security incident.** A security event that requires action on the part of an entity in order to protect information assets and resources.

**senior management.** The chief executive officer or equivalent organizational leader and senior management team.

**service provider.** A supplier (such as a service organization) engaged to provide services to the entity. Service providers include outsourced service providers as well as suppliers that provide services not associated with business functions, such as janitorial, legal, and audit services.

**SOC 2 engagement.** An examination engagement to report on the fairness of the presentation of management's description of the service organization's system, the suitability of the design of the controls included in the description, and, in a type 2 engagement, the operating effectiveness of those controls. This engagement is performed in accordance with the attestation standards and AICPA Guide [\*SOC 2<sup>®</sup> Reporting on an Examination of Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy\*](#).

**SOC 3 engagement.** An examination engagement to report on the suitability of design and the operating effectiveness of an entity's controls over a system relevant to one or more of the trust services categories.

**SOC for Cybersecurity examination.** An examination engagement to report on whether (a) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (b) the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria. A SOC for Cybersecurity examination is performed in accordance with the attestation standards and AICPA Guide [\*Reporting on an Entity's Cybersecurity Risk Management Program and Controls\*](#).

**SOC for Supply Chain examination.** An examination engagement to report on whether (a) the description of the entity's system is presented in accordance with the description criteria and (b) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria. Such an examination is based on guidance contained in AICPA Guide [\*SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System\*](#).

**stakeholders.** Parties that are affected by the entity, such as shareholders, the communities in which an entity operates, employees, customers, and suppliers.

**subsequent events.** Events or transactions that occur after the specified period addressed by the description but prior to the date of the practitioner's report; such events or transactions could have a significant effect on the evaluation of whether the description is presented in accordance with the description criteria or whether controls were effective to provide reasonable assurance that the entity's principal system objectives were achieved based on the applicable trust services criteria.

**supplier.** See definition for *vendor*.

**system.** Refers to the infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements.

**system boundaries.** The specific aspects of an entity's infrastructure, software, people, procedures, and data necessary to perform a function (such as producing, manufacturing, or distributing a product) or provide a service. When systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap but the boundaries of each system will differ.

**system components.** Refers to the individual elements of a system. System components can be classified into the following five categories: infrastructure, software, people, processes, and data.

**system event.** An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and could result in an entity's failure to achieve its system objectives. Such an occurrence may arise from actual or attempted unauthorized access or use by internal or external parties and (a) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems; (b) result in unauthorized disclosure or theft of information or other assets or the destruction or corruption of data; or (c) cause damage to systems. Such occurrences also may arise from the failure of the system to process data as designed or from the loss, corruption, or destruction of data used by the system.

**system incident.** A system event that requires action on the part of entity management to prevent or reduce the impact of a system event on the entity's achievement of its system objectives.

**system objectives.** The entity's objectives, established by entity management, that are embodied in the product commitments it makes to customers, including producing or manufacturing a product that meets product performance specifications and other production, manufacturing, or distribution specifications. The system objectives also include the requirements established for the functioning of the system to meet production, manufacturing, or distribution commitments.

**system requirements.** Specifications regarding how the system should function to (a) meet the entity's commitments to customers and others (such as customers' customers); (b) meet the entity's commitments to suppliers and business partners; (c) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (d) achieve other entity objectives that are relevant to the trust services category or categories addressed by the description. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations.

System requirements may result from the entity's commitments relating to security, availability, processing integrity, confidentiality, or privacy. For example, a commitment to programmatically

enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration.

**third party.** An individual or organization other than the entity and its employees. Third parties may be customers, suppliers, business partners, or others.

**trust services.** A set of professional attestation and advisory services based on a core set of criteria related to security, availability, processing integrity, confidentiality, or privacy.

**unauthorized access.** Access to information or system components that (a) has not been approved by a person designated to do so by management and (b) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate).

**vendor (or supplier).** An individual or business (and its employees) that is engaged to provide goods or services to the entity. Depending on the services provided (for example, if the vendor operates certain controls on behalf of the entity that are necessary to achieve the entity's objectives), it also might be a service provider.



