

RESOLUTION NO. \_\_\_\_\_

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF MESQUITE, TEXAS, AUTHORIZING THE CITY MANAGER TO EXECUTE AGREEMENTS WITH TEXAS DEPARTMENT OF TRANSPORTATION FOR THE SHARING OF INTELLIGENT TRANSPORTATION SYSTEMS (ITS) DATA AND TRAFFIC VIDEO BETWEEN THE DEPARTMENT AND CITY FOR FIVE YEARS; AND PROVIDING AN EFFECTIVE DATE THEREOF.

WHEREAS, the City of Mesquite (the “City”) has requested and the Texas Department of Transportation (“TxDOT”) has agreed to share information regarding intelligent transportation systems (“ITS”) data and traffic video; and

WHEREAS, the Interlocal Cooperation Act, V.T.C.A., Texas Government Code, Chapter 791, provides authorization for any local government to contract with one or more local governments to perform governmental functions and services under the terms of the Act; and

WHEREAS, agreements between the City and TxDOT will allow the sharing of ITS data and traffic video between TxDOT and the City for a period of five years.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF MESQUITE, TEXAS:

SECTION 1. That the City Manager is hereby authorized to execute the Agreement for Sharing Intelligent Transportation Systems (ITS) Data and the Agreement for Sharing Traffic Video, attached hereto as Exhibits A and B, respectively, between the City of Mesquite and the Texas Department of Transportation for a term of five years once the Agreements are fully executed.

DULY RESOLVED by the City Council of the City of Mesquite, Texas, on the 17th day of October 2022.

---

Daniel Alemán, Jr.  
Mayor

ATTEST:

APPROVED:

---

Sonja Land  
City Secretary



---

David L. Paschall  
City Attorney

STATE OF TEXAS §  
COUNTY OF TRAVIS §

**AGREEMENT for SHARING  
INTELLIGENT TRANSPORTATION SYSTEMS (ITS) DATA**

**EXHIBIT A**

**CONTRACTING PARTIES:**

Texas Department of Transportation	<b>TxDOT</b>
Dallas District	
City of Mesquite	<b>Grantee</b>

TxDOT is the owner of Intelligent Transportation Systems (ITS) infrastructure that consists of:

- an ITS Field Network (including but not limited to sensors, cameras, signs, and communications links constructed along segments of the State highway system); and
- an ITS Business Network that has produced and produces transportation-related information that is used for the purpose of traffic management in which the State owns certain rights, title, and interests related thereto, including copyrights.

The Grantee desires TxDOT to grant rights to receive and use TxDOT transportation-related information (“Traffic Data”). TxDOT is agreeable to grant rights provided the Grantee agrees to the terms and conditions established in this agreement.

This agreement incorporates the provisions of **Attachment A**, Descriptions and Specifications of Rights Granted in Article 2, **Attachment B**, Guidelines for Use of State Equipment and Infrastructure, **Attachment C**, Information Resources and Security Requirements, and **Attachment D**, Connectivity Diagram.

**BACKGROUND**

TxDOT, in accordance with Texas Transportation Code, §201.205, may:

1. Apply for, register, secure, hold and protect its intellectual property, patents, copyrights, trademarks, or other evidence of protection of exclusivity; and
2. Enter into non-exclusive license agreements with any third party for the receipt of fees, royalties, or other things of monetary and non-monetary value; and
3. Waive or reduce the amount of fees if it determines that such waiver will further the goal and missions of TxDOT and result in a net benefit to TxDOT; and

Texas Transportation Code, §202.052 authorizes TxDOT to lease highway assets if the area to be leased is not needed for highway purposes during the term of the lease and TxDOT charges fair market value for the leased asset, and authorizes TxDOT to waive such fees for social, economic, and environmental mitigation purposes.

TxDOT – alone or as a stakeholder in multiple regional traffic management centers (TMCs), the regional traffic management center (TMC) – has trademark registrations on marks in accordance with the requirements of Title 15 U.S.C. Section 1051 et seq., as amended:

- Registration Number 1802491, hereinafter identified as the “TxDOT Logo.”
- Registration Number 3027037, hereinafter identified as the “DalTrans Logo.”

**AGREEMENT**

In consideration of the mutual promises contained in this agreement, TxDOT and the Grantee now agree as follows:

**ARTICLE 1. CONTRACT PERIOD**

This agreement becomes effective when signed and dated by the last party whose signing makes the agreement fully executed. This agreement shall terminate five (5) years from that date, or when otherwise modified or terminated, as hereinafter provided.

**ARTICLE 2. RIGHTS GRANTED**

TxDOT hereby grants the Grantee a non-exclusive right, license, and privilege worldwide to use all or portions of Traffic Data from TxDOT’s ITS Field Network and ITS Business Network. The Grantee agrees that this agreement does not transfer or convey any ownership or any rights other than those rights expressly granted by the agreement.

TxDOT further agrees to provide connectivity to Grantee to access TxDOT Traffic Data as described in Attachment A to this agreement, which is attached hereto and incorporated herein for all purposes.

### **ARTICLE 3. PROVISION OF INFRASTRUCTURE**

The Grantee is responsible for providing and maintaining any hardware, software, and additional ITS infrastructure that is necessary to obtain the Traffic Data. TxDOT may provide unused ITS infrastructure and TxDOT facilities to support the additional infrastructure when possible, and when deemed to be in the best interest of TxDOT. Grantee agrees that TxDOT does not guarantee the availability of the Traffic Data or a minimum response time to reestablish the availability of the Traffic Data due to maintenance or network or system failures. A more detailed description of ITS infrastructure to be provided by each party is shown in Attachment A. The Grantee shall not place any objects or equipment in the State Right-of-Way or on any other TxDOT property without advanced written permission from the District Engineer or designee.

### **ARTICLE 4. FEE**

As the use of the Traffic Data will result in social, economic, and environmental mitigation, by increasing mobility and reducing congestion on public highways, TxDOT agrees to waive any monetary fee associated with the use of the Traffic Data. After the initial year, TxDOT reserves the right to charge a fee for the use of the Traffic Data by providing not less than thirty (30) days written notice to the Grantee defining the terms of the fee.

### **ARTICLE 5. COPYRIGHT INFRINGEMENT**

The Grantee shall notify TxDOT of any infringement or potential infringement by a third party, of which it becomes aware, of the copyright or any other rights owned by TxDOT relating to the use of the Traffic Data. The Grantee shall provide TxDOT, if feasible, any information or other assistance requested by TxDOT to assist in TxDOT's prosecution of any breaches or infringements.

### **ARTICLE 6. TAXES AND FEES**

Grantee agrees to report to the appropriate taxation authority and pay all federal, state, and local taxes or fees that may be imposed by any governmental entity for the use of the Traffic Data.

### **ARTICLE 7. ASSIGNMENT PROHIBITION**

The Grantee is prohibited from assigning any of the rights conferred by this agreement, to any third party. Notwithstanding the foregoing, the Grantee may assign the rights of this agreement of the Traffic Data to an affiliated corporate entity or to a purchaser of substantially all its assets without TxDOT's consent, provided that TxDOT's rights under this agreement remain unaffected. Any assignments shall be subject to the terms and conditions of this agreement.

### **ARTICLE 8. TERMINATION**

- a) Including the provisions established herein, this agreement may be terminated by any of the following conditions.
  - i) Mutual agreement and consent of the parties hereto.
  - ii) By TxDOT for reason of its own and not subject to the approval of the Grantee upon not less than thirty (30) days written notice to the Grantee.
  - iii) By the Grantee for reason of its own and not subject to the approval of TxDOT upon not less than thirty (30) days written notice to TxDOT.
  - iv) Immediately for breach of this agreement as determined by TxDOT.
- b) Termination of the agreement shall extinguish all rights, duties, obligations and liabilities of TxDOT and Grantee of this agreement. All rights granted to the Grantee shall revert to TxDOT as owner of the Traffic Data. Upon termination of this agreement, the Grantee will immediately cease transmitting, using, distributing and/or modifying the electronic signals of the Traffic Data.
- c) Termination or expiration of this agreement shall not extinguish any of the Grantee's or TxDOT's obligations under this agreement which by their terms continue after the date of termination or expiration.

### **ARTICLE 9. HOLD HARMLESS**

The Grantee shall indemnify and save harmless TxDOT and its officers and employees from all claims and liability due to its materials or activities of itself, its agents, or employees, performed under this agreement and that are caused by or result from error, omission, or negligent act of the Grantee or of any person employed by the Grantee. The Grantee shall also indemnify and save harmless TxDOT from any and all expense, including but not limited to attorney fees that may be incurred by TxDOT in litigation or otherwise resisting the claim or liabilities that may be imposed on TxDOT as a result of such activities by the Grantee, its agents, or employees. The Grantee agrees to indemnify and save

harmless TxDOT and its officers, agents, and employees from any and all claims, damages, and attorneys' fees arising from the use of outdated Traffic Data or other information. The Grantee's indemnification of TxDOT shall extend for a period of three (3) years beyond the date of termination of this agreement.

**ARTICLE 10. RELATIONSHIP BETWEEN THE PARTIES**

Each party acknowledges that it is not an agent, servant, or employee of the other party. Each party is responsible for its own acts and deeds and for those of its agents, servants, or employees.

**ARTICLE 11. REMEDIES**

Violation or breach of contract by the Grantee shall be grounds for termination of the agreement. Any increased costs arising from the Grantee's default, breach of contract or violation of contract terms shall be paid by the Grantee.

**ARTICLE 12. AMENDMENTS**

Any changes in the contract period, character, or agreement terms shall be enacted by a written amendment executed by both parties. Amendments must be executed during the contract period established in Article I.

**ARTICLE 13. VENUE**

This agreement is governed by the laws of the State of Texas.

**ARTICLE 14. NOTICES**

All notices to either party by the other party required under this agreement shall be delivered personally or sent by certified or U.S. Mail, postage prepaid, addressed to such party at the following respective physical addresses:

**STATE:** Texas Department of Transportation  
ATTN: Director of Operations  
4777 East Highway 80  
Mesquite, TX 75150-6643

**GRANTEE:** City of Mesquite  
ATTN: Manager of Traffic Engineering and Street Lighting  
1515 North Galloway Avenue  
Mesquite, Texas 75149

and shall be deemed to be received by the addressee on the date so delivered or so deposited in the mail, unless otherwise provided within. Either party hereto may change the above address by sending written notice of such change to the other.

**ARTICLE 15. PUBLIC INFORMATION AND CONFIDENTIALITY**

A. To the extent permitted by law, the Grantee shall not disclose information obtained from TxDOT under this agreement without the express written consent of TxDOT.

B. The Grantee is required to make any information created or exchanged with the state pursuant to this contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the state.

**ARTICLE 16. COMPLIANCE WITH LAWS**

The Grantee shall comply with all applicable federal, state, and local laws, statutes, ordinances, rules and regulations, and with the orders and decrees of any court or administrative bodies or tribunals in any manner affecting the performance of this agreement. When requested, the Grantee shall furnish TxDOT with satisfactory proof of this compliance. The Grantee shall provide or obtain all applicable permits, plans, or other documentation required by a federal or state entity.

**ARTICLE 17. COMPLIANCE WITH INFORMATION TECHNOLOGY REQUIREMENTS**

The third party will be creating, accessing, transmitting, storing, or using public data in the third-party environment. The third-party's environment must comply with the TxDOT Low security baseline.

A copy of the TxDOT Information Security Controls Standards Catalog that outlines the security baseline requirements can be downloaded from

<https://www.txdot.gov/inside-txdot/division/information-technology/Cybersecurity/cybersecurity-resources.html>.

The third party must provide evidence that the third-party system is compliant with the TxDOT Low security baseline prior to any Public TxDOT data being created, accessed, transmitted, used, or stored in the third-party environment.

**ARTICLE 18. PROHIBITION AGAINST VIDEOTAPING OF TxDOT VIDEO FEED**

Grantee further agrees that it shall not copy nor duplicate, or allow to be copied, any of the video feeds that are provided by TxDOT in connection with this agreement, but Grantee shall, if it is a media outlet, have permission to maintain recorded footage from the provided video feeds that became part of its regular programming.

**ARTICLE 19. STATE AUDITOR'S PROVISION**

The State Auditor may conduct an audit or investigation of any entity receiving funds from TxDOT directly under this agreement or indirectly through a subcontract under this agreement. Acceptance of funds directly under this agreement or indirectly through a subcontract under this agreement acts as acceptance of the authority of the State Auditor, under the direction of the legislative audit committee, to conduct an audit or investigation in connection with those funds. An entity that is the subject of an audit or investigation must provide the State Auditor with access to any information the State Auditor considers relevant to the investigation or audit.

**ARTICLE 20. SIGNATORY WARRANTY**

The signatories to this agreement warrant that each has the authority to enter into this agreement on behalf of the party they represent.

**IN TESTIMONY WHEREOF**, TxDOT and the Grantee have executed duplicate counterparts of this agreement.

**CITY OF MESQUITE**

By \_\_\_\_\_ Date \_\_\_\_\_  
Cliff Keheley, City Manager

**THE STATE OF TEXAS**

Executed for the Executive Director and approved for the Texas Transportation Commission for the purpose and effect of activating and/or carrying out the orders, established policies or work programs heretofore approved and authorized by the Texas Transportation Commission.

By \_\_\_\_\_ Date \_\_\_\_\_  
Mohamed K. Bur, P.E., Dallas District Engineer

**ATTACHMENT A**  
**Descriptions and Specifications of Rights Granted**

<b>RIGHTS GRANTED</b>	
<b>By TxDOT</b>	<b>By Grantee</b>
<ol style="list-style-type: none"> <li>1. TxDOT will make its Traffic Data available to Grantee.</li> <li>2. TxDOT will provide TxDOT Lonestar software as a user client at a secure level to be determined by TxDOT.</li> <li>3. TxDOT will provide the Grantee the right to use TxDOT Lonestar software necessary to obtain the Traffic Data.</li> <li>4. TxDOT will provide the Grantee with TxDOT logos for identification of traffic service and information provided by TxDOT. The use of the TxDOT and/or TMC logos is limited to giving TxDOT credit for contributed data. The Grantee shall not use the logos for any other purpose.</li> </ol>	<ol style="list-style-type: none"> <li>1. Grantee will use traffic data to monitor real-time traffic conditions for immediate response to traffic crashes or delays. Grantee shall provide TxDOT with Non-Monetary Compensation as identified below.</li> </ol>

<b>PROVISION OF INFRASTRUCTURE</b>	
<b>By TxDOT</b>	<b>By Grantee</b>
<ol style="list-style-type: none"> <li>1. TxDOT will provide the Grantee a connection into TxDOT's Statewide portal for Grantee to obtain Traffic Data.</li> <li>2. TxDOT will provide and maintain any communication links, hardware, software, and additional ITS infrastructure that is necessary to obtain Grantee's traffic data.</li> <li>3. TxDOT will provide the Grantee with its Center-to-Center (C2C) Development Toolkit needed to develop plug-in software compatible with the C2C infrastructure to extract the Traffic Data.</li> <li>4. TxDOT will provide the Grantee with TxDOT logos for identification of traffic service and information provided by TxDOT. The use of the TxDOT and/or TMC logos is limited to giving TxDOT credit for contributed data. The Grantee shall not use the logos for any other purpose.</li> </ol>	<ol style="list-style-type: none"> <li>1. As described in Article 3-Provision of Infrastructure, the Grantee is responsible for providing and maintaining any communication links, hardware, software, and additional ITS infrastructure that is necessary to obtain the Traffic Data.</li> <li>2. Grantee shall provide TxDOT with (a) verifiable, static, routable IP address(es).</li> </ol>