**Exhibit B**

**CTRMA DATA PLATFORM RELEASE 3 STATEMENT OF WORK  
APPENDIX E PRICING FORM - Deloitte Consulting**

Release 3 Data Platform Deliverables		Total Hrs	
		Price	
<b>Tolling Product Management</b>			
Development and deployment of Product database(s) and relationships	Hours	386	
	Price	\$50,055.00	
Design and development of automated Product Management process(es)	Hours	386	
	Price	\$50,055.00	
Development of automated business process(es) for payor ID and payment path routing logic	Hours	386	
	Price	\$50,055.00	
<b>Discount Management</b>			
Development and deployment of Discount database(s) and relationships	Hours	386	
	Price	\$50,055.00	
Design and development of automated Discount Management process(es)	Hours	386	
	Price	\$50,055.00	
Integration of Discount Management with Product Management processes	Hours	386	
	Price	\$50,055.00	
<b>Invoice Management</b>			
Development and deployment of Invoice database(s) and relationships	Hours	386	
	Price	\$50,055.00	
Design and development of automated Invoice Management process(es)	Hours	386	
	Price	\$50,055.00	
Integration of Invoice Management with Product and Discount Management	Hours	386	
	Price	\$50,055.00	
<b>Data Exchange Management</b>			
Design, development, and testing for Pay by Mail('PBM') Invoice data exchange modifications (Fixed file, API, XML, JSON)	Hours	386	
	Price	\$50,055.00	
Design, development, and testing for IOP Hub Invoice data exchange modifications (Fixed file, API, XML, JSON)	Hours	386	
	Price	\$50,055.00	
Development of DMV Hub database(s) and relationships	Hours	386	
	Price	\$50,055.00	
Design, development, and testing for external DMV Hub data exchanges (Fixed file, API, XML, JSON)	Hours	386	
	Price	\$50,055.00	
Design, development, and testing for Public Reporting data exchange (Fixed file, API, XML, JSON, GitHub)	Hours	386	
	Price	\$50,055.00	
<b>Reporting Cache &amp; Reporting Management</b>			
Development of Reporting Cache data platform	Hours	386	
	Price	\$50,055.00	
Development of Public Reporting database(s) and relationships	Hours	386	
	Price	\$50,055.00	
Implementation and testing of Public Reporting data push from master data source to Reporting Cache	Hours	386	
	Price	\$50,055.00	
Development of automated Public Report(s) generation	Hours	386	
	Price	\$50,055.00	
End-to-end testing of Reporting Cache and Public Reporting data exchange solutions	Hours	386	
	Price	\$50,055.00	
<b>Data Governance &amp; SOC 2 Compliance</b>			
SOC 2 Risk Objectives, Control Objectives, and Policies	Hours	386	
	Price	\$50,055.00	
SOC 2 Compliance Processes & Procedures	Hours	386	
	Price	\$50,055.00	
Support for establishment of Data Governance strategy and approach	Hours	386	
	Price	\$50,055.00	
Definition of Data Use criteria	Hours	386	
	Price	\$50,055.00	
Automation of Data Governance process(es) including Certification and Attestation for data use	Hours	386	
	Price	\$50,055.00	
Documentation of Data Use Governance Policies & Procedures	Hours	386	
	Price	\$50,055.00	