<b>NON-MONETARY COMPENSATION</b>	
<b>By TxDOT</b>	<b>By Grantee</b>
<ol style="list-style-type: none"> <li>1. none</li> </ol>	<ol style="list-style-type: none"> <li>1. Grantee shall provide TxDOT with a list of IP addresses for all City owned traffic detectors. Grantee shall give TxDOT and/or TMC voice and/or visual credit (TxDOT and/or TMC logos) for all Traffic Data provided by TxDOT. TxDOT may transmit video data to the Grantee with an embedded logo; the Grantee shall not block, modify, or remove the Logo.</li> </ol>

**ATTACHMENT B****Guidelines for Use of State Equipment and Infrastructure**

(Applicable to Rights Granted in Attachment A)

---

**ITS FIELD EQUIPMENT: Closed Circuit Television (CCTV) Cameras; Dynamic Message Sign (DMS); Highway Advisory Radio (HAR) System; Lane Control Signal (LCS) System**

1. During periods of peak traffic flow, access shall normally be limited to TxDOT. Peak traffic flow is normally considered to exist regularly during two periods of the day, Monday through Friday. In general, one period of peak traffic flow exists in the early morning and the other period of peak traffic flow exists in the late afternoon. Additional periods of peak traffic flow may exist at other times during the weekday and weekend due to special events and public gatherings. Precise times of regular and additional anticipated peak periods of traffic flow shall be the sole determination of TxDOT and may change from time to time.
2. During an incident, access shall normally be limited to TxDOT and local emergency service agencies. An incident is defined as any condition in which traffic flow is not normal. As an example, abnormal traffic flow could be caused by debris in the road, such as a mattress or board, or could be caused by non-recurring congestion, such as on-lookers to an automobile accident, public gathering, construction, or roadway maintenance. The duration of the incident shall be considered complete once any TxDOT and/or emergency service personnel and vehicles have departed from the incident scene and traffic flow has returned to normal.
3. During periods described above in which TxDOT normal daily operations have ceased or local emergency service agencies do not operate, access to TxDOT equipment shall be limited to the following:
  - CCTV – pan, tilt, and zoom controls shall be limited to obtaining broad general traffic information. Panning, tilting, or zooming to obtain visual detailed information of an incident scene or traffic flow is limited to TxDOT and emergency service agencies at all times.
  - DMS and HAR – messages shall be limited to a pre-approved library and schedule of broad general traffic information. Removal of existing messages and posting of new messages shall require approval by TxDOT or emergency personnel and be limited to pre-approved library and hierarchy rules for control.
  - LCS – indicators will be turned off. If an incident requires activation of LCS, TxDOT or emergency personnel must be contacted for direction.
4. During all other periods, not described above, access shall be limited to obtaining and providing transportation-related information only.
  - CCTV pan, tilt, and zoom for enforcement and any non-transportation related information purpose is forbidden at any time. A single breach of any of the above guidelines shall be grounds to immediately withdraw the privilege of pan, tilt, and zoom.
  - Changes to DMS, HAR or LCS settings for any non-transportation related information purpose is forbidden at any time. A single breach of any of the above guidelines shall be grounds to immediately withdraw the privilege of DMS, LCS or HAR control.
5. Access to ITS field equipment may be withdrawn at anytime By TxDOT without notice if access is determined to not be in the best interest of TxDOT.

## **ATTACHMENT C**

### **Information Resources and Security Requirements**

#### **1. TYPES OF DATA**

“**TxDOT Data**” means TxDOT information, data, records, and information to which the Contractor has access, has possession, or is otherwise provided to the Contractor by TxDOT, whether or not intended under or for the purposes of the agreement, including, without limitation, data generated or collected under this agreement, intellectual property created as a work for hire under this agreement, and Personal Identifying Information (as defined below).

TxDOT Data is classified into the four categories that control applicability of security standards: Regulated, Confidential, Sensitive, and Public. See Section 4 for Definitions.

Any data that the Contractor accesses and downloads from a TxDOT system, for use, manipulation, storage, or management is considered Confidential Data unless otherwise specified in writing by TxDOT.

#### **2. DATA REQUIREMENTS**

##### **2.1 Data, Data Dictionaries, and Data Flow Diagrams**

Contractor shall ensure that all TxDOT Data that is generated, manipulated, transmitted, or stored, utilizes the TxDOT taxonomy, with documented data dictionaries, and data flow diagrams (including security protocols).

##### **2.2 Data Transfer**

- (a) At the completion of a deliverable, the Contractor shall transfer all TxDOT Data generated and stored for that deliverable to TxDOT in a manner and format acceptable to TxDOT and approved by TxDOT’s Information Technology Division (“**ITD**”).
- (b) All metadata associated with the TxDOT Data transferred must remain attached to that data.
- (c) Contractor shall maintain the appropriate level of data security throughout the transfer of the TxDOT Data.

##### **2.3 Backup and Disaster Recovery**

- (a) Contractor shall implement business continuity procedures to fulfill all requirements of this agreement that address, as a minimum, fire, theft, natural disaster, technical difficulty, workforce problems equipment failure, or other disruption of business.
- (b) Contractor shall maintain a disaster recovery plan. Contractor is responsible for all project related costs of disaster recovery during the project except for costs associated with disasters beyond Contractor’s reasonable control, and for those costs included as part of the TxDOT infrastructure responsibilities.

##### **2.4 Open Records Requests**

Contractor shall not release Information in response to an open record request related to this agreement request unless TxDOT has approved the release in writing.

##### **2.5 Encryption**

For Sensitive, Confidential, and Regulated TxDOT Data, the Contractor shall encrypt the TxDOT Data while in-transit and while at-rest in accordance with the TxDOT Controls Catalog Standard SC-13,

Cryptographic Protection and SC-08, Transmission Confidentiality and Integrity security requirements.

## 2.6 Accessibility

State agencies shall procure products which comply with the State of Texas Accessibility requirements for Electronic and Information Resources specified in 1 Texas Administrative Code (TAC) Chapters 206 and 213 when such products are available in the commercial marketplace or when such products are developed in response to a procurement solicitation. Vendor represents and warrants that technology to be provided to TxDOT and for TxDOT is in compliance with these requirements.

## 3. INFORMATION RESOURCE AND SECURITY REQUIREMENTS

### 3.1 Information Security Safeguards

- (a) Contractor shall implement appropriate administrative, physical, and technical safeguards, in accordance with TxDOT's security requirements, that reasonably and appropriately protects the confidentiality, integrity, and availability of TxDOT Data.
- (b) Contractor shall conform its policies and procedures relating to the implementation of security safeguards to comply with TxDOT's Information Resources security program pursuant to the TxDOT and DIR's Information Security Controls Catalog Standards.

### 3.2 Potential Cybersecurity Incident or Breach Notification

Contractor shall immediately report to TxDOT via the Report Cybersecurity Incident Page on TxDOT.gov, any potential cybersecurity incident or breach involving TxDOT Data (See Section 4, Definitions).