Development of Data Governance Awareness training, compliance, and certification	Hours	386	
	Price	\$50,055.00	
Declaration and implementation of Data Governance Audit(s)	Hours	386	
	Price	\$50,055.00	
<b>IT Enterprise Management</b>			
Policies & Procedures documentation	Hours	386	
	Price	\$50,055.00	
Revision of Source Data Entity Catalog	Hours	386	
	Price	\$50,055.00	
Data Platform IT Service Catalog(s) and Service Level definition & documentation	Hours	386	
	Price	\$50,055.00	
<b>UX/UI Approaches, Tools, and Deliverables</b>			
Discovery and strategic road mapping for User Experience (near and long-term)	Hours	136	
	Price	\$18,075.71	
User types/roles, tasks, and experience-based priorities	Hours	136	
	Price	\$18,075.71	
User story generation and cataloging (features/functionality suite)	Hours	136	
	Price	\$18,075.71	
Rapid Prototyping for UX & UI design (clickable, codeless)	Hours	136	
	Price	\$18,075.71	
User flows, navigation models, and information flows	Hours	136	
	Price	\$18,075.71	
UI mockups, low-fidelity wireframes, and high-fidelity wireframes	Hours	136	
	Price	\$18,075.71	
Business rules implications, validations, and constraints	Hours	136	
	Price	\$18,075.71	
Style standards, documentation, and controls	Hours	136	
	Price	\$18,075.71	
Multi-workstream Agile-driven sprint release approach	Hours	136	
	Price	\$18,075.71	
Angular v12 Components	Hours	136	
	Price	\$18,075.71	
<b>Feature Deliverables</b>			
Design and development of UX/UI for Manage Roadside Vendor Data Exchange (TCS DEX)	Hours	136	
	Price	\$18,075.71	
Design and development of UX/UI for Manage CUSIOP Hub Data Exchanges (Hub DEX)	Hours	136	
	Price	\$18,075.71	
Design and development of UX/UI for Manage PBM Data Exchanges (PBM DEX)	Hours	136	
	Price	\$18,075.71	
Design and development of UX/UI for Manage General Transaction Processing Day to Day needs	Hours	136	
	Price	\$18,075.71	
Design and development of UX/UI for Product Management (View List, View Item, Create, Modify, Delete)	Hours	136	
	Price	\$18,075.71	
Design and development of UX/UI for monitoring and reporting of automated business process(es) for payor ID and payment path routing logic	Hours	136	
	Price	\$18,075.71	
Design and development of UX/UI for Discount Management (View List, View Item, Create, Modify, Delete)	Hours	136	
	Price	\$18,075.71	
Design and development of UX/UI for Billing Management (View List, View Item, Create, Modify, Delete)	Hours	136	
	Price	\$18,075.71	
Development of UX/UI for monitoring and reporting of automated business process(es) for end-to-end Transaction Pricing, Discounting & Billing process(es)	Hours	136	
	Price	\$18,075.71	
Development of UX/UI for monitoring and reporting of automated business process(es) for Public Reporting metrics & performance	Hours	136	
	Price	\$18,075.71	
Design and development of UX/UI for administration and facilitation of Data Governance process(es)	Hours	136	
	Price	\$18,075.71	
<b>Total Hours by Role</b>		<b>14,450</b>	
<b>Total Price by Role</b>		<b>\$1,881,240</b>	



The Deloitte logo is positioned in the top left corner of the slide. It consists of the word "Deloitte" in a bold, white, sans-serif font, followed by a small green dot. The background of the slide is a photograph of the Texas State Capitol building in Austin, Texas, with a street scene in the foreground. The building is a large, classical-style structure with a prominent dome. The street is lined with trees, and there are several people walking across the street. The overall scene is captured in a slightly desaturated, high-angle perspective.

**Deloitte.**

**Central Texas Regional  
Mobility Authority:**

**Data Platform Services**

**Release 3 & TOMS – Pricing  
Updates**

**Sept 7, 2021**



# Agenda

- Release 3 Scope and Deliverables
- TOMS Scope, Requirements and Deliverables
- Pricing & Project Timeline Information



# Release 3 – Revised High-Level Scope and Assumptions

Category	Detail
High Level Scope	<ul style="list-style-type: none"> <li>• <b>Plan &amp; Strategy</b> <ul style="list-style-type: none"> <li>○ Conduct up to 8 Discovery/Design Sessions</li> </ul> </li> <li>• <b>Tolling Product Management</b> <ul style="list-style-type: none"> <li>○ Design &amp; Develop Database Model</li> <li>○ Design &amp; Develop (~2) Data Processing routines for 2 active current products</li> <li>○ Develop/Modify required Payor ID and Payment routing Process</li> </ul> </li> <li>• <b>Discount Management</b> <ul style="list-style-type: none"> <li>○ Design &amp; Develop Discount Database Model</li> <li>○ Design &amp; Develop (~5) Discount Data Processing routines</li> <li>○ Integrate Product and Discount Management Process</li> </ul> </li> <li>• <b>Invoice Management</b> <ul style="list-style-type: none"> <li>○ Design &amp; Develop Invoice Database Model</li> <li>○ Design &amp; Develop (~9) automated Invoice Data Processing routines</li> <li>○ Integrate Product and Discount Management Process with Invoicing</li> </ul> </li> <li>• <b>Data Exchange Management</b> <ul style="list-style-type: none"> <li>○ Design &amp; Develop (~5) Data Processing/Exchange Routines to support DMV, PBM etc.</li> <li>○ Modify required existing Data Exchange Routines (~10) related to CUSIOP, PBM, TCS etc.,</li> </ul> </li> <li>• <b>Reporting Cache &amp; Reporting Management</b> <ul style="list-style-type: none"> <li>○ Create Reporting Data Model in BigQuery to support Public Reporting</li> <li>○ Design &amp; Develop (~20) Data transfer routines from master data source to reporting cache</li> <li>○ Install and Configure GCP Looker Service tool</li> <li>○ Develop up to 8 Public Reports/API Services and 5 Looker Reports to support Operational Monitoring</li> </ul> </li> <li>• <b>Data Governance &amp; IT Enterprise Management</b> <ul style="list-style-type: none"> <li>○ Define relevant SOC 2 Compliance Processes &amp; Procedures</li> <li>○ Documentation of Data Governance Policies &amp; Procedures</li> <li>○ Development of Data Governance Awareness training, compliance, and certification</li> <li>○ Declaration and implementation of Data Governance Audit(s)</li> <li>○ Revision of Source Data Entity Catalog</li> <li>○ Data Platform IT Service Catalog(s) and Service Level definition &amp; documentation</li> </ul> </li> </ul>

# Release 3 – Revised High-Level Scope and Assumptions

Category	Detail
High Level Scope	<ul style="list-style-type: none"> <li>• <b>Testing and Go-Live</b> <ul style="list-style-type: none"> <li>○ Perform end to end testing of Release 3 system changes and coordinate with CTRMA/external stakeholders for User Acceptance testing (~400 test cases)</li> <li>○ Transition of operations post Go-Live to Run and Operate team</li> </ul> </li> </ul>
Assumptions	<ul style="list-style-type: none"> <li>▪ This solution is based on existing Google Cloud Platform (GCP)</li> <li>▪ CTRMA will procure any additional required software licenses and services per mutual agreement</li> <li>▪ GCP Cloud consumption cost is not included on the pricing</li> <li>▪ CTRMA business teams and SME to be available for requirements discovery and design review sessions</li> <li>▪ CTRMA payments are processed by an external third party and either of PCI-DSS Self-Assessment Questionnaire (SAQ) A or A-EP shall be applicable wherein Deloitte team shall support CTRMA in completing the questionnaire (if applicable)</li> <li>▪ Deloitte will leverage existing procedures and processes wherever applicable</li> <li>▪ Data governance activities will leverage DPS data dictionary and attribute list</li> <li>▪ Deloitte shall update or create up to 10 procedures as a part of CTRMA Data Platform documentation</li> <li>▪ Policy and procedure documentation will be limited to relevant IT, security, and compliance components in-scope for the CTRMA Data Platform</li> <li>▪ Duration excludes 3 weeks of holiday break</li> <li>▪ Coordinate and conduct 6 weeks of UAT with HUB and PBM vendor</li> <li>▪ Scope adjusted based on active products and corresponding discounts &amp; invoices</li> <li>▪ Test scenarios/ Test cases will be provided related to production business situations/operational items</li> <li>▪ CTRMA team will support with production data to verify and validate DPS codebase functionality/performance</li> <li>▪ Data Use Criteria and Data Entity Catalog Deliverables will be combined</li> <li>▪ Security Deliverables will be combined into one document as appropriate with sections detailing the content of stated deliverables</li> </ul>
Out of Scope	<ul style="list-style-type: none"> <li>▪ Historic Data Migration/conversion</li> <li>▪ Operate and Production Support services</li> <li>▪ PCI-DSS certification and SOC2 attestation</li> <li>▪ Reporting for public access and viewing</li> </ul>