### 3.3 Demonstrating Compliance with Information Security Requirements

Prior to contract award, at renewal, on a recurring basis as documented in the contract, upon reasonable notice to the Contractor, and if TxDOT determines that the Contractor has violated this agreement, TxDOT, directly or through its agent, may request an attestation, which may include the TxDOT Security Questionnaire or additional attestations, and evidence that Contractor is in compliance with applicable laws, regulations, and standards outlined in 3.5.

### 3.4 Security Training

- (a) In accordance with Section 2054.5192 of the Texas Government Code, each Contractor Personnel that will access a TxDOT computer system or database must complete a TxDOT approved cybersecurity training program that is certified under Section 2054.5192 of the Texas Government Code. The training program must be completed by each Contractor Personnel during the term of the contract and during any renewal period. The Contractor shall provide verification of completion of the cybersecurity training program in a method designated by TxDOT.
- (b) In this section 3, "**Contractor Personnel**" means all persons under the control of the Contractor including officers and employees of both the Contractor and its subcontractors.

### 3.5 Applicable Laws, Regulations, and Standards

Contractor shall perform the services in accordance with the following standards, notify TxDOT of situations where compliance is not achievable, and assist TxDOT with the prevention of security gaps or conflicts that could impair security performance. Contractor shall comply with all applicable federal, state, and local laws and regulations necessary to perform the services. A non-exhaustive list of federal, state, and local laws and regulations that might be applicable include the following.

- (1) DIR Security Controls Standard Catalog and applicable TxDOT Security Requirements

- (A) For Public Data, TxDOT and DIR Security Controls Standards Catalog low baseline and applicable TxDOT security requirements.
  - (B) For Sensitive Data TxDOT and DIR Security Controls Standards Catalog low baseline with Sensitive overlay and applicable TxDOT security requirements.
  - (C) For Confidential, TxDOT and DIR Security Controls Standards Catalog moderate baseline and applicable TxDOT security requirements.
  - (D) For Regulated Data, TxDOT and DIR Security Controls Standards Catalog moderate baseline, applicable TxDOT security requirements, and applicable regulated security requirements.
- (2) TX-RAMP Requirements
- (A) Any third party providing a cloud computing service to TxDOT to create, access, transmit, use, or store TxDOT data must be authorized in the Texas Risk and Authorization Management Program (“**TX-RAMP**”)
  - (B) TX-RAMP provisional status may be considered in lieu of a TX-RAMP certification if approved by the TxDOT Chief Information Security Officer (“**CISO**”).
  - (C) Applicable third parties must achieve the following levels of authorization by the following dates for any new contract or renewal of existing contract:
    - a. Low Security Baseline – TX-RAMP Level 1 Status no later than January 1, 2023
    - b. Moderate Security Baseline – TX-RAMP Level 2 Status no later than January 1, 2022
    - c. High Security Baseline – Federal Risk and Authorization Management Program (“**FedRAMP**”) High Baseline no later than January 1, 2022
- (3) State Laws and Regulations:
- (A) Texas Administrative Code, Chapter 202 – Information Security Standards
  - (B) Texas Administrative Code, Chapter 206 – State Websites
  - (C) Texas Administrative Code, Chapter 213 – Electronic and Information Resources
  - (D) Texas Government Code, Chapter 552 – Public Information
  - (E) Texas Government Code, Chapter 2054 – Information Resources
  - (F) Texas Penal Code, Chapter 33 – Computer Crimes
  - (G) For Confidential data, Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information
  - (H) For Confidential data containing Protected Health Information, Texas Health and Safety Code, Chapter 181 – Medical Records Privacy
  - (I) For Regulated data containing Payment Card Industry (PCI) information, the Payment Card Industry Data Security Standards (PCI-DSS)
  - (J) For Regulated data containing Criminal Justice Information (CJI), the Criminal Justice Information Services (CJIS) Security Policy

### 3.6 Information Resources Technology

- (a) Any proposed information resources technology that will be installed on any TxDOT owned equipment or that will access any TxDOT network must be reviewed and approved by the ITD Architectural Review Board (“**ARB**”) prior to any development or design.
- (b) Any proposed information resources technology that will be installed on any TxDOT owned

equipment or that will access any TxDOT network must be reviewed and approved by the ITD Change Advisory Board (“CAB”) prior to implementation or delivery.

### 3.7 Information Resources Technology (“IRT”) Procurements

ITD must approve all procurements of:

- (1) Information Resources Technology that will be owned by TxDOT.
- (2) IT services for any environment that provides processing, storage, networking, management and the distribution of data to ensure alignment with Texas Government Code, Chapter 2054, Subchapter L.

### 3.8 Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

In accordance with 2 CFR §§ 200.216 and 200.471, Contractor shall not provide services, equipment, or systems for telecommunications or video surveillance that (a) are provided or manufactured by or (b) have components provided or manufactured by any of the following business entities:

- (1) Huawei Technologies Company
- (2) ZTE Corporation
- (3) Hyatera Communications Corporation
- (4) Hangzhou Hikvision Digital Technology Company
- (5) Dahua Technology Company
- (6) Any subsidiary or affiliate of an entity listed above

## 4. DEFINED TERMS

- 4.1 “**Breach**” means “breach of system security” as defined in Section 521.053(a) of the Texas Business and Commerce Code, which defines breach of system security as “the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.”
- 4.2 “**Cloud Computing Service**” means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is referenced in Texas Government Code Title 10, Subtitle D, Chapter 2157, Subchapter A, Section 2157.007 and is defined in NIST 800-145.
- 4.3 “**Confidential Information**” has the meaning provided in 1 Texas Administrative Code § 202.1(5), which states the confidential information means “information that must be protected from unauthorized disclosure or public release based on published laws or legal agreements.” Information that is Confidential Information under this definition includes:
  - (a) Dates of birth of living persons
  - (b) Driver’s license numbers
  - (c) License plate numbers
  - (d) Credit card numbers
  - (e) Insurance policy numbers
  - (f) Attorney-Client communications
  - (g) Drafts of policymaking documents

- (h) Information related to pending litigation
  - (i) Audit working papers
  - (j) Competitive bidding information before contract awarded.
  - (k) Personal Identifiable Information
  - (l) Sensitive Personal Information
  - (m) Regulated data
  - (n) Information excepted from disclosure requirements of Chapter 552 of the Texas Government Code ("**Texas Public Information Act**") or other applicable state or federal law
  - (o) Compliance reports for which the Texas Attorney General has granted permission to withhold
  - (p) Investigative working papers and draft reports excepted from disclosure under Section 552.116 of the Texas Government Code
- 4.4 "**Data**" means the representation of facts; as the raw material of information that is used as a basis for reasoning, decision-making, discussion, or calculation.
- 4.5 "**Data Dictionary**" means a directory of the definitions, purpose, policies and structure about data. It is a compilation of information about the data owned by the enterprise. It describes every data item in a database in enough detail for users and application developers to know what the data is and how to make use of it.
- 4.6 "**Information**" means data, regardless of form, that is created, contained in, or processed by information resources facilities, communications networks, or storage media.
- 4.7 "**Information Resources Technology**" means data processing and telecommunications hardware, software, services, supplies personnel, facility resources, maintenance and training that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.
- 4.8 "**Personal Identifying Information**" means information that alone or in conjunction with other information identifies an individual, including an individual's:
- (a) Name, social security number, date of birth, or government-issued identification number;
  - (b) Mother's maiden name;
  - (c) Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
  - (d) Unique electronic identification number, address, or routing code; and
- 4.9 "**Potential Cybersecurity Incident**" means an event which may result in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.
- 4.10 "**Public Data**" means Data that is subject to public disclosure pursuant to the Texas Public Information Act and freely and without reservation made available to the public.
- 4.11 "**Public information**" means information written, produced, collected, assembled, or maintained by or for a governmental body, including information held by individual officers or employees of a governmental body, in connection with the transaction of official TxDOT business. This includes information that is held by contractors and consultants and that TxDOT owns, to which TxDOT has a right of access, or on which public money was spent for the purpose of writing, producing, collecting, assembling, or maintaining the information. Public information includes any electronic communication created, transmitted, received, or maintained on any device if the communication is in connection with the transaction of official business. Public information may be stored in any