# TOMS – High-Level Scope and Assumptions

Category	Detail
High Level Scope	<p><b>Plan &amp; Strategy</b></p> <ul style="list-style-type: none"> <li>▪ Conduct 1-3 discovery sessions with 4-6 key stakeholders to gather and identify design and functionality requirements*</li> </ul> <p><b>UI/UX Features</b></p> <p><b>Data Exchange Management</b></p> <ul style="list-style-type: none"> <li>▪ Design &amp; Development of UX/UI to manage TCS Data Exchange (TCS DEX)</li> <li>▪ Design &amp; Development of UX/UI to manage CUSIOP Hub Data Exchange (Hub DEX)</li> <li>▪ Design &amp; Development of UX/UI to manage PBM Data Exchange (PBM DEX)</li> <li>▪ Design &amp; Development of UX/UI to manage General Transactional Processing Day To Day Needs</li> </ul> <p><b>Product Management</b></p> <ul style="list-style-type: none"> <li>▪ Design &amp; Development of UX/UI for Product Management (View &amp; List Items and support CRUD Ops)</li> <li>▪ Design &amp; Development of UX/UI for Monitoring Payor ID &amp; Payment Path Routing Logic, managing Pricing Adjustments</li> </ul> <p><b>Discount Management</b></p> <ul style="list-style-type: none"> <li>▪ Design &amp; Development of UX/UI for Managing Discount Types, Discount Programs and Discount Pricing</li> </ul> <p><b>Billing Management</b></p> <ul style="list-style-type: none"> <li>▪ Design &amp; Development of UX/UI for Managing Billing (View &amp; List Items and support CRUD Ops)</li> <li>▪ Design &amp; Development of UX/UI for Monitoring and Managing of automated processes of End-To-End Transaction Pricing, Discounting, Billing</li> </ul> <p><b>Reporting Management</b></p> <ul style="list-style-type: none"> <li>▪ Design &amp; Development of UX/UI for Monitoring of automated business processes for Public Reporting Metrics and Performance</li> </ul> <p><b>Data Governance</b></p> <ul style="list-style-type: none"> <li>▪ Design &amp; Development of UX/UI for Managing Administration and Facilitation of Data Governance processes</li> </ul>

# TOMS – Revised High-Level Scope and Assumptions

Category	Detail
<b>High Level Scope</b>	<p><b>UI/UX Approaches and Tools</b></p> <ul style="list-style-type: none"> <li>▪ Provide user types/roles, tasks, and experience-based priorities as needed</li> <li>▪ User story generation and cataloging (features/functionality suite)*</li> <li>▪ Provide experience architecture - application map, user flows, navigation models, and key workflows</li> <li>▪ Create all necessary UI screen mockups, zone diagrams &amp; wireframes</li> <li>▪ Create prototypes (clickable, codeless) as needed to demonstrate interaction design</li> <li>▪ Business rules implications, validations, and constraints</li> <li>▪ Develop design system guide: style standards, templates, components, and proposed governance</li> <li>▪ Sprint planning: Multi-workstream Agile-driven sprint release approach</li> <li>▪ Deliver code as Angular v12 Components</li> </ul> <p><b>Testing</b></p> <ul style="list-style-type: none"> <li>▪ Conduct and facilitate design validation testing and UAT testing with CTRMA stakeholders</li> <li>▪ Perform Functional Testing including accessibility/performance</li> </ul>
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ *Any features/functionality identified as future enhancements (i.e., not to be not delivered in current phase) will be added to a future state backlog and will require additional scope to conduct a vision workshop and provide a strategic experience roadmap.</li> <li>▪ QA will be required for functional / accessibility (508) testing and to help with visual QA based on front-end designs.</li> <li>▪ Existing DPS UI application framework will be extended for TOMS</li> </ul>
<b>Out of Scope</b>	<ul style="list-style-type: none"> <li>▪ <b>Any internal and external reporting tied with UI/UX will be addressed in CTRMA future Release 4</b> <ul style="list-style-type: none"> <li>▪ DEX Reporting</li> <li>▪ Product Reporting</li> <li>▪ Payment Path Reporting</li> <li>▪ Discount Reporting</li> <li>▪ Invoice Reporting</li> <li>▪ Reporting &amp; Analytics Management</li> <li>▪ Quality Management</li> <li>▪ Case Management</li> </ul> </li> </ul>