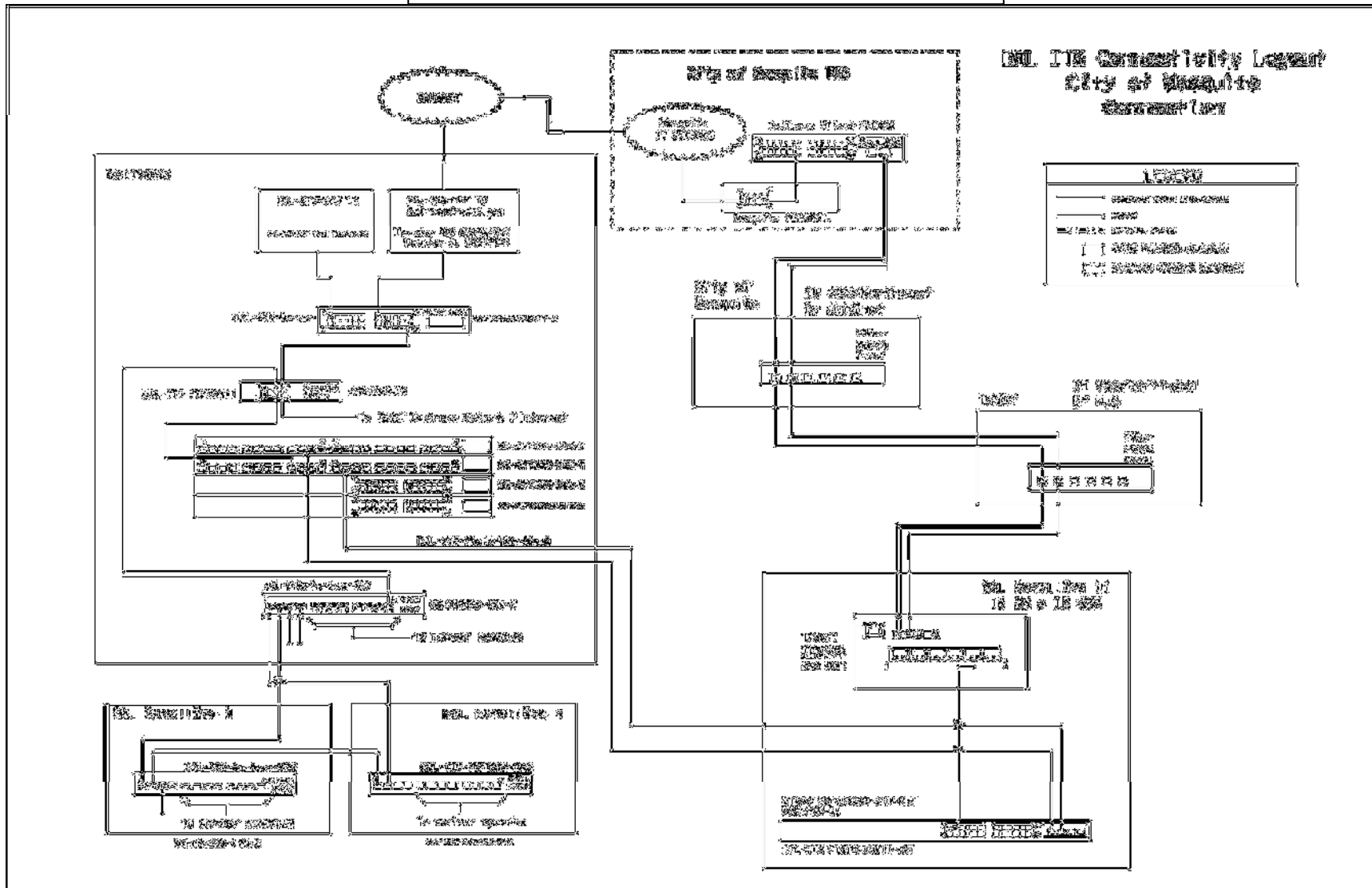
medium and may exist in forms such as books, papers, letters, documents, e-mails, Internet postings, text messages, instant messages, printouts, photographs, maps, drawings, and audio and video recordings. Public information does not include tangible items, such as computers or guardrails.

- 4.12 **“Regulated Data”** means information that its use and protection dictated by a state or federal agency or by third party agreements.
- 4.13 **“Sensitive Data”** means information that could be subject to release under an open records requests, but should be controlled to protect third parties, and should be vetted and verified before release. At TxDOT, this could include operational information, personnel records, research, or internal communications.
- 4.14 **“Sensitive Personal Information”** has the meaning provided by Section 521.002(2) of the Texas Government Code, which defines sensitive personal information as:
- (a) An individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and item are not encrypted:
    - (1) Social Security Number
    - (2) Driver’s license number or government-issued identification number; or
    - (3) Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or
  - (b) Information that identifies an individual and relates to:
    - (1) The physical or mental health or condition of the individual;
    - (2) The provision of health care to the individual; or
    - (3) Payment for the provision of health care to the individual.
- 4.15 **“TxDOT Security Questionnaire”** means a cybersecurity and privacy questionnaire that provides TxDOT ITD necessary information for third party attestation in accordance with TxDOT requirements.

ATTACHMENT D

Connectivity Diagram

IMPORTANT NOTICE: This Agreement is specific to TxDOT Traffic Data. TxDOT Traffic Video will be transmitted to Grantee through an internet connection as specified in a TxDOT *Agreement for Sharing Traffic Video*.



STATE OF TEXAS §  
 COUNTY OF TRAVIS §

**AGREEMENT for SHARING  
 TRAFFIC VIDEO**

**EXHIBIT B**

**CONTRACTING PARTIES:**

Texas Department of Transportation	<b>TxDOT</b>
City of Mesquite	<b>Grantee</b>

The Grantee desires TxDOT to grant rights to receive and use TxDOT traffic video (“Traffic Video”). TxDOT is agreeable to grant rights provided the Grantee agrees to the terms and conditions established in this agreement.

This agreement incorporates the provisions of **Attachment A**, Descriptions and Specifications of Rights Granted in Article 2, **Attachment B**, and **Attachment C** (Connectivity Diagram).

**BACKGROUND**

TxDOT, in accordance with Texas Transportation Code, §201.205, may:

1. Apply for, register, secure, hold and protect its intellectual property, patents, copyrights, trademarks, or other evidence of protection of exclusivity; and
2. Enter into non-exclusive license agreements with any third party for the receipt of fees, royalties, or other things of monetary and non-monetary value; and
3. Waive or reduce the amount of fees if it determines that such waiver will further the goal and missions of TxDOT and result in a net benefit to TxDOT; and

TxDOT – alone or as a stakeholder in multiple regional traffic management centers (TMCs), the regional traffic management center (TMC) – has trademark registrations on marks in accordance with the requirements of Title 15 U.S.C. Section 1051 et seq., as amended:

- Registration Number 1802491, hereinafter identified as the “TxDOT Logo.”
- Registration Number 3027037, hereinafter identified as the “DaITrans Logo.”
- Registration Number 3540052, hereinafter identified as the “TransVISION Logo.”
- Registration Number 3626456, hereinafter identified as the “TransVista Logo.”
- Registration Number 3660330, hereinafter identified as the “TransGuide Logo.”
- Registration Number 3987629, hereinafter identified as the “TranStar Logo.”

**AGREEMENT**

In consideration of the mutual promises contained in this agreement, TxDOT and the Grantee now agree as follows:

**ARTICLE 1. CONTRACT PERIOD**

This agreement becomes effective when signed and dated by the last party whose signing makes the agreement fully executed. This agreement shall terminate five (5) years from that date, or when otherwise modified or terminated, as hereinafter provided.

**ARTICLE 2. RIGHTS GRANTED**

TxDOT hereby grants the Grantee a non-exclusive right, license, and privilege worldwide to use all or portions of Traffic Video. The Grantee agrees that this agreement does not transfer or convey any ownership or any rights other than those rights expressly granted by the agreement.

**ARTICLE 3. PROVISION OF INFRASTRUCTURE**

The Grantee is responsible for providing and maintaining any hardware, software, and additional ITS infrastructure that may be necessary to obtain the Traffic Video. Grantee agrees that TxDOT does not guarantee the availability of the Traffic Video or a minimum response time to reestablish the availability of the Traffic Video due to maintenance or network or system failures. The Grantee shall not place any objects or equipment in the State Right-of-Way or on any other TxDOT property without advanced written permission from the District Engineer or designee.

**ARTICLE 4. FEE**

As the use of the Traffic Video will result in social, economic, and environmental mitigation, by increasing mobility and reducing congestion on public highways, TxDOT agrees to waive any monetary fee associated with the use of the Traffic Video.

**ARTICLE 5. COPYRIGHT INFRINGEMENT**

The Grantee shall notify TxDOT of any infringement or potential infringement by a third party, of which it becomes aware, of the copyright or any other rights owned by TxDOT relating to the use of the Traffic Video. The Grantee shall provide TxDOT, if feasible, any information or other assistance requested by TxDOT to assist in TxDOT's prosecution of any breaches or infringements.

**ARTICLE 6. ASSIGNMENT PROHIBITION**

The Grantee is prohibited from assigning any of the rights conferred by this agreement, to any third party. Notwithstanding the foregoing, the Grantee may assign the rights of this agreement of the Traffic Video to an affiliated corporate entity or to a purchaser of substantially all its assets without TxDOT's consent, provided that TxDOT's rights under this agreement remain unaffected. Any assignments shall be subject to the terms and conditions of this agreement.

**ARTICLE 7. TERMINATION**

- a) Including the provisions established herein, this agreement may be terminated by any of the following conditions.
  - i) Mutual agreement and consent of the parties hereto.
  - ii) By TxDOT for reason of its own and not subject to the approval of the Grantee upon not less than thirty (30) days written notice to the Grantee.
  - iii) By the Grantee for reason of its own and not subject to the approval of TxDOT upon not less than thirty (30) days written notice to TxDOT.
  - iv) Immediately for breach of this agreement as determined by TxDOT.
- b) Termination of the agreement shall extinguish all rights, duties, obligations, and liabilities of TxDOT and Grantee of this agreement. All rights granted to the Grantee shall revert to TxDOT as owner of the Traffic Video. Upon termination of this agreement, the Grantee will immediately cease transmitting, using, distributing and/or modifying the Traffic Video.
- c) Termination or expiration of this agreement shall not extinguish any of the Grantee's or TxDOT's obligations under this agreement which by their terms continue after the date of termination or expiration.

**ARTICLE 8. HOLD HARMLESS**

All provisions in this Article apply to Grantee to the extent allowed by law: The Grantee shall indemnify and save harmless TxDOT and its officers and employees from all claims and liability due to its materials or activities of itself, its agents, or employees, performed under this agreement and that are caused by or result from error, omission, or negligent act of the Grantee or of any person employed by the Grantee. The Grantee shall also indemnify and save harmless TxDOT from any and all expense, including but not limited to attorney fees that may be incurred by TxDOT in litigation or otherwise resisting the claim or liabilities that may be imposed on TxDOT as a result of such activities by the Grantee, its agents, or employees. The Grantee agrees to indemnify and save harmless TxDOT and its officers, agents, and employees from any and all claims, damages, and attorneys' fees arising from the use of outdated Traffic Data or other information. The Grantee's indemnification of TxDOT shall extend for a period of three (3) years beyond the date of termination of this agreement.

**ARTICLE 9. RELATIONSHIP BETWEEN THE PARTIES**

Each party acknowledges that it is not an agent, servant, or employee of the other party. Each party is responsible for its own acts and deeds and for those of its agents, servants, or employees.

**ARTICLE 10. REMEDIES**

Violation or breach of contract by the Grantee shall be grounds for termination of the agreement. Any increased costs arising from the Grantee's default, breach of contract or violation of contract terms shall be paid by the Grantee.

**ARTICLE 11. AMENDMENTS**

Any changes in the contract period, character, or agreement terms shall be enacted by a written amendment executed by both parties. Amendments must be executed during the contract period established in Article I.

**ARTICLE 12. VENUE**

This agreement is governed by the laws of the State of Texas.

**ARTICLE 13. NOTICES**

All notices to either party by the other party required under this agreement shall be delivered personally or sent by certified or U.S. Mail, postage prepaid, addressed to such party at the following respective physical addresses:

**STATE:** Texas Department of Transportation  
ATTN: Director, Traffic Safety Division  
125 E. 11<sup>th</sup> Street  
Austin, TX 78701

**GRANTEE:** City of Mesquite  
ATTN: Manager of Traffic Engineering and Street Lighting  
1515 North Galloway Avenue  
Mesquite, Texas 75149

and shall be deemed to be received by the addressee on the date so delivered or so deposited in the mail, unless otherwise provided within. Either party hereto may change the above address by sending written notice of such change to the other.

**ARTICLE 14. PUBLIC INFORMATION AND CONFIDENTIALITY**

A. The Grantee shall not disclose information obtained from TxDOT under this agreement without the express written consent of TxDOT.

B. The Grantee is required to make any information created or exchanged with the state pursuant to this contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the state.

**ARTICLE 15. COMPLIANCE WITH LAWS**

The Grantee shall comply with all applicable federal, state, and local laws, statutes, ordinances, rules, and regulations, and with the orders and decrees of any court or administrative bodies or tribunals in any manner affecting the performance of this agreement. When requested, the Grantee shall furnish TxDOT with satisfactory proof of this compliance. The Grantee shall provide or obtain all applicable permits, plans, or other documentation required by a federal or state entity.

**ARTICLE 16. COMPLIANCE WITH INFORMATION TECHNOLOGY REQUIREMENTS**

The third party will be creating, accessing, transmitting, storing, or using Public data in the third-party environment. The third-party's environment must comply with the TxDOT Low security baseline.

A copy of the TxDOT Information Security Controls Standards Catalog that outlines the security baseline requirements can be downloaded from

<https://www.txdot.gov/inside-txdot/division/information-technology/Cybersecurity/cybersecurity-resources.html>.

The third party must provide the following evidence that the third-party system is compliant with the TxDOT Low security baseline prior to any Public TxDOT data being created, accessed, transmitted, used, or stored in the third-party environment.

**ARTICLE 17. PROHIBITION AGAINST RECORDING OF TxDOT VIDEO**

Grantee further agrees that it shall not copy nor duplicate, or allow to be copied, any of the video that is provided by TxDOT in connection with this agreement, but Grantee shall, if it is a media outlet, have permission to maintain recorded footage from the provided Traffic Video that became part of its regular programming.