# Release 3 – Revised Deliverable Schedule

Proposed Release 3 deliverable/payment schedule information

No.	Deliverables	Estimated Sprint Schedule	Estimated Week Ending	Estimated Due Date*	Payment Amount
1	Development and deployment of Product database(s) and relationships	2	4	10/30/2021	\$50,055
2	Design and development of automated Product Management process(es)	2	4	10/30/2021	\$50,055
3	Development of automated business process(es) for payor ID and payment path routing logic	2	4	10/30/2021	\$50,055
4	Development and deployment of Discount database(s) and relationships	4	9	12/3/2021	\$50,055
5	Design and development of automated Discount Management process(es)	4	9	12/3/2021	\$50,055
6	Integration of Discount Management with Product Management processes	4	9	12/3/2021	\$50,055
7	Development and deployment of Invoice database(s) and relationships	5	11	12/17/2021	\$50,055
8	Design and development of automated Invoice Management process(es)	5	11	12/17/2021	\$50,055
9	Integration of Invoice Management with Product and Discount Management	5	11	12/17/2021	\$50,055
10	Design, development, and testing for Pay by Mail('PBM') Invoice data exchange modifications (Fixed file, API, XML, JSON)	6	15	1/14/2022	\$50,055
11	Design, development, and testing for IOP Hub Invoice data exchange modifications (Fixed file, API, XML, JSON)	6	15	1/14/2022	\$50,055
12	Development of DMV Hub database(s) and relationships	6	15	1/14/2022	\$50,055
13	Design, development, and testing for external DMV Hub data exchanges (Fixed file, API, XML, JSON)	7	17	1/28/2022	\$50,055
14	Design, development, and testing for Public Reporting data exchange (Fixed file, API, XML, JSON, GitHub)	7	17	1/28/2022	\$50,055
15	Development of Reporting Cache data platform	7	17	1/28/2022	\$50,055
16	Development of Public Reporting database(s) and relationships	8	19	2/11/2022	\$50,055
17	Implementation and testing of Public Reporting data push from master data source to Reporting Cache	8	19	2/11/2022	\$50,055
18	Development of automated Public Report(s) generation	8	19	2/11/2022	\$50,055
19	End-to-end testing of Reporting Cache and Public Reporting exchange solutions	9	21	2/25/2022	\$50,055
20	SOC 2 Risk Objectives, Control Objectives, and Policies	9	21	2/25/2022	\$50,055
21	SOC 2 Compliance Processes & Procedures	9	21	2/25/2022	\$50,055
22	Support for establishment of Data Governance strategy and approach	9	21	2/25/2022	\$50,055
23	Definition of Data Use criteria	9	21	2/25/2022	\$50,055
24	Automation of Data Governance process(es) including certification and affirmation for data use	9	21	2/25/2022	\$50,055
25	Documentation of Data Governance Policies & Procedures	9	21	2/25/2022	\$50,055
26	Development of Data Governance Awareness training, compliance, and certification	10	23	3/11/2022	\$50,055
27	Declaration and implementation of Data Governance Audit(s)	10	23	3/11/2022	\$50,055
28	Policies & Procedures documentation	10	23	3/11/2022	\$50,055
29	Revision of Source Data Entity Catalog	11	25	3/28/2022	\$50,055
30	Data Platform IT Service Catalog(s) and Service Level definition & documentation	11	25	3/28/2022	\$50,055
				<b>Sub-Total</b>	<b>\$1,501,650</b>