**ARTICLE 18. STATE AUDITOR'S PROVISION**

The State Auditor may conduct an audit or investigation of any entity receiving funds from TxDOT directly under this agreement or indirectly through a subcontract under this agreement. Acceptance of funds directly under this agreement or indirectly through a subcontract under this agreement acts as acceptance of the authority of the State Auditor, under the direction of the legislative audit committee, to conduct an audit or investigation in connection with those funds. An entity that is the subject of an audit or investigation must provide the State Auditor with access to any information the State Auditor considers relevant to the investigation or audit.

**ARTICLE 19. SIGNATORY WARRANTY**

The signatories to this agreement warrant that each has the authority to enter into this agreement on behalf of the party they represent.

**IN TESTIMONY WHEREOF**, TxDOT and the Grantee have executed duplicate counterparts of this agreement.

**CITY OF MESQUITE**

By \_\_\_\_\_ Date \_\_\_\_\_  
Cliff Keheley, City Manager

**THE STATE OF TEXAS**

Executed for the Executive Director and approved for the Texas Transportation Commission for the purpose and effect of activating and/or carrying out the orders, established policies or work programs heretofore approved and authorized by the Texas Transportation Commission.

By \_\_\_\_\_ Date \_\_\_\_\_  
Michael A. Chacon, P.E., Director, Traffic Safety Division

**ATTACHMENT A**  
**Descriptions and Specifications of Rights Granted**

<b>RIGHTS GRANTED</b>	
<b>By TxDOT</b>	<b>By Grantee</b>
<ol style="list-style-type: none"> <li>1. TxDOT will make its Traffic Video available to Grantee.</li> <li>2. TxDOT hereby grants Grantee a limited revocable non-exclusive license to use the registered TxDOT trademark logo (TxDOT Flying "T") for the purpose of attributing TxDOT as a video's source. Grantee shall not make any use of the registered TxDOT trademark logo on any other materials or documents unless it first submits that request in writing to TxDOT and receives approval for the proposed use. Grantee shall not alter, modify, dilute, or otherwise misuse the registered TxDOT trademark logo or bring it into disrepute. Grantee's use of the Flying 'T' under this article must be followed by the capital letter R enclosed within a circle (®) giving notice that the Flying 'T' is registered in the United States Patent and Trademark Office. Grantee shall not assign or sublicense the rights granted by this article without the prior written consent of the TxDOT. Grant of this license will terminate upon termination of this agreement.</li> </ol>	<ol style="list-style-type: none"> <li>1. Grantee will use traffic video to monitor real-time traffic conditions for immediate response to traffic crashes or delays.</li> <li>2. Grantee shall provide TxDOT with Non-Monetary Compensation as identified below.</li> </ol>

<b>NON-MONETARY COMPENSATION</b>	
<b>By TxDOT</b>	<b>By Grantee</b>
<ol style="list-style-type: none"> <li>1. None</li> </ol>	<ol style="list-style-type: none"> <li>1. Grantee shall provide TxDOT with a list of IP addresses for all City owned traffic cameras.</li> <li>2. Grantee shall give TxDOT and/or TMC voice and/or visual credit (TxDOT and/or TMC logos) for all Video provided by TxDOT. TxDOT may transmit Video to the Grantee with an embedded logo; the Grantee shall not block, modify, or remove the Logo.</li> </ol>

## **ATTACHMENT B**

### **Information Resources and Security Requirements**

#### **TYPES OF DATA**

“**TxDOT Data**” means TxDOT information, data, records, and information to which the Contractor has access, has possession, or is otherwise provided to the Contractor by TxDOT, whether or not intended under or for the purposes of the agreement, including, without limitation, data generated or collected under this agreement, intellectual property created as a work for hire under this agreement, and Personal Identifying Information (as defined below).

TxDOT Data is classified into the four categories that control applicability of security standards: Regulated, Confidential, Sensitive, and Public. See Section 4 for Definitions.

Any data that the Contractor accesses and downloads from a TxDOT system, for use, manipulation, storage, or management is considered Confidential Data unless otherwise specified in writing by TxDOT.

#### **DATA REQUIREMENTS**

##### Data, Data Dictionaries, and Data Flow Diagrams

Contractor shall ensure that all TxDOT Data that is generated, manipulated, transmitted, or stored, utilizes the TxDOT taxonomy, with documented data dictionaries, and data flow diagrams (including security protocols).

##### Data Transfer

At the completion of a deliverable, the Contractor shall transfer all TxDOT Data generated and stored for that deliverable to TxDOT in a manner and format acceptable to TxDOT and approved by TxDOT’s Information Technology Division (“**ITD**”).

All metadata associated with the TxDOT Data transferred must remain attached to that data.

Contractor shall maintain the appropriate level of data security throughout the transfer of the TxDOT Data.

##### Backup and Disaster Recovery

Contractor shall implement business continuity procedures to fulfill all requirements of this agreement that address, as a minimum, fire, theft, natural disaster, technical difficulty, workforce problems equipment failure, or other disruption of business.

Contractor shall maintain a disaster recovery plan. Contractor is responsible for all project related costs of disaster recovery during the project except for costs associated with disasters beyond Contractor’s reasonable control, and for those costs included as part of the TxDOT infrastructure responsibilities.

##### Open Records Requests

Contractor shall not release Information in response to an open record request related to this agreement request unless TxDOT has approved the release in writing.

##### Encryption

For Sensitive, Confidential, and Regulated TxDOT Data, the Contractor shall encrypt the TxDOT Data while in-transit and while at-rest in accordance with the TxDOT Controls Catalog Standard SC-13, Cryptographic Protection and SC-08, Transmission Confidentiality and Integrity security requirements.

##### Accessibility

State agencies shall procure products which comply with the State of Texas Accessibility requirements for Electronic and Information Resources specified in 1 Texas Administrative Code (TAC) Chapters 206 and 213 when such products are available in the commercial marketplace or when such products are developed in response to a procurement solicitation. Vendor represents and warrants that technology to be provided to TxDOT and for TxDOT is in compliance with these requirements.

## INFORMATION RESOURCE AND SECURITY REQUIREMENTS

### Information Security Safeguards

Contractor shall implement appropriate administrative, physical, and technical safeguards, in accordance with TxDOT's security requirements, that reasonably and appropriately protects the confidentiality, integrity, and availability of TxDOT Data.

Contractor shall conform its policies and procedures relating to the implementation of security safeguards to comply with TxDOT's Information Resources security program pursuant to the TxDOT and DIR's Information Security Controls Catalog Standards.

### Potential Cybersecurity Incident or Breach Notification

Contractor shall immediately report to TxDOT via the Report Cybersecurity Incident Page on TxDOT.gov, any potential cybersecurity incident or breach involving TxDOT Data (See Section 4, Definitions).

### Demonstrating Compliance with Information Security Requirements

Prior to contract award, at renewal, on a recurring basis as documented in the contract, upon reasonable notice to the Contractor, and if TxDOT determines that the Contractor has violated this agreement, TxDOT, directly or through its agent, may request an attestation, which may include the TxDOT Security Questionnaire or additional attestations, and evidence that Contractor is in compliance with applicable laws, regulations, and standards outlined in 3.5.

### Security Training

In accordance with Section 2054.5192 of the Texas Government Code, each Contractor Personnel that will access a TxDOT computer system or database must complete a TxDOT approved cybersecurity training program that is certified under Section 2054.5192 of the Texas Government Code. The training program must be completed by each Contractor Personnel during the term of the contract and during any renewal period. The Contractor shall provide verification of completion of the cybersecurity training program in a method designated by TxDOT.

In this section 3, "**Contractor Personnel**" means all persons under the control of the Contractor including officers and employees of both the Contractor and its subcontractors.