# TOMS - Deliverable Schedule

Proposed TOMS deliverable/payment schedule information

No.	Deliverables	Estimated Sprint Schedule	Estimated Week Ending	Estimated Due Date*	Payment Amount
1	Discovery and strategic road mapping for User Experience (near and long-term)	4	9	12/3/2021	\$18,075
2	User types/roles, tasks, and experience-based priorities	4	9	12/3/2021	\$18,075
3	User story generation and cataloging (features/functionality suite)	4	9	12/3/2021	\$18,075
4	Rapid Prototyping for UX & UI design (clickable, codeless)	5	11	12/17/2021	\$18,075
5	User flows, navigation models, and information flows	5	11	12/17/2021	\$18,075
6	UI mockups, low-fidelity wireframes, and high-fidelity wireframes	5	11	12/17/2021	\$18,075
7	Business rules implications, validations, and constraints	6	15	1/14/2022	\$18,075
8	Style standards, documentation, and controls	6	15	1/14/2022	\$18,075
9	Multi-workstream Agile-driven sprint release approach	6	15	1/14/2022	\$18,075
10	Angular v12 Components	7	17	1/28/2022	\$18,075
11	Design and development of UX/UI for Manage Roadside Vendor Data Exchange (TCS DEX)	7	17	1/28/2022	\$18,075
12	Design and development of UX/UI for Manage CUSIOP Hub Data Exchanges (Hub DEX)	7	17	1/28/2022	\$18,075
13	Design and development of UX/UI for Manage PBM Data Exchanges (PBM DEX)	8	19	2/11/2022	\$18,075
14	Design and development of UX/UI for Manage General Transaction Processing Day to Day needs	8	19	2/11/2022	\$18,075
15	Design and development of UX/UI for Product Management (View List, View Item, Create, Modify, Delete)	8	19	2/11/2022	\$18,075
16	Design and development of UX/UI for monitoring and reporting of automated business process(es) for payor ID and payment path routing logic	9	21	2/25/2022	\$18,075
17	Design and development of UX/UI for Discount Management (View List, View Item, Create, Modify, Delete)	9	21	2/25/2022	\$18,075
18	Design and development of UX/UI for Billing Management (View List, View Item, Create, Modify, Delete)	9	21	2/25/2022	\$18,075
19	Development of UX/UI for monitoring and reporting of automated business process(es) for end-to-end Transaction Pricing, Discounting & Billing process(es)	10	23	3/11/2022	\$18,075
20	Development of UX/UI for monitoring and reporting of automated business process(es) for Public Reporting metrics & performance	10	23	3/11/2022	\$18,075
21	Design and development of UX/UI for administration and facilitation of Data Governance process(es)	10	23	3/11/2022	\$18,090
				<b>Sub-Total</b>	<b>\$379,590</b>
				<b>Total</b>	<b>\$1,881,240</b>

\* Based on project state date of 10/4/21



# Pricing & Productivity Gain Synopsis – From Release 1 & 2 to 3

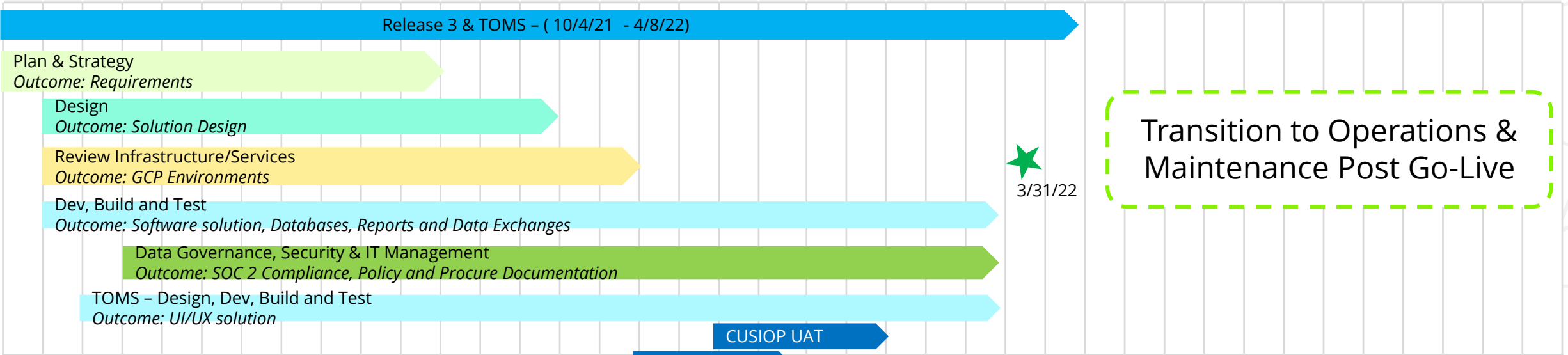
We have leveraged knowledge, experience and expertise from the execution of Release 1 & 2 to optimize delivery approach and estimates of Release 3 and TOMS

Release	No. of Deliverables	No. of Sprints	Total Fees	Fees / Deliverable
Release 1 & 2	17	12	\$1,540,860	\$90,639
Release 3 with TOMS	51	12	\$1,881,240	\$36,887
<b>Productivity Gain / Deliverable</b>	<b>Release 3 with TOMS - 59% Productivity Gain Over Release 1&amp;2</b>			

# Release 3 & TOMS – Timeline and Sprint Plan

Data Platform Services Release 3 Requirements and TOMS is expected to occur during Fall 2021 to early Summer 2022.