### Applicable Laws, Regulations, and Standards

Contractor shall perform the services in accordance with the following standards, notify TxDOT of situations where compliance is not achievable, and assist TxDOT with the prevention of security gaps or conflicts that could impair security performance. Contractor shall comply with all applicable federal, state, and local laws and regulations necessary to perform the services. A non-exhaustive list of federal, state, and local laws and regulations that might be applicable include the following.

#### DIR Security Controls Standard Catalog and applicable TxDOT Security Requirements

For Public Data, TxDOT and DIR Security Controls Standards Catalog low baseline and applicable TxDOT security requirements.

For Sensitive Data TxDOT and DIR Security Controls Standards Catalog low baseline with Sensitive overlay and applicable TxDOT security requirements.

For Confidential, TxDOT and DIR Security Controls Standards Catalog moderate baseline and applicable TxDOT security requirements.

For Regulated Data, TxDOT and DIR Security Controls Standards Catalog moderate baseline, applicable TxDOT security requirements, and applicable regulated security requirements.

(1) TX-RAMP Requirements

- (A) Any third party providing a cloud computing service to TxDOT to create, access, transmit, use, or store TxDOT data must be authorized in the Texas Risk and Authorization Management Program (“**TX-RAMP**”)
- (B) TX-RAMP provisional status may be considered in lieu of a TX-RAMP certification if approved by the TxDOT Chief Information Security Officer (“**CISO**”).
- (C) Applicable third parties must achieve the following levels of authorization by the following dates for any new contract or renewal of existing contract:
  - Low Security Baseline – TX-RAMP Level 1 Status no later than January 1, 2023
  - Moderate Security Baseline – TX-RAMP Level 2 Status no later than January 1, 2022
  - High Security Baseline – Federal Risk and Authorization Management Program (“**FedRAMP**”) High Baseline no later than January 1, 2022

State Laws and Regulations:

- Texas Administrative Code, Chapter 202 – Information Security Standards
- Texas Administrative Code, Chapter 206 – State Websites
- Texas Administrative Code, Chapter 213 – Electronic and Information Resources
- Texas Government Code, Chapter 552 – Public Information
- Texas Government Code, Chapter 2054 – Information Resources
- Texas Penal Code, Chapter 33 – Computer Crimes
- For Confidential data, Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information
- For Confidential data containing Protected Health Information, Texas Health and Safety Code, Chapter 181 – Medical Records Privacy
- For Regulated data containing Payment Card Industry (PCI) information, the Payment Card Industry Data Security Standards (PCI-DSS)
- For Regulated data containing Criminal Justice Information (CJI), the Criminal Justice Information Services (CJIS) Security Policy

Information Resources Technology

Any proposed information resources technology that will be installed on any TxDOT owned equipment or that will access any TxDOT network must be reviewed and approved by the ITD Architectural Review Board (“**ARB**”) prior to any development or design.

Any proposed information resources technology that will be installed on any TxDOT owned equipment or that will access any TxDOT network must be reviewed and approved by the ITD Change Advisory Board (“**CAB**”) prior to implementation or delivery.

Information Resources Technology (“**IRT**”) Procurements

ITD must approve all procurements of:

Information Resources Technology that will be owned by TxDOT.

IT services for any environment that provides processing, storage, networking, management and the distribution of data to ensure alignment with Texas Government Code, Chapter 2054, Subchapter L.

#### Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

In accordance with 2 CFR §§ 200.216 and 200.471, Contractor shall not provide services, equipment, or systems for telecommunications or video surveillance that (a) are provided or manufactured by or (b) have components provided or manufactured by any of the following business entities:

Huawei Technologies Company

ZTE Corporation

Hyatera Communications Corporation

Hangzhou Hikvision Digital Technology Company

Dahua Technology Company

Any subsidiary or affiliate of an entity listed above

#### DEFINED TERMS

**“Breach”** means “breach of system security” as defined in Section 521.053(a) of the Texas Business and Commerce Code, which defines breach of system security as “the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.”

**“Cloud Computing Service”** means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is referenced in Texas Government Code Title 10, Subtitle D, Chapter 2157, Subchapter A, Section 2157.007 and is defined in NIST 800-145.

**“Confidential Information”** has the meaning provided in 1 Texas Administrative Code § 202.1(5), which states the confidential information means “information that must be protected from unauthorized disclosure or public release based on published laws or legal agreements.” Information that is Confidential Information under this definition includes:

Dates of birth of living persons

Driver’s license numbers

License plate numbers

Credit card numbers

Insurance policy numbers

Attorney-Client communications

Drafts of policymaking documents

Information related to pending litigation

Audit working papers

Competitive bidding information before contract awarded.

Personal Identifiable Information

Sensitive Personal Information

Regulated data

Information excepted from disclosure requirements of Chapter 552 of the Texas Government Code (“**Texas Public Information Act**”) or other applicable state or federal law

Compliance reports for which the Texas Attorney General has granted permission to withhold

Investigative working papers and draft reports excepted from disclosure under Section 552.116 of the Texas Government Code

“**Data**” means the representation of facts; as the raw material of information that is used as a basis for reasoning, decision-making, discussion, or calculation.

“**Data Dictionary**” means a directory of the definitions, purpose, policies and structure about data. It is a compilation of information about the data owned by the enterprise. It describes every data item in a database in enough detail for users and application developers to know what the data is and how to make use of it.

“**Information**” means data, regardless of form, that is created, contained in, or processed by information resources facilities, communications networks, or storage media.

“**Information Resources Technology**” means data processing and telecommunications hardware, software, services, supplies personnel, facility resources, maintenance and training that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

“**Personal Identifying Information**” means information that alone or in conjunction with other information identifies an individual, including an individual's:

Name, social security number, date of birth, or government-issued identification number;

Mother's maiden name;

Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

Unique electronic identification number, address, or routing code; and

“**Potential Cybersecurity Incident**” means an event which may result in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.

“**Public Data**” means Data that is subject to public disclosure pursuant to the Texas Public Information Act and freely and without reservation made available to the public.

“**Public information**” means information written, produced, collected, assembled, or maintained by or for a governmental body, including information held by individual officers or employees of a governmental body, in connection with the transaction of official TxDOT business. This includes information that is held by contractors and consultants and that TxDOT owns, to which TxDOT has a right of access, or on which public money was spent for the purpose of writing, producing, collecting, assembling, or maintaining the information. Public information includes any electronic communication created, transmitted, received, or maintained on any device if the communication is in connection with the transaction of official business. Public information may be stored in any medium and may exist in forms such as books, papers, letters, documents, e-mails, Internet postings, text messages, instant messages, printouts, photographs, maps, drawings, and audio and video recordings. Public information does not include tangible items, such as computers or guardrails.

“**Regulated Data**” means information that its use and protection dictated by a state or federal agency or by third party agreements.

**“Sensitive Data”** means information that could be subject to release under an open records request, but should be controlled to protect third parties, and should be vetted and verified before release. At TxDOT, this could include operational information, personnel records, research, or internal communications.

**“Sensitive Personal Information”** has the meaning provided by Section 521.002(2) of the Texas Government Code, which defines sensitive personal information as:

An individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and item are not encrypted:

Social Security Number

Driver’s license number or government-issued identification number; or

Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;  
or

Information that identifies an individual and relates to:

The physical or mental health or condition of the individual;

The provision of health care to the individual; or

Payment for the provision of health care to the individual.

**“TxDOT Security Questionnaire”** means a cybersecurity and privacy questionnaire that provides TxDOT ITD necessary information for third party attestation in accordance with TxDOT requirements.

**ATTACHMENT C**  
**Connectivity Diagram**