Release 3																																						
2021													2022																									
October				November				December					January				February				March			April			May			June								
Sprint 1		Sprint 2		Sprint 3		Sprint 4		Sprint 5			Holiday Break		Sprint 6		Sprint 7		Sprint 8		Sprint 9		Sprint 10		Sprint 11		Sprint 12		Sprint 13		Sprint 14		Sprint 15		Sprint 16		Sprint 17		Sprint 18	
Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15	Week 16	Week 17	Week 18	Week 19	Week 20	Week 21	Week 22	Week 23	Week 24	Week 25	Week 26	Week 27	Week 28	Week 29	Week 30	Week 31	Week 32	Week 33	Week 34	Week 35	Week 36	Week 37	Week 38	Week 39
10/4	10/11	10/18	10/25	11/1	11/8	11/15	11/22	11/29	12/6	12/13	12/20	12/27	1/3	1/10	1/17	1/24	1/31	2/7	2/14	2/21	2/28	3/7	3/14	3/21	3/28	4/4	4/11	4/18	4/25	5/2	5/9	5/16	5/23	5/30	6/6	6/13	6/20	6/27
10/8	10/15	10/23	10/30	11/5	11/12	11/19	11/26	12/3	12/10	12/17	12/24	12/31	1/7	1/14	1/21	1/28	2/4	2/11	2/18	2/25	3/4	3/11	3/18	3/28	4/2	4/8	4/15	4/22	4/29	5/6	5/13	5/20	5/27	6/3	6/10	6/17	6/24	7/2



- ◆ **Deploy Product Management**
- ◆ **Deploy Discount Management**
- ◆ **Deploy Invoice Management**
- ◆ **Deploy PBM, DMV & DX**
- ◆ **Deploy Reporting Cache Platform**
- ◆ **Governance & IT Management**

## 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**

**CENTRAL TEXAS REGIONAL  
MOBILITY AUTHORITY**

---

Uday Katira, Managing Director  
Deloitte Consulting LLP

---

James Bass  
Executive Director

---

Date

---

Date

## DIR Vendor Agreement

This is to signify that the Central Texas Regional Mobility Authority and Deloitte Consulting LLP Corporation have entered into an Agreement **in an amount not to exceed \$2,069,364** (*amount includes a 10% project contingency; does not include required hardware, software or software licenses*) pursuant to Texas Government Code Section 2054.0565 utilizing Texas Department of Information Resources Contract No. #DIR-TSO-4031 for the deliverable-based information technology services described in this proposal. All terms and conditions of Texas Department of Information Resources Contract No. #DIR-TSO-4031 are applicable to and made part of this agreement.

**DELOITTE CONSULTING LLP**

**CENTRAL TEXAS REGIONAL  
MOBILITY AUTHORITY**

---

Uday Katira, Managing Director  
Deloitte Consulting LLP

---

James Bass  
Executive Director

---

Date

---

Date



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
**AGENDA ITEM #10**

---

Potential options for aesthetic  
improvements to the Montopolis  
Bridge

Strategic Plan Relevance: Regional Mobility  
Department: Engineering  
Contact: Mike Sexton, Acting Director of Engineering  
Associated Costs: N/A  
Funding Source: N/A  
Action Requested: Briefing and Board Discussion Only

**Project Description/Background:**

Presentation on options for aesthetic improvements to the Montopolis Bridge.

**Backup provided:** None



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
AGENDA ITEM #11

---

Executive Director Board Report

Strategic Plan Relevance: Regional Mobility  
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:**

A. Resumption of Pay by Mail invoicing related to TxTag processing.

**Backup provided:** None



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
AGENDA ITEM #12

---

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 29, 2021  
AGENDA ITEM #13

---

Executive Session

*Executive Session:*

Discuss legal issues relating to procurement and financing of Mobility Authority transportation projects, as authorized by §551.071 (Consultation with Attorney).





CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
AGENDA ITEM #14

---

Executive Session

*Executive Session:*

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



CENTRAL TEXAS REGIONAL  
**MOBILITY AUTHORITY**

September 29, 2021  
AGENDA ITEM #15

---

Adjourn Meeting

Adjourn Board Meeting.